Chandrashekhar B. Khare and Michael Larsen

**Abelian varieties with isogenous reductions**


Published online: 5 January 2021

https://doi.org/10.5802/crmath.129

This article is licensed under the Creative Commons Attribution 4.0 International License.
http://creativecommons.org/licenses/by/4.0/
Number Theory / Théorie des nombres

Abelian varieties with isogenous reductions

Chandrashekhar B. Khare*,a and Michael Larsenb

a UCLA Department of Mathematics, Box 951555, Los Angeles, CA 90095, USA
b Department of Mathematics, Indiana University, Bloomington, IN 47405, USA
E-mails: shekhar@math.ucla.edu (C. B. Khare), mjlarsen@indiana.edu (M. Larsen)

Abstract. Let $A_1$ and $A_2$ be abelian varieties over a number field $K$. We prove that if there exists a non-trivial morphism of abelian varieties between reductions of $A_1$ and $A_2$ at a sufficiently high percentage of primes, then there exists a non-trivial morphism $A_1 \to A_2$ over $\bar{K}$. Along the way, we give an upper bound for the number of components of a reductive subgroup of $GL_n$ whose intersection with the union of $Q$-rational conjugacy classes of $GL_n$ is Zariski-dense. This can be regarded as a generalization of the Minkowski–Schur theorem on faithful representations of finite groups with rational characters.

Résumé. Soient $A_1$ et $A_2$ deux variétés abéliennes sur un corps de nombres $K$. Nous montrons que, s'il existe un morphisme non trivial de variétés abéliennes entre réductions de $A_1$ et $A_2$ pour une proportion suffisamment grande d'idéaux premiers, il existe un morphisme non trivial $A_1 \to A_2$ sur $\bar{K}$. Nous donnons également une majoration du nombre du composantes d'un sous-groupe réductif de $GL_n$ dont l'intersection avec l'union des classes de conjugaison $Q$-rationnelles de $GL_n$ est dense pour la topologie de Zariski; c'est une généralisation d'un théorème de Minkowski–Schur sur les représentations fidèles des groupes finis à caractère rationnel.

Funding. Michael Larsen was partially supported by NSF grant DMS-2001349.

Manuscript received 7th September 2020, revised and accepted 6th October 2020.

In this note, we answer a recent question of Dipendra Prasad and Ravi Raghunathan [6, Remark 1]. We are grateful to Dipendra Prasad and Jean-Pierre Serre for helpful correspondence. We would also like to thank the referee for several improvements and corrections.

Let $K$ be a number field and $A_1$ and $A_2$ abelian varieties over $K$. If $\wp$ is a prime of $K$, we denote by $k_\wp$ the residue field of $\wp$. If $\wp$ is a prime of good reduction for $A_1$, we denote by $A_{1,\wp}$ the reduction and by $\text{Frob}_\wp$ the Frobenius element regarded as an automorphism, well defined up to conjugacy, of the $\ell$-adic Tate module of $A_1$ or, dually, of $H^1(\bar{A}_1,\mathbb{Z}_\ell)$.

Theorem 1. Let $A_1$ and $A_2$ be abelian varieties over a number field $K$. Suppose that for a density one set of primes $\wp$ of $K$, there exists a non-trivial morphism of abelian varieties over $\bar{k}_\wp$ from $A_{1,\wp}$ to $A_{2,\wp}$. Then there exists a non-trivial morphism of abelian varieties from $A_1$ to $A_2$ defined over $\bar{K}$.

* Corresponding author.
Let $G$ be a connected reductive algebraic group over an algebraically closed field $F$ of characteristic 0, and let $V$ be a finite dimensional representation of $G$. Let $T$ be a maximal torus of $G$ and $W$ the Weyl group of $G$ with respect to $T$. If $V$ is irreducible, we say it is minuscule if $W$ acts transitively on the weights of $V$ with respect to $T$. The highest weight of $V$ with respect to any choice of Weyl chamber has multiplicity 1, so every element of the Weyl orbit has multiplicity one.

For general finite dimensional representations $V$, we say $V$ is minuscule if each of its irreducible factors is so. Regarding the character of a representation $V$ as a function $f_V$ from $W$-orbits in $X^*(T)$ to non-negative integers, when $V$ is minuscule, for any dominant weight $\lambda$, the multiplicity in $V$ of the irreducible $G$-representation $V_{\lambda}$ with highest weight $\lambda$ is the value of $f_V$ on the $W$-orbit containing $\lambda$.

**Proposition 2.** Let $V_1$ and $V_2$ be minuscule representations of $G$. If $\dim \text{Hom}_T(V_1, V_2) > 0$, then $\dim \text{Hom}_G(V_1, V_2) > 0$.

**Proof.** If $\dim \text{Hom}_T(V_1, V_2) > 0$, then $V_1$ and $V_2$ must have a common $T$-irreducible factor, and that means they have a common weight $\chi$ with respect to $T$. If $\lambda$ is the dominant weight in the orbit of $\chi$, then $V_1$ and $V_2$ each contain $V_\lambda$ as a subrepresentation, so $\dim \text{Hom}_G(V_1, V_2) > 0$. □

Now let $A_1$ and $A_2$ denote abelian varieties over a number field $K$ with absolute Galois group $G_K := \text{Gal}(\bar{K}, K)$. Let $\ell$ be a fixed rational prime, and let $F = \overline{\mathbb{Q}}_\ell$. Let $V_i = H^1(A_i, F)$, regarded as $G_K$-modules. Let $V_{12} := V_1 \oplus V_2$ as $G_K$-module and $G_{12}$ the Zariski closure of $G_K$ in $\text{Aut}_F(V_{12})$. By the semisimplicity of Galois representations defined by abelian varieties [3], $G_{12}$ is reductive. Let $G$ denote the identity component $G_{12}$.

**Proposition 3.** There exists a positive density set of primes $\wp$ of $K$ such that $A_1 \times A_2$ has good reduction at $\wp$, and $\text{Frob}_\wp$ generates a Zariski dense subgroup of a maximal torus of $G$.

**Proof.** The condition that $\text{Frob}_\wp$ lies in the identity component $G$ has density $[G_{12} : G]^{-1} > 0$. By a theorem of Serre [4, Theorem 1.2], there exists a proper closed, conjugation-stable subvariety $X$ of $G$ such that $\text{Frob}_\wp \in G \setminus X$ implies that $\text{Frob}_\wp$ generates a Zariski-dense subgroup of a maximal torus of $G$. However, by a second theorem of Serre [8, Théorème 10], the set of $\wp$ such that $\text{Frob}_\wp \in X$ has density 0. □

We can now prove the main Theorem 1.

**Proof.** A well-known theorem of Tate [11] asserts that the existence of a non-trivial $\mathbb{F}_q$-morphism between abelian varieties over $\mathbb{F}_q$ is equivalent to the existence of a $\text{Frob}_q$-stable morphism of their $\ell$-adic Tate modules. By the easy direction of this result, the existence of a non-trivial morphism defined over $\mathbb{F}_q$ implies the existence of a $\text{Frob}_q^m$-stable morphism of their Tate modules for some positive integer $m$.

By Proposition 3, the hypothesis of the Theorem 1 therefore implies that

$$\dim \text{Hom}_G(V_1, V_2)^{\text{Frob}_\wp^m} > 0$$

for some prime $\wp$ for which $\text{Frob}_\wp$ generates a Zariski-dense subgroup of a maximal torus $T$ of $G$ and some positive integer $m$. As $T$ is connected, $\text{Frob}_\wp^m$ likewise generates a Zariski-dense subgroup of $T$. Thus $\dim \text{Hom}_T(V_1, V_2) > 0$. By a theorem of Pink [5, Corollary 5.11], the $G$-representations $V_1$ and $V_2$ are minuscule. Thus Proposition 2 implies that $\dim \text{Hom}_G(V_1, V_2) > 0$. Finally, Faltings’ proof of Tate’s Conjecture [3] implies $\text{Hom}_K(A_1, A_2)$ is non-zero. □

**Remark 4.** One might ask whether there exists a non-trivial homomorphism $A_1 \rightarrow A_2$ defined over $K$ itself if for a density one set of $\wp$ there exists a non-trivial $k_\wp$-homomorphism $A_{1\wp} \rightarrow A_{2\wp}$. D. Prasad pointed out the following counterexample to us. Let $E$ be an elliptic curve over $\mathbb{Q}$ which does not have complex multiplication. Let $E_n$ denote the quadratic twist of $E$ by $n \in \mathbb{Q}^\times$. Let
$A_1 = E, A_2 = E_2 \times E_3 \times E_6$. For every rational prime $p > 3$, either 2, 3, or 6 lies in $\mathbb{F}_p^\times$, so if $E$ has good reduction at $p$, the same is true for both $A_1$ and $A_2$, and there exists an $\mathbb{F}_p$-isomorphism from $(A_1)_p$ to at least one of $(E_2)_p$, $(E_3)_p$, and $(E_6)_p$, and therefore a non-trivial $\mathbb{F}_p$-homomorphism to $(A_2)_p$. On the other hand, there is no $\mathbb{Q}$-isogeny from $A_1$ to any one of $E_2, E_3, \text{ or } E_6$, and therefore no non-trivial $\mathbb{Q}$-homomorphism to $A_2$.

We can prove a stronger version of Theorem 1 in analogy with the theorem of C. S. Rajan [7].

**Theorem 5.** Let $n$ be a positive integer. If $A_1$ and $A_2$ are abelian varieties of dimension $\leq n$ over a number field $K$ and the set of primes $\mathfrak{p}$ of $K$ for which there exists a non-trivial $k_{\mathfrak{p}}$-morphism of abelian varieties from $A_1\mathfrak{p}$ to $A_2\mathfrak{p}$ has upper density $> 1 - e^{-6n^2}$, then there exists a non-trivial $\overline{K}$-morphism of abelian varieties from $A_1$ to $A_2$.

The only additional ingredient necessary to prove Theorem 5 is an upper bound, depending only on $n$, on the number of components of $G_{12}$. This is an immediate consequence of the following theorem.

**Theorem 6.** Let $n$ be a positive integer, $F$ a field of characteristic 0, and $G \subset \text{GL}_n$ a reductive $F$-subgroup. If the set of $\overline{F}$-points of $G$ consisting of matrices whose characteristic polynomials lie in $\mathbb{Q}[x]$ is Zariski-dense, then $|G/G^o| < e^{6n^2} n^{12n}$.

We remark that without the rationality assumption, this statement fails even for $n = 1$, where $G$ could be an arbitrarily large cyclic group.

**Proof.** The locus of $\overline{F}$-points of $G$ whose characteristic polynomials lie in $\mathbb{Q}[x]$ is $G_{F}$-stable, so the Zariski-closure does not change when the base field is changed from $F$ to $\overline{F}$. This justifies assuming that $F$ is algebraically closed.

We can write $G^o = DZ^o$, where $D$ and $Z := Z(G^o)$ are the derived group and the center of $G^o$ respectively. By [10, Corollary 2.14], the outer automorphism group of $D$ is contained in the automorphism group of the Dynkin diagram $\Delta$ of $D$. Every automorphism of $\Delta$ preserves the set of isomorphic components. We claim that $|\text{Aut} \Delta| \leq n!$. It suffices to prove this when $\Delta$ consists of $m$ mutually isomorphic connected diagrams $\Delta_0$ of rank $r = n/m$. The claim obviously holds when $r = 1$. It is easily verified for $n \leq 4$. For $n \geq 5$, the classification of connected Dynkin diagrams gives $|\text{Aut}(\Delta_0)|^{2/r} \leq \sqrt{6} < n/2$, so if $r \geq 2$,

$$|\text{Aut}(\Delta)| = |\text{Aut}(\Delta_0)|^{n/r} (n/r)! < (n/2)^{n/2} [n/2]! < n!.$$

Any automorphism of $G^o$ is determined by its restrictions to the characteristic subgroups $D$ and $Z^o$. An automorphism which is inner on $D$ and trivial on $Z^o$ is inner. Thus, the homomorphism $\text{Aut}(G^o) \rightarrow \text{Aut}(D) \times \text{Aut}(Z^o)$ gives an injective homomorphism

$$\text{Out}(G^o) \rightarrow \text{Out}(D) \times \text{Out}(Z^o) = \text{Out}(D) \times \text{GL}_k(Z),$$

where $k = \dim Z^o \leq n$. By Minkowski’s theorem [9, Theorem 9.1], every finite subgroup of $\text{GL}_k(Z)$ has order at most

$$M(k) := \prod_p \sum_{i \geq 0} \left\lfloor \frac{k}{(p-1)p^i} \right\rfloor.$$

We have

$$\log M(k) \leq \sum_{p=2}^{k+1} \frac{kp \log p}{(p-1)^2} = k \sum_{i=1}^{k} \frac{(i+1) \log(i+1)}{i^2} \leq 2k^2,$$

since $(i+1) \log(i+1) \leq 2i^2$ for all $i \geq 1$. Thus, any finite subgroup of $\text{Out}(G^o)$ has order $\leq n!e^{2n^2}$. 

C. R. Mathématique, 2020, 358, no 9-10, 1085-1089
The conjugation action on $G^o$ defines a homomorphism $G/G^o \to \text{Out}(G^o)$. Let $\Gamma_0$ denote the kernel of this homomorphism and $G_0$ the inverse image of $\Gamma_0$ in $G$. Thus, the index of $\Gamma_0$ in the component group $G/G^o$ is $\leq n!e^{2n^2} \leq e^{3n^2}$. Arguing by contradiction, we may assume the order of $\Gamma_0$ is at least 
\[ e^{-3n^2} \left| G/G^o \right| \geq e^{3n^2} n^{2n}. \]

Let $\Gamma := Z_{G_0}(G^o)/Z^o$, so $\Gamma_0 \cong Z_{G_0}(G^o)/Z$ is a quotient group of $\Gamma$. Consider the short exact sequence 
\[ 0 \to Z^o \to Z_{G_0}(G^o) \to \Gamma \to 0. \]
The extension class $\alpha \in H^2(\Gamma, Z^o)$ is annihilated by $N := |\Gamma|$. As $Z^o \cong (F^*)^k$ is a divisible group, it follows that the extension class $\alpha$ lies in the image of $H^2(\Gamma, Z^o[N])$, where $Z^o[N]$ denotes the kernel of the $N$th power map on $Z^o$. We can therefore represent $\alpha$ by a 2-cocycle with values in $Z^o[N]$. This means that there exists a set-theoretic section $i: \Gamma \to Z_{G_0}(G^o)$ such that the associated 2-coycle takes values in $Z^o[N]$, and it follows that $\Gamma_0 := Z^o[N]i(\Gamma)$ is a finite subgroup of $Z_{G_0}(G^o) \subset G$ which maps onto $\Gamma$ and therefore onto $\Gamma_0$.

By Jordan’s theorem, $\Gamma_0$ contains an abelian normal subgroup $\tilde{A}_0$ of index $\leq J(n)$, a constant depending only on $n$. The optimal Jordan constant has been computed by Michael Collins [2], and for all $n$, we have $J(n) \leq e^{2n^2}$. Indeed, for $n \geq 71$, the bound, $(n + 1)!$, is given by Theorem A, and 
\[ (n + 1)! < (n + 1)^n < \left(\frac{n^2}{2}\right)^n = e^{2n^2}. \]
For $20 \leq n \leq 70$ and $n \leq 19$, the bounds are given by Theorems B and D respectively, and they can be checked by machine to be less than $e^{2n^2}$ in every case.

Let $T$ be a maximal torus of $G^o$, so $\tilde{A}_0 T$ is a commutative subgroup of $G_0$. As 
\[ \tilde{A}_0 \cap T \subset \tilde{A}_0 \cap G^o = \ker \tilde{A}_0 \to \Gamma_0, \]
we have 
\[ |\tilde{A}_0 T/T| = |\tilde{A}_0 / (\tilde{A}_0 \cap T)| \geq |\text{Im} \tilde{A}_0 \to \Gamma_0| \cong \frac{|\Gamma_0|}{e^{2n^2}} \geq e^{n^2} n^{2n}. \]
Therefore, if $M := e^n n^{2n}$, then $\tilde{A}_0 T$ has at least $M^n$ components. Since $\tilde{A}_0 T/T$ is a quotient group of $\tilde{A}_0 \subset \text{GL}_n(F)$, it contains no elementary $p$-group of rank $> n$, so it must have an element of order $\geq M$. Let $g \in \tilde{A}_0$ map to such an element.

By hypothesis, there exists $t \in G^o \times [g]$ such that the characteristic polynomial of $gt$ has coefficients in $Q$. We can further assume that $t$ is semisimple, so we can choose our maximal torus $T$ to contain $t$. Let $T' = (g)T$. Every element of $T'$ is the product of two commuting elements, one of which is of finite order, and one which belongs to $T$, so both are semisimple, from which it follows that their product is semisimple. Thus $T'$ is diagonalizable, so it is a closed subgroup of a maximal torus of $\text{GL}_n$ [1, Proposition 8.4]. Without loss of generality, we may assume this maximal torus is the group $\text{GL}_n^0$ of invertible diagonal matrices.

The contravariant functor taking an algebraic group to its character group gives an equivalence of categories between diagonalizable groups and finitely generated abelian groups [1, Proposition 8.12]. In particular, there is a bijective correspondence between subgroups $\Lambda \subset \mathbb{Z}^n$ and closed subgroups $D_\Lambda$ of the group $\text{GL}_n^0$ of diagonal matrices in $\text{GL}_n$, where 
\[ D_\Lambda = \{ (x_1, \ldots, x_n) \in \text{GL}_n^0 | \Lambda(x_1, \ldots, x_n) = 1 \ \forall \ \Lambda \in \Lambda \}. \]

Let $\Lambda$ be the subgroup of $\mathbb{Z}^n$ such that $D_\Lambda = T$ and $\Lambda'$ the subgroup such that $D_{\Lambda'} = T'$. The inclusion $T \hookrightarrow T'$ corresponds to the surjection $\mathbb{Z}^n/\Lambda' \to \mathbb{Z}^n/\Lambda$ and thus to the inclusion $\Lambda' \subset \Lambda$. As $T'/T$ is cyclic, $\Lambda/\Lambda'$ is cyclic of the same order $k$. Let $\lambda \in \Lambda$ map to a generator of $\Lambda/\Lambda'$. Then the smallest integer $m$ such that $\lambda((gt)^m) = 1$ is the smallest such that $\lambda(g^m) = 1$, which is $k$.

Writing $gt = (x_1, \ldots, x_n) \in \text{GL}_1(F)^n \subset \text{GL}_n(F)$, the $x_i$ are the eigenvalues of $gt$, so they all lie in some Galois extension of $Q$ of degree $\leq n!$. Therefore $\lambda(g^t)$ lies in this extension. Since it is a
primitive $k$th root of unity, this implies $\phi(k) \leq n!$. Now $\phi(q) \geq \sqrt{q}$ for all prime powers $q$ except 2, and it follows from the multiplicativity of $\phi$ that $\phi(k) \geq \sqrt{k}/2$ for all $k \geq 1$, so $M \leq k \leq 2n!^2$, which is a contradiction. □

References