Finiteness theorems for torsion of
abelian varieties over large algebraic fields

by

Marcel Jacobson (Jerusalem) and Moshe Jarden (Tel Aviv)

Introduction. The main goal of our work is to prove the following result:

MAIN THEOREM. *Let K be a finitely generated field, A an abelian variety over K, and e a positive integer. Then the following statements hold for almost all $\boldsymbol{\sigma} \in G(K)^e$:*

(a) *$A_{l^\infty}(\widetilde{K}(\boldsymbol{\sigma}))$ is a finite group for all prime numbers l.*

(b) *If $e \geq 2$ and $\operatorname{char}(K) = 0$, then $A_{\operatorname{tor}}(\widetilde{K}(\boldsymbol{\sigma}))$ is a finite group.*

Here we say that a field K is *finitely generated* if it is finitely generated over its prime field. We denote the separable (resp. algebraic) closure of K by K_{s} (resp. $\widetilde{K}$) and let $G(K) = \mathcal{G}(K_{\mathrm{s}}/K)$ be the *absolute Galois group* of K. Each $\sigma \in G(K)$ uniquely extends to an automorphism of $\widetilde{K}$ having the same notation σ. We consider the cartesian product $G(K)^e$ of e copies of $G(K)$. If $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e)$ is in $G(K)^e$ and N is a normal extension of K, then $N(\boldsymbol{\sigma})$ is the fixed field in N of $\sigma_1, \ldots, \sigma_e$. In particular, $\widetilde{K}(\boldsymbol{\sigma}) = K_{\mathrm{s}}(\boldsymbol{\sigma})_{\mathrm{ins}}$ is the maximal purely inseparable extension of $K_{\mathrm{s}}(\boldsymbol{\sigma})$. In general we denote the maximal purely inseparable extension of a field M by M_{ins}.

For an abelian variety A which is defined over K (usually abbreviated to "an abelian variety A over K") and for each positive integer n let A_n be the kernel of multiplying A by n. If M is an extension of K, then $A_n(M) = \{\mathbf{p} \in A(M) \mid n\mathbf{p} = 0\}$. We use l to denote prime numbers and let $A_{l^\infty}(M) = \bigcup_{i=1}^\infty A_{l^i}(M)$. We also let $A_{\operatorname{tor}}(M)$ be the group of all points of $A(M)$ of finite order.

Finally, we equip $G(K)^e$ with the unique Haar measure μ_K which is normalized with $\mu_K(G(K)) = 1$. Then the clause "for almost all $\boldsymbol{\sigma} \in G(K)^e$"

means as usual "for all but a set of measure 0 of $\boldsymbol{\sigma}$ in $G(K)^e$". This ends the explanation of the Main Theorem.

The Main Theorem solves Part (C) of the Geyer–Jarden Conjecture in all cases and Part (B) for $\mathrm{char}(K) = 0$.

CONJECTURE OF GEYER–JARDEN [GeJ]. *Let K be a finitely generated field, A an abelian variety over K, and e a positive integer. Then the following statements hold for almost all $\boldsymbol{\sigma} \in G(K)^e$:*

(A)   *If $e = 1$, then there are infinitely many prime numbers l with $A_l(K_\mathrm{s}(\boldsymbol{\sigma})) \neq 0$.*

(B)   *If $e \geq 2$, there are only finitely many l with $A_l(K_\mathrm{s}(\boldsymbol{\sigma})) \neq 0$.*

(C)   *If $e = 1$, then for each l the group $A_{l^\infty}(\widetilde{K}(\boldsymbol{\sigma}))$ is finite.*

Since the intersection of countably many sets of measure 1 is again a set of measure 1, and since a variety which is defined over $\widetilde{K}$ is already defined over a finite extension of K, it is possible to switch the order of the quantifiers in the Geyer–Jarden Conjecture (Remark 3.8):

COROLLARY TO THE GEYER–JARDEN CONJECTURE. *Let K be a finitely generated field and e a positive integer. Then for almost all $\boldsymbol{\sigma} \in G(K)^e$ and for each abelian variety A over $\widetilde{K}(\boldsymbol{\sigma})$ the following statements hold:*

(I) *If $e = 1$, then $A_\mathrm{tor}(\widetilde{K}(\boldsymbol{\sigma}))$ is infinite.*

(II) *If $e \geq 2$, then $A_\mathrm{tor}(\widetilde{K}(\boldsymbol{\sigma}))$ is finite.*

The main result of [GeJ] is that the Geyer–Jarden Conjecture holds for elliptic curves. The proof relies on an analysis of the action of $G(K)$ on $A_n(\widetilde{K})$ and on $A_{l^\infty}(\widetilde{K})$, where A is now an elliptic curve over K. This action gives rise to representations $\varrho_{A,n} : G(K) \to \mathrm{GL}(2d, \mathbb{Z}/n\mathbb{Z})$ and $\varrho_{A,l^\infty} : G(K) \to \mathrm{GL}(2d, \mathbb{Z}_l)$, where $d = 1 = \dim(A)$ (at least if $\mathrm{char}(K) \nmid n$ and $\mathrm{char}(K) \neq l$). The proof distinguishes between five cases. In each of these cases, the image of $G(K)$ in the corresponding matrix group is known to such an extent that allows the computation of the probability that an e-tuple of elements has a common eigenvector.

As the dimension of A grows, the number of types of those representations grows. Moreover, there are only few cases in the literature where those representations are described in detail. So, any attempt to prove the Geyer–Jarden Conjecture should rely on general principles which are less precise than those used for elliptic curves but powerful enough to yield the desired result.

Our previous work [JaJ1] uses such principles to prove Part (C) of the conjecture for every global field K and for $l \neq \mathrm{char}(K)$. There is an attempt in [JaJ1] to prove Part (A) of the conjecture for an arbitrary finitely gen-

erated field of positive characteristic. Unfortunately, the proof contains an error (see [JaJ2]).

In this work we use the same principles as in [JaJ1] in a more careful way and complete the proof of Part (C) of the conjecture in all cases.

We also use a result of Bogomolov–Serre which asserts that if K is a number field, then $\varrho_{A,l}(G(K))$ contains "many" homotheties. This leads to a proof of Part (B) of the conjecture for number fields. The theory of good reduction of abelian varieties extends the result to arbitrary finitely generated extensions of K.

Part (B) of the conjecture in positive characteristic and Part (A) of the conjecture are still open.

1. Torsion of abelian varieties under good reduction. We enhance the theory of good reduction of abelian varieties with some ingredients which are not well documented in the literature. We use it in the next section to prove Part (C) of the Geyer–Jarden Conjecture.

Let K be a field of characteristic p equipped with a valuation v. Choose an extension $\widetilde{v}$ of v to $\widetilde{K}$. Denote reduction of objects at $\widetilde{v}$ by a bar. We will be careful to make only such statements on the reduced objects which will depend on v but not on $\widetilde{v}$. If we wish to make the reference to v explicit, we add v as an index. We use the expression "for almost all v" as an abbreviation for "there exist $a_1, \ldots, a_n \in K^\times$ such that for all valuations v of K which satisfy $v(a_i) = 0$, $i = 1, \ldots, n$".

Denote the *Tate module* of an abelian variety A over a field K associated with a prime number l by $T_l(A)$. By definition, $T_l(A) = \varprojlim A_{l^i}(\widetilde{K})$, where the maps $A_{l^n}(\widetilde{K}) \to A_{l^{n-1}}(\widetilde{K})$ are multiplication by l.

LEMMA 1.1. *Let A be an abelian variety over K and let l be a prime number. Then, for almost all valuations v of K, reduction at v induces isomorphisms $A_{l^n}(\widetilde{K}) \to \overline{A}_{l^n}(\overline{\widetilde{K}})$, $n = 1, 2, \ldots$ and $T_l(A) \to \overline{T}_l(\overline{A})$.*

Proof. Shimura and Taniyama prove that for almost all v, A has good reduction at v. That is, $\overline{A}$ is an abelian variety over $\overline{K}$ [ShT, p. 109, Prop. 25]. Alternatively, one may consider A as a closed algebraic subgroup of $\mathbb{P}^n$ [Mil, p. 113, Thm. 7.1]. Together with the group operations, A is defined by finitely many polynomials with coefficients in K. The conditions on A to be an abelian variety translate into elementary statements on the coefficients which should be satisfied over $\widetilde{K}$. By elimination of quantifiers for the elementary theory of algebraically closed fields [FrJ, Thm. 8.3], these statements remain true over $\overline{\widetilde{K}}$ for almost all v (see also [Jar, §1]).

Suppose A has good reduction at v. It defines a homomorphism $\varphi : A(\widetilde{K}) \to \overline{A}(\overline{\widetilde{K}})$ of groups. For each n let $\varphi_n : A_n(\widetilde{K}) \to \overline{A}_n(\overline{\widetilde{K}})$ be the corresponding restriction of φ.

Consider points $\mathbf{p}_1, \ldots, \mathbf{p}_m$ of $A(\widetilde{K})$. Then "$\mathbf{p}_1, \ldots, \mathbf{p}_m$ are the distinct points of order l in $A(\widetilde{K})$" is an elementary statement on $\widetilde{K}$. Hence, as in the preceding paragraph, it remains true for almost all v. In other words, for almost all v, $\overline{\mathbf{p}}_1, \ldots, \overline{\mathbf{p}}_m$ are the distinct points of order l in $\overline{A}(\widetilde{\overline{K}})$. So, φ_l is bijective.

There exists a nonnegative integer r with $A_{l^i}(\widetilde{K}) \cong (\mathbb{Z}/l^i\mathbb{Z})^r$ for each i. If $l \neq p$, then $r = 2\dim(A)$. If $l = p$, then $0 \leq r \leq \dim(A)$ [Mum, p. 64]. Similarly, there exists a nonnegative integer $\overline{r}$ with $\overline{A}_{l^i}(\widetilde{\overline{K}}) \cong (\mathbb{Z}/l^i\mathbb{Z})^{\overline{r}}$ for each i. By the preceding paragraph $r = \overline{r}$. So,

$$(1) \qquad |A_{l^i}(\widetilde{K})| = |\overline{A}_{l^i}(\widetilde{\overline{K}})|, \quad i = 1, 2, \ldots$$

Since φ_l is surjective, Nakayama's lemma implies that φ_{l^i} is surjective. Hence, by (1), φ_{l^i} is bijective.

Finally, taking the inverse limit over all i, the φ_i define an isomorphism $\varphi : T_l(A) \to T_l(\overline{A})$. ∎

For a field K, an abelian variety A over K, and a positive integer n write $K(A_n)$ for $K(A_n(\widetilde{K}))$. Also, let $K(A_{l^\infty}) = \bigcup_{i=1}^\infty K(A_{l^i})$.

COROLLARY 1.2. *Let A be an abelian variety over a field K and let l be a prime number. Then almost all valuations v of K have trivial inertia groups in $K(A_{l^\infty}) \cap K_s$. In particular, almost all discrete valuations v of K are unramified in $K(A_{l^\infty}) \cap K_s$.*

Proof. Replace K by K_{ins}, if necessary, to assume that K is perfect. It suffices to prove that each v satisfying the conclusion of Lemma 1.1 has trivial inertia groups in $K(A_{l^\infty})$. Since $K(A_{l^\infty}) = \bigcup_{i=1}^\infty K(A_{l^i})$, it suffices to prove that for each n, v has trivial inertia groups in $N = K(A_{l^i})$.

We repeat a well known argument. Let w be an extension of v to N. Let $D(w) = \{\sigma \in \mathcal{G}(N/K) \mid w(x) \geq 0 \text{ implies } v(\sigma x) \geq 0 \text{ for each } x \in N\}$ be the decomposition group of w in N/K. Then the map $D(w) \to \mathcal{G}(\overline{K}(\overline{A}_{l^n})/\overline{K})$ given by $\sigma \mapsto \overline{\sigma}$ with $\overline{\sigma}\,\overline{x} = \overline{\sigma x}$ if $x \in N$ and $w(x) \geq 0$ is a homomorphism whose kernel is the inertia group $I(w)$. We prove that $I(w)$ is trivial. (This will also imply that $\overline{K}(\overline{A}_{l^n})/\overline{K}$ is Galois [Ser3, p. 33, Remarque].)

Indeed, let $\sigma \in I(w)$ and consider $\mathbf{p} \in A_{l^n}(\widetilde{K})$. Then $\overline{\sigma \mathbf{p}} = \overline{\sigma}\,\overline{\mathbf{p}} = \overline{\mathbf{p}}$ and $\sigma \mathbf{p} \in A_{l^n}(\widetilde{K})$. By our choice of v, $\sigma \mathbf{p} = \mathbf{p}$. We conclude that $\sigma = 1$, as desired. ∎

2. Finiteness of the l-power torsion. In this section we prove Part (C) of the Geyer–Jarden Conjecture. The proof uses the following condition on a field K:

(C′)   Let A be an abelian variety over K and l a prime number. Then $A_{l^\infty}(\widetilde{K}(\sigma))$ is finite for almost all $\sigma \in G(K)$.

REMARK 2.1 (Reduction steps). (a) Let A be an abelian variety over a field K. Let L be a purely inseparable extension of K. Then $\mathrm{res}_{K_\mathrm{s}} : G(L) \to G(K)$ is an isomorphism. If $\sigma' \in G(L)$ and $\sigma = \mathrm{res}_{K_\mathrm{s}}(\sigma')$, then $\widetilde{K}(\sigma) = \widetilde{L}(\sigma')$. Hence, $A_{l^\infty}(\widetilde{K}(\sigma))$ is finite for almost all $\sigma \in G(K)$ if and only if $A_{l^\infty}(\widetilde{L}(\sigma))$ is finite for almost all $\sigma \in G(L)$.

(b) The field $N = K(A_{l^\infty})$ is a normal extension of K. If $l \neq \mathrm{char}(K)$, then multiplication by l^i is an étale endomorphism of A [Mum, p. 64, Prop. 2 and p. 74, Cor. 1]. In particular, it is étale over 0. Hence, N/K is Galois. So, $A_{l^\infty}(M) = A_{l^\infty}(M_\mathrm{ins})$ for each algebraic extension M of K. In particular, $A_{l^\infty}(\widetilde{K}(\sigma)) = A_{l^\infty}(K_\mathrm{s}(\sigma))$ for each $\sigma \in G(K)$.

If, however, $l = \mathrm{char}(K)$, this need not be the case. For example, let $K = \mathbb{F}_p((t))$ be the field of formal power series in t over $\mathbb{F}_p$ and A the Tate curve over K with period t. By [Roq, p. 19, IV and V], $A(L) = L^\times/\langle t \rangle$ for every finite extension L of K. In particular, $K(A_p) = K(t^{1/p})$ is a purely inseparable extension of K of degree p.

The arguments of the first paragraph (of step (b)) also imply that $\bigcup_l A_l(M)$ is finite if and only if $\bigcup A_l(M_\mathrm{ins})$ is finite.

(c) Let M be an algebraic extension of K. We prove that $T_l(A)(M) \neq 0$ if and only if $A_{l^\infty}(M)$ is infinite.

Indeed, if $T_l(A)(M)$ has a nonzero point $\mathbf{p}$, then there is i_0 such that for all $i \geq i_0$, the ith component $\mathbf{p}_i$ of $\mathbf{p}$ is a nonzero point in $A_{l^i}(M)$. Moreover, $l\mathbf{p}_{i+1} = \mathbf{p}_i$ and therefore $l \cdot \mathrm{ord}(\mathbf{p}_i) = \mathrm{ord}(\mathbf{p}_{i+1})$. Thus, the $\mathbf{p}_i$, $i \geq i_0$, are distinct.

Conversely, suppose $A_{l^\infty}(M)$ is infinite. Since each $A_{l^i}(M)$ is finite, there are infinitely many i's with $A_{l^i}^*(M) = \{\mathbf{p} \in A_{l^i}(M) \mid \mathrm{ord}(\mathbf{p}) = l^i\}$ nonempty. It follows from $l \cdot \mathrm{ord}(l\mathbf{p}) = \mathrm{ord}(\mathbf{p})$ that each of the finite sets $A_{l^i}^*(M)$ is nonempty. The same formula implies that multiplication by l maps $A_{l^{i+1}}^*(M)$ into $A_{l^i}^*(M)$. Hence, $\varprojlim A_{l^i}^*(M)$ is nonempty [FrJ, Lemma 1.2]. Each point in the inverse limit is a nonzero point of $T_l(A)(M)$. ∎

Proposition 5.1 of [JaJ1] proves (C′) for every global field K and every prime number $l \neq \mathrm{char}(K)$. Having proved Lemma 1.1 and Corollary 1.2, the proof of [JaJ1, Prop. 5.1] basically works also for the remaining case where $l = \mathrm{char}(K)$. Since it requires no extra effort, we state and prove the result over global fields for all l.

PROPOSITION 2.2. *Every global field K satisfies condition* (C′).

Proof. Let A and l be as in (C′). The field $N = K(A_{l^\infty})$ is a normal extension of K. Let L be the maximal separable subextension of N/K and K' the fixed field in N of $\mathrm{Aut}(N/K)$. Then K' is a purely inseparable extension of K, both L/K and N/K' are Galois extensions, and $\mathrm{res}_L : \mathcal{G}(N/K') \to \mathcal{G}(L/K)$ is an isomorphism.

We have to prove that almost no $\sigma \in \mathcal{G}(N/K')$ fixes a nonzero element of $T_l(A)$ (Remark 2.1(c)). To this end let r be a nonnegative integer with $T_l(A) \cong \mathbb{Z}_l^r$. Then the action of $\mathcal{G}(N/K')$ on $T_l(A)$ defines an isomorphism ϱ of $\mathcal{G}(N/K')$ onto a closed subgroup G of $\mathrm{GL}(r, \mathbb{Z}_l)$. In particular G is an l-adic Lie group.

Let S be the set of all $\sigma \in \mathcal{G}(N/K')$ that fix a nonzero element of $T_l(A)$. Then ϱ maps S onto the set of all $g \in G$ for which 1 is an eigenvalue. In other words, $\varrho(S) = \{g \in G \mid \det(1 - g) = 0\}$. It follows that $\varrho(S)$ is an analytic subset of G. As such, $\varrho(S)$ has a boundary of Haar measure zero in G [Ser2, p. I-8, Exercise; alternatively, use Proposition 4.2]. We conclude that S is a closed subset of $\mathcal{G}(N/K')$ with boundary of Haar measure zero. In addition, S is invariant under conjugation by elements of $\mathcal{G}(N/K')$. It follows that $\mathrm{res}_L S$ is a $\mathcal{G}(L/K)$-invariant closed subset of $\mathcal{G}(L/K)$ whose boundary is of measure 0.

Assume $\mu(S) > 0$. Then $\mu(\mathrm{res}_L S) > 0$. By Corollary 1.2, almost all primes of K are unramified in L. As K is global, "almost all" means "all but finitely many". Hence by a generalization of the Chebotarev density theorem [Ser2, I-8, Cor. 2; alternatively, use Proposition 4.3], the set of all primes $\mathfrak{p}$ of K such that

(1) $\mathfrak{p}$ is unramified in L and $\left(\frac{L/K}{\mathfrak{p}}\right) \subseteq \mathrm{res}_L S$

has a positive Dirichlet density. In particular, the set is infinite. Hence, by Lemma 1.1, there exists $\mathfrak{p}$ with the property (1) such that

(2) A has a good reduction at $\mathfrak{p}$, and

(3)   the maps $A_{l^n}(\overline{K}) \to \overline{A}_{l^n}(\widetilde{\overline{K}})$, $n = 1, 2, \ldots$ are bijective.

Let $\sigma \in \mathcal{G}(L/K)$ be a Frobenius element over $\mathfrak{p}$ and extend σ to an element of $\mathrm{Aut}(N/K)$ (also denoted by σ) in the unique possible way. Then $\sigma \in S$ (by (1)) and therefore σ fixes infinitely many points of $A_{l^\infty}(\overline{K})$. Reduction modulo $\mathfrak{p}$ maps σ onto the Frobenius automorphism $\mathrm{Frob}_{\overline{K}}$ of $G(\overline{K})$. By (3), $\mathrm{Frob}_{\overline{K}}$ fixes infinitely many points of $\overline{A}_{l^\infty}(\widetilde{\overline{K}})$. Each of these points is in $\overline{A}_{l^\infty}(\overline{K})$. Hence $\overline{K}$ is an infinite field. But $\overline{K}$, as a residue field of a global field, must be finite. This contradiction proves that our assumption is false. We conclude that $\mu(S) = 0$. ∎

Next we prove that the finiteness of $A_{l^\infty}(\widetilde{K}(\boldsymbol{\sigma}))$ is preserved under finitely generated extensions of K.

LEMMA 2.3. *Let G be a closed subgroup of $\mathrm{GL}(n, \mathbb{Z}_l)$. Then*

(a) *G is finitely generated* (*as a topological group*);

(b) *G has an open pro-l subgroup; and*

(c) *the Frattini subgroup, $\Phi(G)$, of G is open.*

Proof. (a) Indeed, the number of generators of G is bounded by a constant which depends only on $\mathrm{GL}(n, \mathbb{Z}_l)$ (and not on G) [DSM, Thm. 5.2 and the remark that follows the theorem].

(b) The subgroup $\Gamma_1 = \{g \in \mathrm{GL}(n, \mathbb{Z}_l) \mid g \equiv 1 \bmod l\}$ of $\mathrm{GL}(n, \mathbb{Z}_l)$ is an open pro-l group [DSM, p. 87]. Hence, $\Gamma_1 \cap G$ is an open pro-l subgroup of G.

(c) Let L be an open pro-l subgroup of G. Replace L, if necessary, by the intersection of its conjugates, to assume that L is normal in G. By (a), L is finitely generated. Hence, by [FrJ, Lemma 20.36], $\Phi(L)$ is an open subgroup of L. Since $\Phi(L) \subseteq \Phi(G)$ [FrJ, Lemma 20.4(c)], $\Phi(G)$ is open in G. ∎

LEMMA 2.4. *Let K_0 be a countable separably Hilbertian field. Suppose every finite extension of K_0 satisfies Condition* (C′). *Then every function field of one variable over K_0 satisfies* (C′).

Proof. Consider a function field of one variable K over K_0, an abelian variety A over K, and a prime number l. We have to prove that $A_{l^\infty}(\widetilde{K}(\sigma))$ is finite for almost all $\sigma \in G(K)$.

Use Remark 2.1(a) to replace K_0 by $K_{0,\mathrm{ins}}$ and K by $K \cdot K_{0,\mathrm{ins}}$, if necessary, to assume that K_0 is perfect. Let N, L, and K' be as in the proof of Proposition 2.2. Then $\mathcal{G}(L/K) \cong \mathcal{G}(N/L')$ is isomorphic to a closed subgroup of $\mathrm{GL}(r, \mathbb{Z}_l)$ for some nonnegative integer r. As such, the Frattini subgroup of $\mathcal{G}(L/K)$ is open (Lemma 2.3). Let K_1 be the fixed field of $\Phi(\mathcal{G}(L/K))$ in L. Then K_1 is a finite Galois extension of K. Choose a separating transcendental element t for K/K_0. Then $K_1/K_0(t)$ is a finite separable extension. Choose a primitive element z for $K_1/K_0(t)$ and let $f(t, X) = \mathrm{irr}(z, K_0(t)) \in K_0(t)[X]$. As K_0 is separably Hilbertian, there exists $a \in K_0$ such that $f(a, X) \in K_0[X]$ is irreducible. Choose a prime divisor $\mathfrak{p}$ of K/K_0 such that $t(\mathfrak{p}) = a$. Using Lemma 1.1 and Corollary 1.2 and possibly avoiding finitely many elements of K_0, we may assume that a also satisfies the following conditions:

(4a) $\overline{K}_1/\overline{K}$ is a Galois extension and $[\overline{K}_1 : \overline{K}] = [K_1 : K]$;

(4b) A has a good reduction at $\mathfrak{p}$;

(4c) reduction modulo $\mathfrak{p}$ gives a bijection $A_{l^\infty}(\widetilde{K}) \to \overline{A}_{l^\infty}(\widetilde{K}_0)$; and

(4d) $\mathfrak{p}$ is unramified in L.

Extend $\mathfrak{p}$ in the unique possible way to a prime divisor $\mathfrak{p}'$ of K'. Then $\mathfrak{p}'$ is unramified in N. Let $K_1' = K_1 K'$. Since K_0 is perfect, $\overline{K}' = \overline{K}$ and $\overline{K_1'} = \overline{K}_1$. Extend $\mathfrak{p}'$ to a prime divisor $\mathfrak{p}_1'$ of K_1' and extend $\mathfrak{p}_1'$ to a prime divisor $\mathfrak{P}$ of N. Then $\mathcal{G}(\overline{N}/\overline{K})$ is isomorphic to the decomposition group $D(\mathfrak{P}/\mathfrak{p}')$. The latter is a subgroup of $\mathcal{G}(N/K')$. By (4a), $\mathrm{res}_{K_1'} D(\mathfrak{P}/\mathfrak{p}') = D(\mathfrak{p}_1'/\mathfrak{p}') \cong \mathcal{G}(\overline{K}_1/\overline{K}) \cong \mathcal{G}(K_1'/K')$. Hence, $\mathrm{res}_{K_1'} D(\mathfrak{P}/\mathfrak{p}') = \mathcal{G}(K_1'/K')$. Since $\mathrm{res}_{K_1'} : \mathcal{G}(N/K') \to \mathcal{G}(K_1'/K')$ is a Frattini cover [FrJ, p. 299], this

implies that $D(\mathfrak{P}/\mathfrak{p}') \cong \mathcal{G}(N/K')$. Thus, by (4c), reduction modulo $\mathfrak{p}$ gives an isomorphism of modules: $(\mathcal{G}(N/K'), A_{l^\infty}(\widetilde{K})) \cong (\mathcal{G}(\overline{N}/\overline{K}), \overline{A}_{l^\infty}(\widetilde{K}_0))$. By assumption, almost all $\sigma \in \mathcal{G}(\overline{N}/\overline{K})$ fix only finitely many points in $\overline{A}_{l^\infty}(\widetilde{K}_0)$. We conclude from (4c) that almost all $\sigma \in \mathcal{G}(N/K')$ fix only finitely many points of $A_{l^\infty}(\widetilde{K})$. ∎

PROPOSITION 2.5. *Condition* (C′) *holds for every finitely generated field* K.

Proof. We proceed by induction on the *absolute transcendence degree* $r(K)$ of K. That is, $r(K) = \text{trans.deg}(K/\mathbb{F}_p)$ if $\text{char}(K) = p > 0$ and $r(K) = \text{trans.deg}(K/\mathbb{Q}) + 1$ if $\text{char}(K) = 0$.

If $r(K) = 0$, then K is finite and (C′) is taken care of by [JaJ1, Prop. 4.2]. If $r(K) = 1$, then K is a global field. Proposition 2.2 proves (C′) in this case.

Let therefore $r \geq 2$. Suppose (C′) is true for all finitely generated fields with absolute transcendence degree $r - 1$. Consider a finitely generated field K with $r(K) = r$. Then K is a function field of one variable over a Hilbertian field K_0 [FrJ, Corollary 12.8 and Theorem 12.10]. Since $r(K_0) = r(K) - 1$, (C′) holds for K_0. Hence, by Lemma 2.4, (C′) holds for K. ∎

Since there are only countably many l, it is possible to switch quantifiers in Proposition 2.5.

LEMMA 2.6. *Let* K *be a countable field and* e *a positive integer. Suppose every finite extension of* K *satisfies Condition* (C′). *Then, for almost all* $\boldsymbol{\sigma} \in G(K)^e$, *for every abelian variety* A *over* $\widetilde{K}(\boldsymbol{\sigma})$, *and for each* l *the group* $A_{l^\infty}(\widetilde{K}(\boldsymbol{\sigma}))$ *is finite.*

Proof. The proof naturally breaks up into two parts.

PART A: *Condition* (C′) *for an arbitrary* e. Let A be an abelian variety over K and let l be a prime number. If $\sigma_1, \ldots, \sigma_e \in G(K)$, then $A_{l^\infty}(\widetilde{K}(\sigma_1, \ldots, \sigma_e)) \subseteq A_{l^\infty}(\widetilde{K}(\sigma_1))$. Hence,

$$\{\sigma_1 \in G(K) \mid A_{l^\infty}(\widetilde{K}(\sigma_1)) \text{ is finite}\} \times G(K)^{e-1}$$
$$\subseteq \{\boldsymbol{\sigma} \in G(K)^e \mid A_{l^\infty}(\widetilde{K}(\boldsymbol{\sigma})) \text{ is finite}\}.$$

By assumption, the left hand side has measure 1. Hence, so does the right hand side.

PART B: *Switch of quantifiers.* Let L be a finite extension of K, A an abelian variety over L, and l a prime number. Define

$$S(L, A, l) = \{\boldsymbol{\sigma} \in G(L)^e \mid A_{l^\infty}(\widetilde{K}(\boldsymbol{\sigma})) \text{ is finite}\}.$$

By Part (A) applied to L instead of to K, $S(L, A, l)$ has measure 1 in $G(L)^e$.

Hence, since there are only countably many triples (L, A, l), the set

$$S = G(K)^e \smallsetminus \bigcup_{L,A,l} [G(L)^e \smallsetminus S(L, A, l)]$$

has measure 1 in $G(K)^e$. If $\boldsymbol{\sigma} \in S$, A is an abelian variety over $\widetilde{K}(\boldsymbol{\sigma})$, and l is a prime number, then A is already defined over a finite extension L of K which is contained in $\widetilde{K}(\boldsymbol{\sigma})$. Then $\boldsymbol{\sigma} \in S(L, A, l)$ and therefore $A_{l^\infty}(\widetilde{K}(\boldsymbol{\sigma}))$ is finite, as desired. ∎

The combination of Proposition 2.5 and Lemma 2.6 proves a stronger version of Part (C) of the Geyer–Jarden Conjecture:

THEOREM 2.7. *Let K be a field which is finitely generated over its prime field. Let e be a positive integer. Then, for almost all $\boldsymbol{\sigma} \in G(K)^e$, for every abelian variety A over $\widetilde{K}(\boldsymbol{\sigma})$, and for every prime number l the group $A_{l^\infty}(\widetilde{K}(\boldsymbol{\sigma}))$ is finite.*

3. Homotheties. In this section we give an alternative proof to Part (C) of the Geyer–Jarden Conjecture in characteristic 0. This proof is based on a theorem of Bogomolov–Serre. The same theorem is also the main ingredient in the proof of Part (B) of the conjecture in characteristic 0.

Consider a subgroup G of $\mathrm{GL}(n, \mathbb{F}_l)$ or a closed subgroup G of $\mathrm{GL}(n, \mathbb{Z}_l)$. We identify each η in $\mathbb{F}_l^\times$ (resp. $\mathbb{Z}_l^\times$) with the corresponding scalar matrix of $\mathrm{GL}(n, \mathbb{F}_l)$ (resp. $\mathrm{GL}(n, \mathbb{Z}_l)$) and call it a *homothety*. This makes $\mathbb{F}_l^\times$ (resp. $\mathbb{Z}_l^\times$) a subgroup of $\mathrm{GL}(n, \mathbb{F}_l)$ (resp. $\mathrm{GL}(n, \mathbb{Z}_l)$). Our main observation is that if G contains a big chunk of the group of homotheties, then the probability that an element of G has eigenvalue 1 is small. Lemmas 3.1 and 3.2 below make this statement precise.

LEMMA 3.1. *Let G be a subgroup of $\mathrm{GL}(n, \mathbb{F}_l)$, and let*

$$E = \{g \in G \mid 1 \text{ is an eigenvalue of } g\}.$$

Suppose that $(\mathbb{F}_l^\times : \mathbb{F}_l^\times \cap G) \le c$. Then $|E| \le \frac{nc}{l-1}|G|$.

Proof. Let $H = \mathbb{F}_l^\times \cap G$. Consider the surjective map $f : H \times E \to HE$ given by $f(\eta, e) = \eta e$. For each $g \in HE$ list the elements of $f^{-1}(g)$ as $(\eta_1, e_1), \ldots, (\eta_m, e_m)$. Then $\eta_i e_i = g$, $i = 1, \ldots, m$, the η_i are distinct and each of them is an eigenvalue of g. Since an element of $\mathrm{GL}(n, \mathbb{F}_l)$ may have at most n eigenvalues, $m \le n$.

It follows that $|H| \cdot |E| \le n \cdot |HE|$. Since $HE \subseteq G$, this implies that

$$|E| \le \frac{n}{|H|}|G| = \frac{n}{l-1}(\mathbb{F}_l^\times : H)|G| \le \frac{nc}{l-1}|G|,$$

as contended. ∎

We denote the normalized Haar measure of a profinite group G by μ_G. In particular $\mu_G(G) = 1$.

LEMMA 3.2. *Let G be a closed subgroup of $\mathrm{GL}(n, \mathbb{Z}_l)$ and let*

$$E = \{g \in G \mid 1 \text{ is an eigenvalue of } g\}.$$

Suppose the group $H = \mathbb{Z}_l^\times \cap G$ of all homotheties in G is infinite. Then $\mu_G(E) = 0$.

Proof. We prove that for each positive integer r and for all r-tuples $\eta_1, \ldots, \eta_r$ of distinct elements of H the measure of $\eta_1 E \cap \ldots \cap \eta_r E$ is 0. The case $r = 1$ and $\eta_1 = 1$ will prove that $\mu_G(E) = 0$.

Indeed, if $r \geq n + 1$ and $\eta_1, \ldots, \eta_r$ are distinct elements of H, then $\eta_1, \ldots, \eta_r$ are distinct eigenvalues of each element of $\eta_1 E \cap \ldots \cap \eta_r E$. Since an element of G has at most n eigenvalues, this implies that $\eta_1 E \cap \ldots \cap \eta_r E$ is empty. In particular its measure is 0.

Suppose now that the above statement is true for $r \geq 2$. We prove it for $r - 1$. To this end consider $r - 1$ distinct elements $\eta_1, \ldots, \eta_{r-1}$ of H and let $D = \eta_1 E \cap \ldots \cap \eta_{r-1} E$. Since H is infinite, it has a subsequence $\zeta_1, \zeta_2, \ldots$ such that $\zeta_k \neq \zeta_j \eta_1 / \eta_i$ for $k = 1, 2, \ldots$, $i = 1, \ldots, r-1$, and $j = 1, \ldots, k-1$. It follows for $k > j$ that $\zeta_j \eta_1, \zeta_k \eta_1, \zeta_k \eta_2, \ldots, \zeta_k \eta_{r-1}$ are r distinct elements of H. Hence, $\mu_G(\zeta_j \eta_1 E \cap \zeta_k \eta_1 E \cap \zeta_k \eta_2 E \cap \ldots \cap \zeta_k \eta_{r-1} E) = 0$. The inclusion

$$\zeta_j D \cap \zeta_k D \subseteq \zeta_j \eta_1 E \cap \zeta_k \eta_1 E \cap \zeta_k \eta_2 E \cap \ldots \cap \zeta_k \eta_{r-1} E$$

then implies that $\mu_G(\zeta_j D \cap \zeta_k D) = 0$. Hence,

$$1 \geq \mu_G \Big(\bigcup_{j=1}^\infty \zeta_j D \Big) = \sum_{j=1}^\infty \mu_G(\zeta_j D) = \sum_{j=1}^\infty \mu_G(D).$$

We conclude that $\mu_G(D) = 0$, as contended. ∎

Consider now an abelian variety A of dimension d over a field K. Let $l \neq \mathrm{char}(K)$ be a prime number. The action of $G(K)$ on the $A_l(\widetilde{K})$ (resp. $T_l(A)$) defines (after choosing appropriate bases) representations $\varrho_{A,l} : G(K) \to \mathrm{GL}(2d, \mathbb{F}_l)$ (resp. $\varrho_{A,l^\infty} : G(K) \to \mathrm{GL}(2d, \mathbb{Z}_l)$) such that $\varrho_{A,l} = \pi_l \circ \varrho_{A,l^\infty}$, where $\pi_l : \mathrm{GL}(2d, \mathbb{Z}_l) \to \mathrm{GL}(2d, \mathbb{F}_l)$ is reduction modulo l. Let $G_l = \varrho_{A,l}(G(K))$ and $G_{l^\infty} = \varrho_{A,l^\infty}(G(K))$. Then $G_l = \pi_l(G_{l^\infty})$. So, $\mathbb{F}_l^\times \cap G_l \supseteq \pi_l(\mathbb{Z}_l^\times \cap G_{l^\infty})$. It follows that

$$(1) \qquad (\mathbb{F}_l^\times : \mathbb{F}_l^\times \cap G_l) \leq (\mathbb{Z}_l^\times : \mathbb{Z}_l^\times \cap G_{l^\infty}).$$

THE HOMOTHETY CONDITION ON A FIELD K. For every abelian variety A over K there exists a constant c such that for all l

$$(2a) \qquad (\mathbb{Z}_l^\times : \mathbb{Z}_l^\times \cap G_{l^\infty}) \leq c.$$

Hence, by (1),

(2b) $$(\mathbb{F}_l^\times : \mathbb{F}_l^\times \cap G_l) \le c. \quad \blacksquare$$

PROPOSITION 3.3. *Let K be a countable field which satisfies the homothety condition. Then the following statements hold for every abelian variety A over K:*

(a) $A_{l^\infty}(\widetilde{K}(\sigma))$ *is finite for each $l \ne \mathrm{char}(K)$ and for almost all $\sigma \in G(K)$.*

(b) *If $e \ge 2$, then for almost all $\boldsymbol{\sigma} \in G(K)^e$ the set $\bigcup_l A_l(\widetilde{K}(\boldsymbol{\sigma}))$ is finite.*

Proof. Let A be an abelian variety over K of dimension d.

(a) By the homothety condition, $\mathbb{Z}_l^\times \cap G_{l^\infty}$ is an infinite group. Hence, by Lemma 3.2, the set $E_{l^\infty} = \{g \in G_{l^\infty} \mid 1 \text{ is an eigenvalue of } g\}$ has measure 0 in G_{l^∞}. Let $\sigma \in G(K)$. Then $\varrho_{A,l^\infty}(\sigma) \in E_{l^\infty}$ if and only if there exists $\mathbf{p} \in T_l(A)$ such that $\mathbf{p} \ne 0$ and $\sigma\mathbf{p} = \mathbf{p}$. Hence, by Remark 2.1(c), the set of all $\sigma \in G(K)$ such that $A_{l^\infty}(K_{\mathrm{s}}(\sigma))$ is infinite is $\varrho_{A,l^\infty}^{-1}(E_{l^\infty})$. So, it is of measure 0. We conclude that for almost all $\sigma \in G(K)$ the group $A_{l^\infty}(K_{\mathrm{s}}(\sigma))$ is finite. Since $l \ne \mathrm{char}(K)$, $A_{l^\infty}(\widetilde{K}(\sigma))$ coincides with $A_{l^\infty}(K_{\mathrm{s}}(\sigma))$ (Remark 2.1(b)). So, it is finite.

(b) Suppose now $e \ge 2$. Let

$$E_l = \{g \in G_l \mid 1 \text{ is an eigenvalue of } g\},$$

$$S_{e,l} = \{\boldsymbol{\sigma} \in G(K)^e \mid \exists \mathbf{a} \in A_l(K_{\mathrm{s}}(\boldsymbol{\sigma})) : \mathbf{a} \ne 0 \text{ and } \sigma_i\mathbf{a} = \mathbf{a}, \ i = 1, \dots, e\}.$$

Then $S_{e,l} \subseteq \varrho_{A,l}^{-1}(E_l)^e$. By (2b), $(\mathbb{F}_l^\times : \mathbb{F}_l^\times \cap G_l) \le c$ and therefore, by Lemma 3.1, $|E_l| \le \frac{2dc}{l-1}|G_l|$ for all $l \ne \mathrm{char}(K)$. Hence

$$\mu_{G(K)}(S_{e,l}) \le \mu_{G_l}(E_l)^e \le \left(\frac{2dc}{l-1}\right)^e.$$

Since $e \ge 2$,

$$\sum_l \mu_{G(K)}(S_{e,l}) \le \sum_l \frac{(2dc)^e}{(l-1)^e} < \infty.$$

Hence, by Borel–Cantelli [FrJ, Lemma 16.7], almost all $\boldsymbol{\sigma} \in G(K)^e$ belong to only finitely many $S_{e,l}$. Thus, for almost all $\boldsymbol{\sigma} \in G(K)^e$ the set $\bigcup_l A_l(K_{\mathrm{s}}(\boldsymbol{\sigma}))$ is finite. We conclude from Remark 2.1(b) that $\bigcup_l A_l(\widetilde{K}(\boldsymbol{\sigma}))$ is finite. $\quad \blacksquare$

LEMMA 3.4. *Suppose every finite extension of a field K_0 satisfies the homothety condition. Then so does every finitely generated extension of K_0.*

Proof. Induction on the transcendence degree shows it suffices to consider a finitely generated extension K of K_0 of transcendence degree 1 and an abelian variety A over K, and to find $c > 0$ such that we have $(\mathbb{Z}_l^\times : \mathbb{Z}_l^\times \cap \varrho_{A,l^\infty}(G(K))) \le c$ for all primes l.

Indeed, replace K_0 by its relative algebraic closure in K, if necessary, to assume that K_0 is algebraically closed in K. Choose a prime divisor $\mathfrak{p}$ of K/K_0 at which A has good reduction. (This holds for almost all $\mathfrak{p}$.) Then, for each $l \neq \mathrm{char}(K_0)$, the inertia groups over $\mathfrak{p}$ in $K(A_{l\infty})$ are trivial [SeT, Thm. 1(b)]. Hence, the reduction map $A_{l\infty}(\widetilde{K}) \to \overline{A}_{l\infty}(\widetilde{K}_0)$ is bijective and $\varrho_{\overline{A},l\infty}(G(\overline{K})) \cong \mathcal{G}(\overline{K}(\overline{A}_{l\infty})/\overline{K})$ embeds into $\varrho_{A,l\infty}(G(K)) \cong \mathcal{G}(K(A_{l\infty})/K)$. Hence $\mathbb{Z}_l^\times \cap \varrho_{\overline{A},l\infty}(G(\overline{K})) \subseteq \mathbb{Z}_l^\times \cap \varrho_{A,l\infty}(G(K))$. Since $\overline{K}$ is a finite extension of K_0, there exists $c > 0$ independent of l with $(\mathbb{Z}_l^\times : \mathbb{Z}_l^\times \cap \varrho_{\overline{A},l\infty}(G(\overline{K}))) \leq c$ (the homothety condition). It follows that $(\mathbb{Z}_l^\times : \mathbb{Z}_l^\times \cap \varrho_{A,l\infty}(G(K))) \leq c$ for all $l \neq \mathrm{char}(K)$. ∎

CONDITION (B′) ON A FIELD K. Let $e \geq 2$ be an integer and A an abelian variety over K. Then $\bigcup_l A_l(K_\mathrm{s}(\boldsymbol{\sigma}))$ is finite for almost all $\boldsymbol{\sigma} \in G(K)^e$. ∎

LEMMA 3.5. *Let K be a countable field and $e \geq 2$. Suppose every finite extension of K satisfies Condition* (B′). *Then for almost all $\boldsymbol{\sigma} \in G(K)^e$ and for each abelian variety A over $\widetilde{K}(\boldsymbol{\sigma})$ the set $\bigcup_l A_l(\widetilde{K}(\boldsymbol{\sigma}))$ is finite.*

Proof. Let L be a finite extension of K and A an abelian variety over L. Consider the set

$$S(L, A) = \left\{\boldsymbol{\sigma} \in G(L)^e \,\middle|\, \bigcup_l A_l(\widetilde{L}(\boldsymbol{\sigma})) \text{ is finite}\right\}.$$

By (B′) and Remark 2.1(b), $S(L, A)$ has measure 1 in $G(L)^e$. Hence, since there are only countably many pairs (L, A), the set

$$S = G(K)^e \smallsetminus \bigcup_{L,A}[G(L)^e \smallsetminus S(L, A)]$$

has measure 1 in $G(K)^e$. Here we have identified $G(L)$ with $G(K_\mathrm{s} \cap L)$ and $S(L, A)$ with its restriction to K_s. If $\boldsymbol{\sigma} \in S$ and if A is an abelian variety over $\widetilde{K}(\boldsymbol{\sigma})$, then A is already defined over a finite extension L of K which is contained in $\widetilde{K}(\boldsymbol{\sigma})$. Then $\boldsymbol{\sigma} \in S(L, A)$ and therefore $\bigcup_l A_l(\widetilde{L}(\boldsymbol{\sigma}))$ is finite. But $\widetilde{L}(\boldsymbol{\sigma}) = \widetilde{K}(\boldsymbol{\sigma})$. We conclude that $\bigcup_l A_l(\widetilde{K}(\boldsymbol{\sigma}))$ is finite. ∎

LEMMA 3.6. *Let B be an abelian group. For each positive integer n let $B_n = \{b \in B \mid nb = 0\}$. Suppose $\bigcup_l B_l$ is a finite set and $B_{l\infty} = \bigcup_{i=1}^\infty B_{l^i}$ is a finite group for each l. Then B_tor is finite.*

Proof. By assumption, there exists l_0 with $B_l = 0$ for all $l \geq l_0$. Hence, $B_{l^i} = 0$ for all $l \geq l_0$ and all i. So, $B_\mathrm{tor} = \bigoplus_{l < l_0} B_{l\infty}$ is finite. ∎

We are now ready to prove our second main result.

THEOREM 3.7. *Let K be a finitely generated extension of $\mathbb{Q}$ and e a positive integer. Then the following statements hold for almost all $\boldsymbol{\sigma} \in G(K)^e$*

and for each abelian variety A over $\widetilde{K}(\boldsymbol{\sigma})$:

(a) *The group $A_{l^\infty}(\widetilde{K}(\boldsymbol{\sigma}))$ is finite for each prime number l.*
(b) *If $e \geq 2$, then $A_{\mathrm{tor}}(\widetilde{K}(\boldsymbol{\sigma}))$ is finite.*

Proof. A theorem of Bogomolov–Serre [Ser1, Thm. 2, or Ser4, p. 92, Thm. 2] confirms the homothety condition for number fields. Hence, by Lemma 3.4, the homothety condition holds for every finitely generated extension K of $\mathbb{Q}$. So, by Proposition 3.3, every finitely generated extension K of $\mathbb{Q}$ satisfies Conditions (B′) and (C′). It follows from Lemmas 3.5 and 2.6 that for almost all $\boldsymbol{\sigma} \in G(K)^e$ and for every abelian variety A over $\widetilde{K}(\boldsymbol{\sigma})$ the following statements are true:

(3a)   For each l the group $A_{l^\infty}(\widetilde{K}(\boldsymbol{\sigma}))$ is finite.
(3a)   If $e \geq 2$, then $\bigcup_l A_l(\widetilde{K}(\boldsymbol{\sigma}))$ is finite.

We conclude from Lemma 3.6 that if $e \geq 2$, then $A_{\mathrm{tor}}(\widetilde{K}(\boldsymbol{\sigma}))$ is finite. ∎

REMARK 3.8. *The Geyer–Jarden Conjecture implies the Corollary to the Geyer–Jarden Conjecture.* Let K be a finitely generated field and e a positive integer. The Conjecture implies Condition (C′) for each finite extension L of K. Hence, by Lemma 2.6,

(4)   for almost all $\boldsymbol{\sigma} \in G(K)^e$, for every abelian variety A over $\widetilde{K}(\boldsymbol{\sigma})$ and for each l the group $A_{l^\infty}(\widetilde{K}(\boldsymbol{\sigma}))$ is finite.

For $e \geq 2$ the Conjecture implies Condition (B′) for every finite extension L of K. Hence, by Lemma 3.5,

(5)   for almost all $\boldsymbol{\sigma} \in G(K)^e$ and for every abelian variety A over $\widetilde{K}(\boldsymbol{\sigma})$ the set $\bigcup_l A_l(\widetilde{K}(\boldsymbol{\sigma}))$ is finite.

We conclude from (4), (5), and Lemma 3.6 that for $e \geq 2$, for almost all $\boldsymbol{\sigma} \in G(K)^e$ and for every abelian variety A over $\widetilde{K}(\boldsymbol{\sigma})$ the group $A_{\mathrm{tor}}(\widetilde{K}(\boldsymbol{\sigma}))$ is finite. This is (II) of the Corollary to the Geyer–Jarden Conjecture.

Next we prove (I) of the Corollary. For each finite extension L of K and each abelian variety A over L the Conjecture and Remark 3.3 imply that $T(L, A) = \{\sigma \in G(L) \mid \bigcup_l A_l(\widetilde{L}(\sigma))$ is infinite$\}$ has measure 1 in $G(L)$. Hence

$$T = G(K) \smallsetminus \bigcup_{L,A} [G(L) \smallsetminus T(L, A)]$$

has measure 1 in $G(K)$. For each $\sigma \in T$ and each abelian variety A over $\widetilde{K}(\sigma)$ the set $\bigcup_l A_l(\widetilde{K}(\sigma))$ is infinite. Hence, $A_{\mathrm{tor}}(\widetilde{K}(\sigma))$ is infinite, as desired. ∎

4. Appendix: Generalization of the Chebotarev density theorem. We solve a special case of an exercise that appears on page I-8

of [Ser2]. In this exercise we consider an l-adically closed subgroup G of $\mathrm{GL}(n, \mathbb{Z}_l)$ and a Zariski-closed subset V of M_n which is defined over $\mathbb{Q}_l$. Here M_n is the variety of all $n \times n$ matrices. The group G is compact and has a normalized Haar measure μ. Let $\partial(V(\mathbb{Z}_l) \cap G)$ be the boundary of $V(\mathbb{Z}_l) \cap G$. We prove that $\mu(\partial(V(\mathbb{Z}_l) \cap G)) = 0$.

LEMMA 4.1. *Let W be a Zariski-closed subset of M_n which is defined over $\mathbb{Q}_l$. Suppose that for each $n \in \mathbb{N}$ and for all $\mathbf{g}_1, \ldots, \mathbf{g}_n, \mathbf{h}_1, \ldots, \mathbf{h}_n \in G$,*

$$(1) \qquad\qquad G \neq \bigcup_{i=1}^{n} \mathbf{g}_i (W(\mathbb{Z}_l) \cap G) \mathbf{h}_i.$$

Then

$$(2) \qquad\qquad \mu(W(\mathbb{Z}_l) \cap G) = 0.$$

Proof. We prove the lemma by induction on $\dim(W)$. Note that the assumption of the lemma holds for each Zariski-closed subset of W which is defined over $\mathbb{Q}_l$. If (2) holds for each $\mathbb{Q}_l$-irreducible component of W, then it also holds for W. We may therefore assume W is $\mathbb{Q}_l$-irreducible.

If $W(\mathbb{Z}_l) \cap G$ is empty, then (2) is certainly true. Otherwise we choose $\mathbf{w} \in W(\mathbb{Z}_l) \cap G$. Then we choose by induction $\mathbf{p}_i \in G$, $i = 1, 2, \ldots$, with $\mathbf{p}_i W \neq \mathbf{p}_j W$ if $i < j$. Indeed, suppose that we have already chosen $\mathbf{p}_1, \ldots, \mathbf{p}_n$. By (1), we may choose $\mathbf{p}_{n+1} \in G \smallsetminus \bigcup_{i=1}^{n} \mathbf{p}_i (W(\mathbb{Z}_l) \cap G) \mathbf{w}^{-1}$. In particular for each i, there exists no $\mathbf{w}' \in W(\mathbb{Z}_l) \cap G$ with $\mathbf{p}_{n+1} \mathbf{w} = \mathbf{p}_i \mathbf{w}'$. So, $\mathbf{p}_i W \neq \mathbf{p}_{n+1} W$ for $i = 1, \ldots, n$.

Let $i < j$. If $\mathbf{g}_1, \ldots, \mathbf{g}_r, \mathbf{h}_1, \ldots, \mathbf{h}_r$ are points in G, then

$$(3) \qquad \bigcup_{k=1}^{r} \mathbf{g}_k ((\mathbf{p}_i W \cap \mathbf{p}_j W)(\mathbb{Z}_l) \cap G) \mathbf{h}_k \subseteq \bigcup_{k=1}^{r} \mathbf{g}_k \mathbf{p}_i (W(\mathbb{Z}_l) \cap G) \mathbf{h}_k.$$

Hence, by (1), G is not equal to the left hand side of (3). Since W is $\mathbb{Q}_l$-irreducible, so is $\mathbf{p}_i W$. Hence, by the dimension theorem, $\dim(\mathbf{p}_i W \cap \mathbf{p}_j W) < \dim(W)$. By the induction hypothesis,

$$\mu((\mathbf{p}_i W \cap \mathbf{p}_j W)(\mathbb{Z}_l) \cap G) = 0.$$

Hence,

$$\mu(\mathbf{p}_i (W(\mathbb{Z}_l) \cap G) \cap \mathbf{p}_j (W(\mathbb{Z}_l) \cap G)) = 0.$$

If $\mu(W(\mathbb{Z}_l) \cap G) > 0$, then

$$\mu\Big(\bigcup_{i=1}^{\infty} \mathbf{p}_i (W(\mathbb{Z}_l) \cap G) \Big) = \infty,$$

which is false. We conclude that (2) is true. ∎

PROPOSITION 4.2. *The boundary of $V(\mathbb{Z}_l) \cap G$ has measure 0 in G.*

Proof. We prove the proposition by induction on $\dim(V)$. By the decomposition-intersection procedure [FrJ, §19.1] there exist absolutely irreducible subvarieties $V_1, \ldots, V_m$ of V which are defined over $\mathbb{Q}_l$ with $V(\mathbb{Q}_l) = \bigcup_{i=1}^m V_i(\mathbb{Q}_l)$. We may therefore assume V is absolutely irreducible.

Let V_{simp} (resp. V_{sing}) be the Zariski-open (resp. Zariski-closed) subset of V of all simple (resp. singular) points. By the density theorem [GeJ, Prop. 8.2], each $\mathbf{p} \in V_{\mathrm{simp}}(\mathbb{Z}_l) \cap G$ has an open l-adic neighborhood $\mathcal{U}$ in $V_{\mathrm{simp}}(\mathbb{Z}_l)$. Hence, $\mathcal{U} \cap G$ is an open l-adic neighborhood of $\mathbf{p}$ in $V(\mathbb{Z}_l) \cap G$. It follows that

$$(4) \qquad \partial(V(\mathbb{Z}_l) \cap G) \subseteq V_{\mathrm{sing}}(\mathbb{Z}_l) \cap G.$$

Denote V_{sing} by W and observe that $\dim(W) < \dim(V)$.

Suppose first that there exist $\mathbf{g}_1, \ldots, \mathbf{g}_n, \mathbf{h}_1, \ldots, \mathbf{h}_n \in G$ such that

$$(5) \qquad G = \bigcup_{i=1}^n \mathbf{g}_i(W(\mathbb{Z}_l) \cap G)\mathbf{h}_i.$$

Then

$$(6) \qquad V(\mathbb{Z}_l) \cap G = \Big(\bigcup_{i=1}^n V \cap \mathbf{g}_i W \mathbf{h}_i \Big)(\mathbb{Z}_l) \cap G.$$

Since $\dim(\bigcup_{i=1}^n V \cap \mathbf{g}_i W \mathbf{h}_i) < \dim(V)$, an induction hypothesis implies that the boundary of the right hand side of (6) has measure 0 in G. Hence, $\mu(\partial(V(\mathbb{Z}_l) \cap G)) = 0$.

If there exist no $\mathbf{g}_1, \ldots, \mathbf{g}_n, \mathbf{h}_1, \ldots, \mathbf{h}_n \in G$ such that (5) holds, then by Lemma 4.1, $\mu(W(\mathbb{Z}_l) \cap G) = 0$. Hence, by (4), $\mu(\partial(V(\mathbb{Z}_l) \cap G)) = 0$.

So, $\mu(\partial(V(\mathbb{Z}_l) \cap G))$ is 0 in each case. ∎

Let $\mathcal{C}$ be a subset of a group G. We call $\mathcal{C}$ a *conjugation domain* of G if $\mathcal{C}^g = \mathcal{C}$ for each $g \in G$.

The conclusion of Proposition 4.2 enters sometimes as an assumption of the following result.

PROPOSITION 4.3 (The Chebotarev density theorem for infinite extensions). *Let N be a Galois extension of a global field K, $G = \mathcal{G}(N/K)$, and μ the normalized Haar measure of G. Suppose almost all prime divisors of K are unramified in N. Denote by P the set of all nonarchimedean prime divisors of K which are unramified in N. Let δ be the Dirichlet density function on P. Consider a conjugacy domain $\mathcal{C}$ of G whose boundary has measure 0 in G. Let $C = \left\{ \mathfrak{p} \in P \mid \left(\frac{N/K}{\mathfrak{p}} \right) \subseteq \mathcal{C} \right\}$. Then $\delta(C) = \mu(\mathcal{C})$.*

Proof. Let $\overline{\mathcal{C}}$ (resp. $\mathcal{C}^0$) be the closure (resp. interior) of $\mathcal{C}$. Then both $\overline{\mathcal{C}}$ and $\mathcal{C}^0$ are measurable sets, $\mathcal{C}^0 \subseteq \mathcal{C} \subseteq \overline{\mathcal{C}}$, and

$$(7) \qquad \partial(\mathcal{C}) = \overline{\mathcal{C}} \smallsetminus \mathcal{C}^0.$$

Hence, $\mathcal{C}$ is measurable and $\mu(\mathcal{C}^0) = \mu(\mathcal{C}) = \mu(\overline{\mathcal{C}})$.

Choose a sequence $L_1 \subseteq L_2 \subseteq \ldots$ of finite Galois extensions of K such that $\bigcup_{i=1}^{\infty} L_i = N$. For each i let $\mathcal{C}_i = \operatorname{Res}_{L_i}^{-1}(\operatorname{Res}_{L_i} \mathcal{C})$ and

$$C_i = \left\{ \mathfrak{p} \in P \,\middle|\, \left(\frac{L_i/K}{\mathfrak{p}} \right) \subseteq \operatorname{Res}_{L_i} \mathcal{C} \right\}.$$

Then $\operatorname{Res}_{L_i}(\mathcal{C})$ is a conjugacy domain in $\mathcal{G}(L_i/K)$, $\mathcal{C} \subseteq \mathcal{C}_i$, and $C \subseteq C_i$. By the Chebotarev density theorem for finite Galois extensions [FrJ, Thm. 5.6],

$$(8) \qquad \delta(C_i) = \frac{|\operatorname{Res}_{L_i}(\mathcal{C})|}{[L_i : K]} = \mu(\mathcal{C}_i).$$

Since $\mathcal{C}_i$ is closed (and open), we have $\mathcal{C} \subseteq \overline{\mathcal{C}} \subseteq \ldots \subseteq \mathcal{C}_3 \subseteq \mathcal{C}_2 \subseteq \mathcal{C}_1$ and $\overline{\mathcal{C}} = \bigcap_{i=1}^{\infty} \mathcal{C}_i$. Hence, by (8) and (7),

$$(9) \qquad \lim_{i \to \infty} \delta(C_i) = \mu(\mathcal{C}).$$

Next let $\mathcal{D} = G \smallsetminus \mathcal{C}$ and $D = \left\{ \mathfrak{p} \in P \,\middle|\, \left(\frac{N/K}{\mathfrak{p}} \right) \subseteq \mathcal{D} \right\}$. Then $D = P \smallsetminus C$. Observe that $\overline{\mathcal{D}} = G \smallsetminus \mathcal{C}^0$ and $\mathcal{D}^0 = G \smallsetminus \overline{\mathcal{C}}$. Hence, $\mu(\mathcal{D}^0) = \mu(\mathcal{D}) = \mu(\overline{\mathcal{D}})$. For each i let $\mathcal{D}_i = \operatorname{Res}_{L_i}^{-1}(\operatorname{Res}_{L_i} \mathcal{D})$ and $D_i = \left\{ \mathfrak{p} \in P \,\middle|\, \left(\frac{L_i/K}{\mathfrak{p}} \right) \subseteq \operatorname{Res}_{L_i} \mathcal{D} \right\}$. Replace $\mathcal{C}$ by $\mathcal{D}$ and C by D in the arguments above to conclude that $D \subseteq D_i$ and $\mu(\mathcal{D}) = \lim_{i \to \infty} \delta(D_i)$. Thus,

$$(10) \qquad P \smallsetminus D_i \subseteq C \quad \text{and} \quad \mu(\mathcal{C}) = \lim_{i \to \infty} \delta(P \smallsetminus D_i).$$

It follows from (9) and (10) that for every $\varepsilon > 0$ there is i_0 such that for all $i \geq i_0$ we have

$$P \smallsetminus D_i \subseteq C \subseteq C_i, \quad \delta(P \smallsetminus D_i) \geq \mu(\mathcal{C}) - \varepsilon, \quad \delta(C_i) \leq \mu(\mathcal{C}) + \varepsilon.$$

This implies that C has Dirichlet density which is equal to $\mu(\mathcal{C})$. ∎

References

[DSM] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p Groups*, 2nd ed., Cambridge Stud. Adv. Math. 61, Cambridge Univ. Press, Cambridge, 1999.

[FrJ] M. D. Fried and M. Jarden, *Field Arithmetic*, Ergeb. Math. Grenzgeb. (3) 11, Springer, Heidelberg, 1986.

[GeJ] 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.

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

[JaJ2] —, —, *On torsion of abelian varieties over large algebraic extensions of finitely generated fields: Erratum*, ibid. 32 (1985), 316.

[Jar] M. Jarden, *An injective rational map of an abstract algebraic variety into itself*, J. Reine Angew. Math. 265 (1974), 23–30.

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

[Mum]   D. Mumford, *Abelian Varieties*, Oxford Univ. Press, London, 1974.

[Roq]   P. Roquette, *Analytic Theory of Elliptic Functions over Local Fields*, Hamburger Math. Einzelschriften (Neue Folge) 1, Vandenhoeck & Ruprecht, Göttingen, 1970.

[Ser1] J.-P. Serre, *Résumé des cours de 1985-1986*, Annuaire du Collège de France, Paris, 1986.

[Ser2] —, *Abelian l-adic Representations and Elliptic Curves*, Addison-Wesley, Reading, 1989.

[Ser3] —, *Corps locaux*, Actualités Sci. Indust. 1296, Hermann, Paris, 1968.

[Ser4] —, *Groupes linéaires modulo p et points d'ordre fini des variétés abéliennes*, cours au Collège de France, unpublished notes of Eva Bayer, 1986.

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

[ShT]   G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and its Applications to Number Theory*, Publ. Math. Soc. Japan 6, Math. Soc. Japan, Tokyo, 1961.

Bayit Lachayim   School of Mathematics
Mekor Baruch 12   Tel Aviv University
93465 Jerusalem, Israel   Ramat Aviv, 69978 Tel Aviv, Israel
E-mail: marjac@math.huji.ac.il   E-mail: jarden@math.huji.ac.il