Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Journal of Number Theory 105 (2004) 322–332
JOURNAL OF Number Theory
http://www.elsevier.com/locate/jnt

Reduction of homomorphisms mod p and algebraicity

Chandrashekhar Khare[a,b] and Dipendra Prasad[b,c,*]

[a] *Department of Math, University of Utah, 155 S 1400 E, Salt Lake City, UT 84112, USA*
[b] *School of Mathematics, Tata Institute of Fundamental Research, Colaba, Bombay 400005, India*
[c] *Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211019, India*

Received 28 February 2003; revised 20 August 2003

Communicated by D. Goss

Abstract

Let A be an abelian variety over a number field K. Let ϕ be an endomorphism of $A(K)$ into itself which reduces modulo v for almost all finite places v of K. The question we discuss in this paper is whether ϕ arises from an endomorphism of the abelian variety A. We answer this question in the affirmative for many cases. The question is inspired by a work of C. Corrales and R. Schoof, and uses a recent work of Larsen. We also look at the analogue of this question for linear algebraic groups.

Keywords: Abelian variety; Reduction of abelian variety; Kummer theory; Algebraicity

1. Introduction

Let A be an abelian variety over a number field K. There is a finite set S of places of K and an abelian scheme $\mathscr{A}$ over $\mathcal{O}_S$, the ring of S-integers of K, with generic fibre A. For v not in S we can consider reduction mod v of $\mathscr{A}$ at v. We will abuse notation to denote the reduction mod v of $\mathscr{A}$ also by A. All the places v we consider below are *outside* S even if this is not mentioned explicitly.

Consider the specialisation map $sp_v : A(K) \to A(k_v)$, and denote the image of $A(K)$ under sp_v by $A(v)$. We say that a homomorphism $\phi : A(K) \to A(K)$ specialises mod v

*Corresponding author.
E-mail addresses: shekhar@math.utah.edu, shekhar@math.tifr.res.in (C. Khare), dprasad@math.tifr.res.in (D. Prasad).

0022-314X/$ - see front matter © 2003 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2003.10.006

if there is a homomorphism $\phi_v : A(v) \to A(v)$ such that the diagram

$$\begin{array}{ccc} A(K) & \stackrel{\phi}{\to} & A(K) \\ sp_v \downarrow & & \downarrow sp_v \\ A(v) & \stackrel{\phi_v}{\to} & A(v) \end{array}$$

commutes.

The following are the two main theorems proved in this paper.

Theorem 1. *Let A be an absolutely simple abelian variety defined over a number field K and let $P \in A(K)$ be a point of infinite order and $Q \in A(K)$ another point such that the order of $Q \bmod v$ divides the order of $P \bmod v$ for almost all places v of K. Then there is a K-endomorphism j of A such that $Q = j(P)$.*

Theorem 2. *Let A be an absolutely simple abelian variety over a number field K. If a homomorphism $\phi : A(K) \to A(K)$ specialises $\bmod v$ for almost all places v of K, then the restriction of ϕ to a subgroup of finite index of $A(K)$ is induced by a K-endomorphism of A. If $A(K)$ is torsion-free, ϕ itself is induced by a K-endomorphism.*

Remark. In Theorem 1 it is necessary to have P of infinite order. Otherwise taking P and Q to be two linearly independent elements of order p in $E(K)$ for an elliptic curve E without CM leads to a counter-example.

Theorem 1 when $\dim(A) = 1$ is a result of [CS]. A result very close to Theorem 1 has been proved in [L] where it is proved that there is a K-endomorphism j of A such that $nQ = j(P)$ for some integer n. The proof of Theorem 1 uses crucially the result of [L].

We were led to the investigations of this paper by the results of [CS,K], and in particular we view Theorem 2 as an analog of the results of [K], that are for compatible systems of Galois representations, in the present geometric context.

An earlier version of this paper was written in late 2001. Around that time, and since then, there have been many works that are devoted to generalising the theorem of [CS] to abelian varieties (see [L] for a bibliography). The result in [L] is the strongest in that direction. In the earlier version we had proved Theorem 1 with stronger assumptions on A. These results are now superseded by Larsen [L]. We can now simply *use* the result of [L] and a technical lemma (see Lemma 5) to prove Theorem 1. For the convenience of the reader, we state Larsen's theorem proved in [L].

Theorem 3. *Let A be an abelian variety defined over a number field K. Let P and Q be two points in $A(K)$ such that the order of $Q \bmod v$ divides the order of $P \bmod v$ for*

almost all places v of K. Then there is a K-endomorphism ϕ of A and an integer $n \neq 0$ such that $\phi(P) = nQ$.

Our main contribution to the proofs of Theorems 1 and 2, after the above theorem due to Larsen, are Lemmas 5 and 6. Lemma 5 is used to make the above theorem of Larsen more precise under our assumption that A is simple (as in Theorem 1), and Lemma 6 proves that the endomorphism which relates P and $\phi(P)$ which we get from Theorem 1 is independent of P.

The viewpoint of our paper is different from the other works (which were interested in generalising the result of [CS] per se) and is more "group theoretic": this is exemplified in Theorem 2. It is this viewpoint which led us to seek analogs of Theorem 2 in the context of arithmetic subgroups of linear algebraic groups, where there is no direct analog of results of [CS] (and hence Theorem 1) as mentioned at the end of the introduction of [CS]. Thus in the last section of the paper we prove an analog of Theorem 2 (see Theorems 4 and 5) for arithmetic groups that we find appealing.

2. Reduction of points of infinite order in $A(K)$ mod v

The main results of this section are Lemmas 4 and 5 below. We need some preliminaries.

The following lemma is well known, cf. S. Lang's book, *Algebra*, Section 10 of the chapter on Galois theory for the case $i = 1$. It also follows from generalities on cohomology once we know it is true for $i = 0$, which is of course clear.

Lemma 1. *Let G be a group, and E a G-module. Let τ be an element in the center of G. Then $H^i(G, E), i = 0, 1, \ldots$ is annihilated by the map on $H^i(G, E)$ induced from the map $x \to \tau x - x$ from E to itself.*

Lemma 2. *Let A be an abelian variety over a number field K. Let $K_{\ell^n} = K(A[\ell^n])$, and $G_{\ell^n} = \mathrm{Gal}(K_{\ell^n}/K)$. Let $G_{\ell^\infty} = \mathrm{Gal}(K_{\ell^\infty}/K)$ with $K_{\ell^\infty} = \cup_n K_{\ell^n}$. Then $H^1(G_{\ell^m}, A[\ell^n])$ $(m \geqslant n)$ and $H^1(G_{\ell^\infty}, A[\ell^n])$ are of finite orders, bounded independent of m and n.*

Proof. We note that G_{ℓ^∞} being a compact ℓ-adic Lie group, is topologically finitely generated, hence each finite quotient such as G_{ℓ^m} is generated by a set of elements of cardinality independent of m.

From the definition of $H^1(G, E)$ in terms of maps ϕ from G to E such that $\phi(g_1 g_2) = \phi(g_1) + g_1\phi(g_2)$, it follows that an element of $H^1(G, E)$ is determined by a map on a set of generators of G. Since $A[\ell^n] \cong (\mathbb{Z}/\ell^n)^{2\dim(A)}$ as abelian groups, it follows that $H^1(G_{\ell^m}, A[\ell^n])$ is a finitely generated abelian group which is generated by a set of elements of cardinality independent of m, n.

It follows from a theorem of Bogomolov, cf. [Bo], that the ℓ-adic Lie group G_{ℓ^∞} contains homotheties congruent to 1 modulo ℓ^N for some integer $N>0$. Therefore by Lemma 1, $H^1(G_{\ell^m}, A[\ell^n])$ is annihilated by ℓ^N. It follows that $H^1(G_{\ell^m}, A[\ell^n])$ is a finitely generated abelian group which is generated by a set of elements of cardinality independent of m,n, and annihilated by ℓ^N, and thus is of finite order, bounded independent of m,n.

The statement about $H^1(G_{\ell^\infty}, A[\ell^n])$ follows either by noting that the cohomology $H^1(G_{\ell^\infty}, A[\ell^n])$ can be calculated in terms of continuous cochains on G_{ℓ^∞}, for which the earlier argument applies as well, or by noting that $H^1(G_{\ell^\infty}, A[\ell^n])$ is the direct limit of $H^1(G_{\ell^m}, A[\ell^n])$ (direct limit over m), and a direct limit of finitely generated abelian groups each of which is generated by a set of elements of cardinality independent of n, and each annihilated by ℓ^N, is of order bounded independent of n. □

Lemma 3. *For sufficiently large integer n, and $m \geqslant n$, the extension $K_{\ell^m, P/\ell^n} = K(A[\ell^m], \frac{1}{\ell^n}.P)$ is a non-trivial extension of $K_{\ell^m} = K(A[\ell^m])$.*

Proof. Denote the Galois group $\mathrm{Gal}(K_{\ell^n}/K)$ by G_{ℓ^n}. By the Kummer sequences, we have a commutative diagram involving short exact sequences,

$$\begin{array}{ccccccccc} 0 & \to & A(K)/\ell^n A(K) & \to & H^1(G_K, A[\ell^n]) & \to & H^1(G_K, A)[\ell^n] & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & A(K_{\ell^m})/\ell^n A(K_{\ell^m}) & \to & H^1(G_{K_{\ell^m}}, A[\ell^n]) & \to & H^1(G_{K_{\ell^m}}, A)[\ell^n] & \to & 0. \end{array}$$

As the kernel of the restriction map $H^1(G_K, A[\ell^n]) \to H^1(G_{K_{\ell^m}}, A[\ell^n])$ is the image of $H^1(G_{\ell^m}, A[\ell^n])$ in $H^1(G_K, A[\ell^n])$, the kernel has order which is bounded independent of m,n by Lemma 2. As P is non-torsion, the image of P under the coboundary map (in the first exact sequence) to $H^1(G_K, A[\ell^n])$ has unbounded order as n varies, hence also in $H^1(G_{K_{\ell^m}}, A[\ell^n])$ which represents the extension $K(A[\ell^m], \frac{1}{\ell^n}.P)$ of K_{ℓ^m}. From this the lemma follows.

Lemma 4. *Given an abelian variety A over K, a point P of $A(K)$ of infinite order, and any prime ℓ, there are infinitely many places v of K (in fact a set of positive density) such that the reduction of $P \bmod v$ has order divisible by ℓ.*

Proof. By Lemma 3, for sufficiently large n, $K(A[\ell^n], \frac{1}{\ell^n}.P)$ is a non-trivial extension of $K_{\ell^n} = K(A[\ell^n])$. Therefore there is a positive density of places v of K that split in $K(A[\ell^n])$ but not in $K(A[\ell^n], \frac{1}{\ell^n}.P)$. Clearly, for such v's, the reduction of $P \bmod v$ has order divisible by ℓ. □

Lemma 5. *Given an absolutely simple abelian variety A over a number field K and a point P of $A(K)$ of infinite order, and any prime ℓ, there are infinitely many places v of*

K (in fact a set of positive density) such that the reduction of $P \bmod v$ has order prime to ℓ.

Proof. Let $K_{P,\ell^n} = K(A[\ell^n], \frac{1}{\ell^n}.P)$, and $K_{\ell^n} = K(A[\ell^n])$. By Lemma 3, $K_{P,\ell^n} = K(A[\ell^n], \frac{1}{\ell^n}.P)$, is a non-trivial extension of $K_{\ell^n} = K(A[\ell^n])$. We will prove that the intersection of the fields K_{P,ℓ^n} and $K_{\ell^{n+1}}$ is K_{ℓ^n} for some n large enough. This, together with the theorem of Bogomolov recalled in Lemma 2, will imply that there is a positive density of primes v in K which are split in K_{P,ℓ^n} and for which the Frobenius as an element of $\mathrm{Gal}(K_{\ell^{n+1}}/K)$ is a non-trivial homothety in $\mathrm{GL}_{2g}(\mathbb{Z}/\ell^{n+1})$, $g = \dim A$, which is congruent to 1 modulo ℓ^n. For such primes v, it can be easily seen that the order of P modulo v is not divisible by ℓ, completing the proof of the lemma. It thus suffices to prove that the intersection of the fields K_{P,ℓ^n} and $K_{\ell^{n+1}}$ is K_{ℓ^n}.

Let E_{ℓ^n} (resp. G_{ℓ^n}) denote the Galois group of K_{P,ℓ^n} (resp. K_{ℓ^n}) over K, and let A_{ℓ^n} denote the Galois group of K_{P,ℓ^n} over K_{ℓ^n}. We have the exact sequence of groups,

$$0 \to A_{\ell^n} \to E_{\ell^n} \to G_{\ell^n} \to 1.$$

It is easy to see that the intersection of the fields K_{P,ℓ^n} and $K_{\ell^{n+1}}$ is K_{ℓ^n} if and only if inside the group E_{ℓ^n} which is a quotient of $E_{\ell^{n+1}}$, the image of $A_{\ell^{n+1}}$ is A_{ℓ^n}.

Let E_{ℓ^∞} denote the Galois group of $K_{P,\ell^\infty} = \cup_n K_{P,\ell^n}$ over K, and A_{ℓ^∞}, the Galois group of K_{P,ℓ^∞} over $K_{\ell^\infty} = \cup_n K_{\ell^n}$. We have the exact sequence of groups,

$$0 \to A_{\ell^\infty} \to E_{\ell^\infty} \to G_{\ell^\infty} \to 1,$$

and a natural mapping of this short exact sequence to the exact sequence earlier involving E_{ℓ^n}. One can think of A_{ℓ^∞} as a subgroup of $T_\ell(A)$ obtained by choosing a sequence of points P_n in $A(\bar{K})$ with $\ell \cdot P_1 = P$, and $\ell \cdot P_{i+1} = P_i$. This same sequence of points can be used to get an embedding of A_{ℓ^n} into $A[\ell^n]$. We wish to prove that the mapping from $A_{\ell^{n+1}}$ to A_{ℓ^n} is surjective for n large. All these groups contain $\ell^m T_\ell(A)$ (or its quotient by ℓ^n) for some m by a theorem due to Bertrand, cf. Theorem 2 of [B], according to which A_{ℓ^∞} is an open subgroup of $T_\ell(A) = \mathbb{Z}_\ell^{2g}$, hence contains $\ell^m T_\ell(A)$ for some m. Dividing by this group, we get an inverse system $A[\ell^r]/\ell^m$ (indexed by r) in which all but finitely many maps are isomorphism from $(\mathbb{Z}/\ell^m)^{2g}$ to itself. In this the subsystem A_{ℓ^r}/ℓ^m, must necessarily become stationery for large r, proving that the mapping from $A_{\ell^{n+1}}$ to A_{ℓ^n} is surjective for n large. □

Remarks. (1) The above proof can be generalised to yield that for any abelian variety A defined over K and any point P of $A(K)$ which does not project to a non-zero torsion point in any (geometric) subquotient of A, given a prime ℓ there are a positive density of places v of K such that $P \bmod v$ has order prime to ℓ.

(2) Although we have given separate proofs of Lemmas 4 and 5, observe that Lemma 5 implies Lemma 4 when A is an absolutely simple abelian variety. This

follows by applying Lemma 5 to the point of infinite order $P+R$ where R is a non-zero ℓ-torsion point. (We note that to prove Lemma 4, we are allowed to go to a finite extension of K, and hence assume that A has non-zero ℓ-torsion point over K.) Lemma 5 implies that there are infinitely many places v of K for which the order of $P+R$ is coprime to ℓ. It is easy to see that for such places v, the order of the reduction of $P \bmod v$ must be divisible by ℓ.

(3) We note that Bertrand's theorem recalled during the course of the proof of Lemma 5 implies Lemma 3.

(4) Lemmas 4 and 5 were proved in the case of $\dim(A)=1$ in [CS] using Siegel's theorem on finiteness of S-integral points on elliptic curves. The proofs of [CS] seem difficult to generalise to higher dimensions.

3. A linear algebra result

We need the following lemma for the proof of Theorem 2.

Lemma 6. *Let A be a finitely generated free abelian group. Let $\mathscr{D}$ be a division algebra which contains $\mathbb{Q}$ and is finite dimensional over $\mathbb{Q}$. Let $\mathscr{O}$ be an order in $\mathscr{D}$. Suppose $\mathscr{O}$ acts on A on the left making it into a left $\mathscr{O}$-module. Suppose that f is an endomorphism of A as an additive group such that for all $a \in A$, there exists $f_a \in \mathscr{O}$ such that $f(a) = f_a \cdot a$. Then f is multiplication by an element of $\mathscr{O}$.*

Proof. Clearly $A \otimes_{\mathbb{Z}} \mathbb{Q}$ is a vector space over $\mathbb{Q}$ on which $\mathscr{O} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathscr{D}$ acts, making it into a $\mathscr{D}$-vector space. From the hypothesis that $f(a) = f_a \cdot a$ for all $a \in A$, we find that any $\mathscr{D}$-subspace of $A \otimes_{\mathbb{Z}} \mathbb{Q}$ is stable under f (extended to $A \otimes_{\mathbb{Z}} \mathbb{Q}$). Write $A \otimes_{\mathbb{Z}} \mathbb{Q} = L_1 \oplus \cdots \oplus L_n$, as a direct sum of $\mathscr{D}$-subspaces L_i of dimension 1 which as has been noted is invariant under f, i.e., $f(L_i) \subset L_i$. Write $M_i = L_i \cap A$; then M_i is a lattice in L_i, and $\oplus M_i$ is a subgroup of finite index in A. Since both L_i and A are invariant under f, so is M_i. Also, each L_i and A being invariant under $\mathscr{O}$, so is M_i. We will now prove that the restriction of f to M_i is given by multiplication by an element f_i in $\mathscr{O}$.

We can clearly assume that M_i is a lattice in $\mathscr{D}$ which is invariant under $\mathscr{O}$. Also, after scaling by an element of $\mathscr{D}^*$ on the right, we can assume that the lattice M_i in $\mathscr{D}$ contains 1.

Suppose that $f_i(1) = \alpha_i \in \mathscr{O}$. We can thus after replacing f_i by $f_i - \alpha_i$, assume that $f_i(1) = 0$. We would like to prove that f_i is identically zero. Assuming the contrary, let x be an element in $M_i \cap \mathscr{O}$ such that $f_i(x) \neq 0$. After scaling x, we can moreover assume that $f_i(x)$ belongs to $\mathscr{O}$.

By hypothesis, for every element $m \in \mathbb{Z}$, there exists an element $\lambda_m \in \mathscr{O}$ such that $f_i(m+x) = \lambda_m \cdot (m+x)$. For an element $z \in \mathscr{D}$, let $\mathrm{Norm}(z)$ denote the determinant of the left multiplication by z on $\mathscr{D}$. Since $f_i(x) = f_i(m+x) = \lambda_m \cdot (x+m)$, it follows that $\mathrm{Norm}(m+x)$ and $\mathrm{Norm}(f_i(x))$ are integers in $\mathbb{Q}$, and $\mathrm{Norm}(m+x)$ divides $\mathrm{Norm}(f_i(x))$. Since $\mathrm{Norm}(m+x)$ is a polynomial in m with coefficients in $\mathbb{Z}$ of degree equal to the dimension of $\mathscr{D}$ over $\mathbb{Q}$ of leading term 1 and constant term

$\mathrm{Norm}(x)$, the polynomial $\mathrm{Norm}(m+x)$, as m varies, takes arbitrary large values, hence cannot divide the fixed integer $\mathrm{Norm}(f_i(x))$.

We have thus proved that f restricted to any 1 dimensional $\mathscr{D}$ submodule of $A\otimes_{\mathbb{Z}}\mathbb{Q}$ is multiplication by an element of $\mathscr{D}$. From this it is trivial to see that the action of f on $A\otimes_{\mathbb{Z}}\mathbb{Q}$ is multiplication by an element of $\mathscr{D}$, which must moreover lie in $\mathscr{O}$, completing the proof of the lemma. □

Remark. The lemma above holds good only in the integral version stated above, and not for vector spaces, and hence is not totally trivial. We point out an example to illustrate that the analogue of the lemma is not true for vector spaces. For this, let K be a finite extension of $\mathbb{Q}$ of degree >1. There is an action of K^* on K via left or right multiplication. Let f be an automorphism of K (considered as a vector space over $\mathbb{Q}$) which does not arise from the action of an element of K^*. Such an automorphism f satisfies the hypothesis of the previous lemma as for any $a\neq 0$, $f(a)\in K^*$, hence $f(a)=f_a\cdot a$ with $f_a\in K^*$, but such an f does not satisfy the conclusion of the lemma.

4. Proof of Theorems 1 and 2

4.1. Theorem 1. Proof

We will deduce Theorem 1 from Lemma 5 and Theorem 3 above due to Larsen. Note that by Theorem 3 and the hypotheses of Theorem 1 there is an isogeny j_0 of A such that $j_0(P)=nQ$ for some integer n. We wish to prove that n can be chosen to be 1 for an appropriate choice of j_0. Let $L=K(A[n])$. Let ℓ^r be the highest power of a prime ℓ which divides n. We will prove that ℓ^r torsion points of $A(L)$ are contained in the kernel of j_0. If that were not the case, there would be an ℓ^r torsion point of $A(L)$, say R, which does not belong to the kernel of j_0. By Lemma 5, there are infinitely many places v of L such that the order of $P+R$ is coprime to ℓ in the residue field ℓ_v of L, and hence the ℓ-primary component of the orders of P and R are the same, of order ℓ^r. For such places v of L, the order of $j_0(P+R)=j_0(P)+j_0(R)=nQ+j_0(R)$ is also coprime to ℓ. By choice, $j_0(R)$ is a non-zero torsion point on A of order dividing ℓ^r, say $\ell^s, 0<s\leqslant r$. Thus since the order of $nQ+j_0(R)$ is coprime to ℓ, the ℓ-primary components of the order of $j_0(R)$ and nQ are the same. Hence the ℓ-primary component of the order of nQ is ℓ^s, and therefore of Q, ℓ^{r+s}, contradicting our hypothesis that the order of Q divides the order P at each place of K, and hence of L. This proves that the ℓ^r torsion points of $A(\bar{K})$ are contained in the kernel of j_0 where ℓ^r is the highest power of ℓ dividing n. Thus all the n-torsion points of $A(\bar{K})$ are contained in the kernel of j_0. Therefore the isogeny j_0 can be written as nj for an isogeny j of A. Since j_0 is defined over K, it follows from the equation $j_0(P)=nQ$ that j is also defined over K. (This follows from the fact that the endomorphism ring of an abelian variety is a torsion-free abelian group.) Thus we have $n(j(P)-Q)=0$. This implies that $j(P)=Q+S$ for a certain torsion point S on $A(K)$. If S is non-zero, let the order of S be divisible by a prime ℓ. Using Lemma 5 choose a place v of K where the order of P, and hence of Q and $j(P)$, is

coprime to ℓ. However, since $j(P) = Q + S$, the order of $j(P)$ is forced to be divisible by ℓ, a contradiction to S being non-zero.

Remark. Note that because of Proposition 2 of [L], Theorem 1 is not true without the assumption that A is simple.

4.2. Theorem 2. Proof

The proof of Theorem 2 is easily accomplished using Theorem 1 and Lemma 6. First note that by the hypothesis of Theorem 2, for almost all places v of K, the order of $\phi(P) \bmod v$ divides the order of $P \bmod v$: thus we are in a position to apply Theorem 1. Choose a torsion-free subgroup B of finite index in $A(K)$ that is preserved by $\mathrm{End}_K(A)$, the latter being an order in a division algebra as A is simple. We deduce from Theorem 1 that for any $P \in B$ there is an K-endomorphism j_P of A such that $\phi(P) = j_P(P)$. From Lemma 6, we may conclude that j_P can be chosen to be independent of P (in fact *is* independent of P as A is simple): thus there is a K-endomorphism j of A such that $\phi(P) = j(P)$ for all $P \in B$. The last line of the theorem follows as in the case when $A(K)$ is torsion-free we can take $B = A(K)$. This finishes the proof of Theorem 2.

5. Rigidity for arithmetic groups

We begin with the following result for tori.

Proposition 1. *Given homomorphism* $\phi : \mathcal{O}_K^* \to \mathcal{O}_K^*$ *that reduces* $\bmod v$ *for almost all places* v *of a number field* K, *then* ϕ *is induced by the* m*th power map for some integer* m.

Proof. The proof is a direct consequence of Theorem 1 of [CS] and the fact that any finite subgroup of K^* is cyclic. □

We next have the following theorem for arithmetic groups.

Theorem 4. *Let* Γ *be a subgroup of* $\mathrm{SL}(2, \mathbb{Z})$ *of finite index. Let* ϕ *be a non-trivial homomorphism of* Γ *into itself. Assume that for all primes* p *in an infinite set* S *of primes,* ϕ *factors to give a homomorphism* $\phi_p : \mathrm{SL}(2, \mathbb{Z}/p) \to \mathrm{SL}(2, \mathbb{Z}/p)$

$$\begin{array}{ccc} \Gamma & \xrightarrow{\phi} & \Gamma \\ \downarrow & & \downarrow \\ \mathrm{SL}(2, \mathbb{Z}/p) & \xrightarrow{\phi_p} & \mathrm{SL}(2, \mathbb{Z}/p). \end{array}$$

Then ϕ is an automorphism of Γ which is the restriction to Γ of the inner-conjugation action of an element in $\mathrm{GL}(2,\mathbb{Q})$.

Proof. Let B be the ring which is the direct product of $\mathbb{Z}/p$ for all p in S. Clearly $\mathbb{Z}$ is a subring of B, and there is thus an injective homomorphism from $\mathrm{SL}(2,\mathbb{Z})$ to $\mathrm{SL}(2,B)$. Since there is an injective homomorphism from $\mathrm{SL}(2,\mathbb{Z})$ to $\mathrm{SL}(2,B)$ for B, the direct product of *any* infinite set of primes, it is clear that ϕ_p can be trivial for at most finitely many p in S. After replacing S by this slightly smaller set, we assume that ϕ_p is surjective for all p in S, and hence the ϕ_p are given by the inner-conjugation action of an element g_p in $\mathrm{GL}(2,\mathbb{Z}/p)$. Here we are using the well-known facts:

1. any surjective homomorphism of $\mathrm{SL}(2,\mathbb{Z}/p)$ into itself is given by the inner-conjugation of an element of $\mathrm{GL}(2,\mathbb{Z}/p)$.
2. any homomorphism of $\mathrm{SL}(2,\mathbb{Z}/p)$ into itself is either trivial or is surjective if $p>3$.

From this we see that the representations $\phi:\Gamma\to\mathrm{GL}_2(\mathbb{Q})$ and the "identity" representation $\mathrm{id}:\Gamma\to\mathrm{GL}_2(\mathbb{Q})$ have the same trace. Further the second representation is irreducible. From this we conclude that ϕ and id are conjugate by an element of $\mathrm{GL}_2(\mathbb{Q})$, i.e., ϕ is the restriction to Γ of an inner-conjugation action on $\mathrm{GL}_2(\mathbb{Q})$. (In particular, this inner-conjugation takes Γ into itself.) By comparing covolumes of Γ and $\phi(\Gamma)$, we see that ϕ is an automorphism of Γ. □

Remarks. (1) The above proof is due to Serre; we had a different proof in an earlier version.

(2) To deduce rigidity results for SL_2 one just needs that the abstract homomorphism specialises for any infinite set of primes rather than for almost all or even a positive density of primes which is crucial for abelian varieties.

(3) The proof works for $\mathrm{SL}(n,\mathbb{Z})$ for any n to say that if ϕ is a homomorphism of a subgroup of finite index of $\mathrm{SL}(n,\mathbb{Z})$ onto another subgroup of finite index $\mathrm{SL}(n,\mathbb{Z})$ which specialises for infinitely many primes p to give a homomorphism of $\mathrm{SL}(n,\mathbb{Z}/p)$ to itself, then ϕ is algebraic. (We recall that an automorphism of $\mathrm{SL}(n,\mathbb{Z}/p)$ is generated by inner automorphism from $\mathrm{GL}(n,\mathbb{Z}/p)$, and the automorphism $A\to{}^tA^{-1}$.) The proof above works also for lattices in $\mathrm{SL}_2(\mathbb{R})$ constructed using quaternion division algebras.

(4) The point of Theorem 4 is that although abstract homomorphism of Γ into itself are in general not algebraic, those which reduce mod p for infinitely many p are algebraic. (*Rigidity theorems* in Lie groups roughly say that for a lattice Γ in a Lie group G of rank greater than 1, an abstract homomorphism of Γ into G is already algebraic.)

The following theorem when combined with Theorem 4, proves that for a subgroup Γ of finite index in $\mathrm{SL}(2,\mathbb{Z})$, any homomorphism of Γ into itself which extends to $\mathrm{SL}(2,B)$ for $B=\prod_{p\in T}\mathbb{Z}/p$, T an infinite set of primes, must be given by an inner-conjugation action by an element of $\mathrm{GL}(2,\mathbb{Q})$, giving a different perspective to the earlier theorem.

Theorem 5. *Let G be any simply connected, split, semisimple algebraic group over $\mathbb{Q}$. Then any homomorphism of $G(B)$ to itself where B is the product of $\mathbb{Z}/p$ for primes p belonging to a set T that may be finite or infinite (and contains only sufficiently large primes) is factorisable, i.e., any homomorphism f from $G(B)$ to itself is of the form $\prod_{p\in B} f_p$ for certain homomorphisms f_p from $G(\mathbb{Z}/p)$ to itself.*

Proof. We will accomplish the proof of this theorem in several steps.

1. Any homomorphism from $G(\mathbb{Z}/p)$ to $G(\mathbb{Z}/q)$, p not q is trivial (for p a sufficiently large prime but q arbitrary).

   Assume that the mapping is non-trivial. Then as $G(\mathbb{Z}/p)$ is a simple group modulo its centre, any homomorphism from $G(\mathbb{Z}/p)$ to $G(\mathbb{Z}/q)$ must be injective when restricted to unipotent elements in $G(\mathbb{Z}/p)$. Because p is not q, image of a unipotent element in $G(\mathbb{Z}/p)$ cannot have a unipotent component in the Jordan decomposition in $G(\mathbb{Z}/q)$. So image of any unipotent element in $G(\mathbb{Z}/p)$ is semi-simple in $G(\mathbb{Z}/q)$.

   Note that a unipotent in $\mathrm{SL}_2(\mathbb{Z}/p)$ has many powers that are conjugate to itself. By Jacobson–Morozov (which is applicable since we are looking only at large primes), the same holds good about non-trivial unipotents in $G(\mathbb{Z}/p)$. Hence the image of a non-trivial unipotent in $G(\mathbb{Z}/p)$ too will have many distinct powers that are conjugate to itself. But a semi-simple element in $G(\mathbb{Z}/q)$ has at most $|W|$ many powers that are conjugate to itself, where $|W|$ denotes the order of the Weyl group of G, completing the proof of this step.
2. Step 1 proves that any homomorphism from $G(B)$ to itself when restricted to direct sum is factorisable. However going from direct sum to direct product needs some more arguments and essentially the following step suffices.
3. Any homomorphism from $G(B^S)$ to $G(\mathbb{Z}/p)$ must be trivial for some finite set S (depending on p) of primes in B where S is the set of prime divisors of $d = |G(\mathbb{Z}/p)|$, and B^S denotes the subring of B in which primes in S are omitted.

   We first prove that a unipotent in $G(B^S)$ must go trivially to $G(\mathbb{Z}/p)$. Again by Jacobson–Morozov (applied to the ring B^S which is a product of fields), this would follow if we can prove that under any homomorphism from $\mathrm{SL}_2(B^S)$ to $G(\mathbb{Z}/p)$, any unipotent in $\mathrm{SL}_2(B^S)$ must go trivially in $G(\mathbb{Z}/p)$. But this follows because multiplication by d is an isomorphism on B^S whereas multiplication by d, i.e., raising by the dth power takes any element of $G(\mathbb{Z}/p)$ to the trivial element.

   We will be done if we can prove that unipotents in $G(B)$, for any ring B which is a product of fields, generates $G(B)$. (This step is not true for an arbitrary ring B, but is true here as we will see below when B is a product of fields.)
4. For $\mathscr{B}$ any Borel subgroup in G defined over $\mathbb{Q}$, any element of $\mathscr{B}(B)$ belongs to the group generated by the unipotents in $G(B)$. For this it suffices to prove that for a torus T contained in $\mathscr{B}$, and defined over $\mathbb{Q}$, elements of $T(B)$ belong to the subgroup generated by the unipotents in $G(B)$.

   For $\mathrm{SL}_2(B)$, this follows from the following matrix identity which expresses a diagonal element of SL_2 as a product of 4 unipotent matrices. We have taken this

identity from Deligne's article in *Modular functions of one variable II*, Springer Lecture Notes in Mathematics, vol. 349:

$$\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & -a^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -(a-1)/a & 1 \end{pmatrix}.$$

As G is simply connected, any element of $T(B)$ is a product of elements of one-dimensional tori in $T(B)$ arising out of the image of the diagonal torus in SL_2 under mappings of SL_2 to G corresponding to the simple roots.

5. Unipotents in $G(B)$ generate $G(B)$.

   This follows from step 4 combined with Bruhat decomposition (applied component-wise to write $g = (g_p)$ as $(u_p w_p b_p)$) and the fact that any element of the Weyl group is a product of unipotent elements, over a set of size bounded independent of p.

6. It follows from steps 1 and 3 that any homomorphism from $G(B)$ to $G(\mathbb{Z}/p)$ is trivial on $G(B^p)$ (where B^p denotes the subring of B in which the factor corresponding to $\mathbb{Z}/p$ is omitted), hence we have proved that any homomorphism from $G(B)$ to itself is factorisable. □

Acknowledgments

We thank D. Bertrand, K. Ribet, and J.-P. Serre for helpful correspondence, and the referee for detailed comments helping improve the exposition of this work.

References

[B] D. Bertrand, Galois representations and transcendental numbers, in: New Advances in Transcendence Theory, Proceedings of the 1986 Conference in Durham, A. Baker (Ed.), Cambridge University Press, Cambridge.

[Bo] F. Bogomolov, Sur l'algébricité des représentations l-adiques, C. R. Acad. Sci. Paris Sér. A-B 290 (15) (1980) 701–703.

[CS] C. Corrales, R. Schoof, The support problem and its elliptic analogue, J. Number Theory 64 (1997) 276–290.

[K] C. Khare, Compatible systems of mod p galois representations and Hecke characters, Math. Res. Lett. 10 (2003) 71–83.

[L] M. Larsen, The support problem for abelian varieties, J. Number Theory 101 (2003) 398–403.