On the Order of the Reduction of a Point on an Abelian Variety

Richard PINK*

November 27, 2003

Abstract

Consider a point of infinite order on an abelian variety over a number field. Then its reduction at any place v of good reduction is a torsion point. For most of this paper we fix a rational prime ℓ and study how the ℓ-part of this reduction varies with v. Under suitable conditions we prove various statements on this ℓ-part for all v in a set of positive Dirichlet density: for example that its order is a fixed power of ℓ, that its order is non-trivial for the reductions of finitely many points, or that its order is larger than a certain explicit value that varies with v.

By similar methods we prove that for all v in a set of positive Dirichlet density the reduction of a given abelian variety possesses no non-trivial supersingular abelian subvariety.

Mathematics Subject Classification: 14K15 (11R45)
Keywords: abelian varieties, rational points, reduction, Galois groups, density theorems

0 Introduction

Consider an abelian variety A over a number field K and a rational point of infinite order $a \in A(K)$. Then the reduction a_v of a at any place v of good reduction is defined over the finite residue field k_v and is therefore a torsion point. It is natural to ask how a_v varies with v. For most of this paper we fix a rational prime ℓ and study the ℓ-part of a_v. Since for $v \nmid \ell$ any ℓ-power torsion point over $\bar{k}_v$ possesses a unique ℓ-power torsion lift to $A(\bar{K})$, one can try to translate this question into one over $\bar{K}$. The main player in this game is the group

$$\ell^{-\infty}(\mathbb{Z}a) \;:=\; \bigl\{x \in A(\bar{K}) \bigm| \exists n \geq 0 : \ell^n x \in \mathbb{Z}a\bigr\}.$$

This group is a natural extension of $\mathbb{Z}[1/\ell]$ with the group of ℓ-power torsion points

$$A[\ell^\infty] \;:=\; \bigl\{x \in A(\bar{K}) \bigm| \exists n \geq 0 : \ell^n x = 0\bigr\}.$$

The latter group has been studied extensively by means of the Galois representation on the associated ℓ-adic Tate module $T_\ell(A)$. The former group also gives rise to a Tate module $T_\ell(A, a)$ which is an extension of $T_\ell(A)$ by $\mathbb{Z}_\ell$. It is a special case of the Tate modules of 1-motives introduced by Deligne [7, §10.1]. Let $\Gamma_\ell \subset \mathrm{Aut}_{\mathbb{Z}_\ell}\bigl(T_\ell(A)\bigr)$ and $\tilde{\Gamma}_\ell \subset \mathrm{Aut}_{\mathbb{Z}_\ell}\bigl(T_\ell(A, a)\bigr)$ be the respective images of $\mathrm{Gal}(\bar{K}/K)$.

In Section 1 we review some known general facts about Γ_ℓ and its Zariski closure. We also prove in Corollary 1.7 that for all v in a set of positive Dirichlet density the

*Dept. of Mathematics, ETH-Zentrum, CH-8092 Zürich, Switzerland, pink@math.ethz.ch

reduction of A possesses no non-trivial supersingular abelian subvariety. Although this statement has no direct relation with the results on a_v, the respective methods of proof have much in common.

General structural properties of $\tilde{\Gamma}_\ell$ are then discussed in Section 2. In particular we recall Theorem 2.8 from the Kummer theory of A which states that $\tilde{\Gamma}_\ell$ is an extension of Γ_ℓ by an open subgroup of $T_\ell(B)$, where B is the identity component of the Zariski closure of $\mathbb{Z}a$. This result is essentially due to Ribet [13], though in the case we need the proof was worked out only by Hindry [9, §2, Prop. 1].

In Section 3 we then show how the ℓ-part of a_v is determined by the action of the Frobenius element Frob_v on $\ell^{-\infty}(\mathbb{Z}a)$. Any question about this ℓ-part can thus be translated completely into a question on the group $\tilde{\Gamma}_\ell$.

In Section 4 we answer some of these questions. In all cases we prove that a certain behavior occurs for all places v of K in a set of Dirichlet density > 0. For example, in Corollary 4.3 we show that under mild conditions every power of ℓ occurs as the order of the ℓ-part of a_v. In Theorem 4.4 we prove that for finitely many given points a_i of infinite order, the ℓ-parts of their reductions $a_{i,v}$ can be made simultaneously non-trivial on a set of positive Dirichlet density. Theorem 4.7 generalizes this result in another direction: Let $f(T) \in \mathbb{Z}[T]$ be any polynomial which is a product of cyclotomic polynomials and a power of T. Let p_v denote the residue characteristic at v. Then for suitable ℓ, the ℓ-parts of all $f(p_v)a_{i,v}$ can be made simultaneously non-trivial on a set of positive Dirichlet density.

In the final section 5 we use these theorems to derive two density results on the $a_{i,v}$ which no longer refer to any particular prime ℓ. These results as well as Corollary 1.7 are needed in joint work with Damian Roessler [12] and provided the motivation for the present paper.[1] Theorem 5.1 can also be deduced from work by Wong [16] who, instead of studying when the ℓ-part of a_v is zero, considers the dual question of when a_v lies in $\ell \cdot A_v(k_v)$. Related questions are addressed in work by Corrales-Rodrigáñez and Schoof [6], Khare and Prasad [10], and Larsen [11].

1 The ℓ-adic Galois group associated to an abelian variety

Let K be a number field and $\bar{K}$ an algebraic closure of K. Consider an abelian variety A of dimension g over K and a rational prime ℓ. Then

$$A[\ell^\infty] \;:=\; \big\{x \in A(\bar{K}) \;\big|\; \exists n \geq 0 : \ell^n x = 0\big\}$$

is a discrete group isomorphic to $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$ with a continuous action of $\mathrm{Gal}(\bar{K}/K)$. One usually describes this action via the ℓ-adic Tate module

$$T_\ell(A) \;:=\; \mathrm{Hom}\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A[\ell^\infty]\big) \;\cong\; \mathbb{Z}_\ell^{2g},$$

which possesses a continuous Galois representation

$$\rho_\ell : \; \mathrm{Gal}(\bar{K}/K) \;\longrightarrow\; \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \;\cong\; \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

We are interested in its image $\Gamma_\ell := \rho_\ell\big(\mathrm{Gal}(\bar{K}/K)\big)$, which is a compact subgroup of $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$. Much can be said about Γ_ℓ by means of its Zariski closure $G_\ell \subset \mathrm{GL}_{2g,\mathbb{Q}_\ell}$. This is a linear algebraic group over $\mathbb{Q}_\ell$ with a natural faithful representation on the rational Tate module

$$V_\ell(A) \;:=\; T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \;\cong\; \mathbb{Q}_\ell^{2g}.$$

The following general facts are known about G_ℓ.

[1] The author wishes to thank Damian Roessler for the very fruitful ongoing collaboration.

Theorem 1.1 *(a) The action of G_ℓ on $V_\ell(A)$ is semisimple and the natural homomorphism*

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \longrightarrow \mathrm{End}_{\mathbb{Q}_\ell, G_\ell}\big(V_\ell(A)\big)$$

is an isomorphism.

(b) G_ℓ is a reductive group.

(c) Γ_ℓ is an open subgroup of $G_\ell(\mathbb{Q}_\ell)$.

Proof. By the definition of G_ℓ the statements in (a) are equivalent to the corresponding ones with Γ_ℓ in place of G_ℓ, which were proved by Faltings [8, Th. 3–4]. Part (b) follows from the first statement in (a). Part (c) is a theorem of Bogomolov [4], [3]. **q.e.d.**

By Galois theory every open subgroup of Γ_ℓ corresponds to a finite extension of K within $\bar{K}$, and replacing K by that extension amounts to replacing Γ_ℓ by the corresponding subgroup. In particular, let G_ℓ° denote the identity component of G_ℓ. Then replacing Γ_ℓ by any open subgroup of $\Gamma_\ell \cap G_\ell^\circ$ has the effect of replacing G_ℓ by G_ℓ°; and thereafter G_ℓ will be connected.

Now consider any finite place v of K and let p_v denote the characteristic of the finite residue field k_v. If $v \nmid \ell$ and A has good reduction at v, it is known that the restriction of ρ_ℓ to any inertia group above v is trivial. Let Frob_v be any element of a decomposition group at v which acts by taking $|k_v|^{\mathrm{th}}$ powers modulo v. Then the conjugacy class of $\rho_\ell(\mathrm{Frob}_v)$ depends only on v and is known to be semisimple, and its characteristic polynomial on $V_\ell(A)$ is known to have coefficients in $\mathbb{Z}$ and to be independent of ℓ.

Choose any semisimple element $t_v \in \mathrm{GL}_{2g}(\mathbb{Q})$ whose characteristic polynomial is equal to that of $\rho_\ell(\mathrm{Frob}_v)$. Let $T_v \subset \mathrm{GL}_{2g,\mathbb{Q}}$ be the Zariski closure of the subgroup generated by t_v. The construction implies that the identity component of T_v is a torus and its $\mathrm{GL}_{2g}(\mathbb{Q})$-conjugacy class depends only on v. Following Serre [14] it is called the *Frobenius torus at v*. Moreover, for any $\ell \neq p_v$ there is a unique conjugate of $T_{v,\mathbb{Q}_\ell}$ by an element of $\mathrm{GL}_{2g}(\mathbb{Q}_\ell)$ which lies in G_ℓ, such that t_v is mapped to $\rho_\ell(\mathrm{Frob}_v)$. Serre [14, §5, pp.12–13] proves:

Theorem 1.2 *If G_ℓ is connected, then for all places v in a set of Dirichlet density* 1 *the group T_v itself is a torus and $T_{v,\mathbb{Q}_\ell}$ is conjugate under* $\mathrm{GL}_{2g}(\mathbb{Q}_\ell)$ *to a maximal torus of G_ℓ.*

Corollary 1.3 *There exists a set of rational primes ℓ of positive Dirichlet density for which G_ℓ splits over $\mathbb{Q}_\ell$.*

Proof. Let T_v be any Frobenius torus as in Theorem 1.2. Choose a finite extension F of $\bar{\mathbb{Q}}$ such that $T_{v,F}$ splits. Then the set of rational primes ℓ which split completely in F has positive Dirichlet density, and for each of them $T_{v,\mathbb{Q}_\ell}$ splits. Since $T_{v,\mathbb{Q}_\ell}$ is conjugate to a maximal torus of G_ℓ, this shows that G_ℓ splits. **q.e.d.**

Next any polarization of A induces a Galois equivariant perfect alternating pairing $V_\ell(A) \times V_\ell(A) \to \mathbb{Q}_\ell(1)$, where $\mathrm{Gal}(\bar{K}/K)$ acts on $\mathbb{Q}_\ell(1)$ through the cyclotomic character. It follows that Γ_ℓ is contained in the group of symplectic similitudes $\mathrm{CSp}_{2g}(\mathbb{Q}_\ell)$. Let $\mu : \mathrm{CSp}_{2g} \to \mathbb{G}_m$ denote the multiplier map; then $\mu\rho_\ell : \mathrm{Gal}(\bar{K}/K) \to \mathbb{Z}_\ell^*$ is the cyclotomic character. The definition of G_ℓ implies that $G_\ell \subset \mathrm{CSp}_{2g,\mathbb{Q}_\ell}$; hence μ defines an algebraic character of G_ℓ.

Proposition 1.4 *Consider a maximal torus S_ℓ of G_ℓ and any weight χ of S_ℓ on $V_\ell(A)$. Then μ and χ are $\mathbb{Q}$-linearly independent in the character group of S_ℓ.*

Proof. The perfect pairing implies that there exists a weight χ^* of S_ℓ on $V_\ell(A)$ such that $\chi\chi^* = \mu$. Both χ and χ^* are non-trivial, because the corresponding Frobenius eigenvalues have complex absolute value > 1. Now by the Hodge-Tate decomposition there exists a cocharacter λ of S_ℓ whose weights on $V_\ell(A)$ are 0 and 1 and whose weight on $\mathbb{Q}_\ell(1)$ is 1; see for instance Serre [14, §5, pp.11–12]. For any such λ we have

$$\langle \chi, \lambda \rangle + \langle \chi^*, \lambda \rangle = \langle \chi\chi^*, \lambda \rangle = \langle \mu, \lambda \rangle = 1,$$

and one of the summands is 0 and the other 1. This implies that χ and χ^* cannot be non-zero rational multiples of each other. Since they are both non-trivial characters, they must be $\mathbb{Q}$-linearly independent. Equivalently χ and $\mu = \chi\chi^*$ are $\mathbb{Q}$-linearly independent, as desired. **q.e.d.**

Proposition 1.5 *Suppose that $A = A_1 \times \ldots \times A_d$ for non-zero abelian varieties $A_1, \ldots, A_d$. Consider a maximal torus S_ℓ of G_ℓ. Then there exist weights χ_i of S_ℓ on $V_\ell(A_i)$ so that μ is $\mathbb{Q}$-linearly independent of $\chi_1, \ldots, \chi_d$.*

Proof. By the Hodge-Tate decomposition, see [14, §5, pp.11–12], there exists a cocharacter λ of S_ℓ which on every $V_\ell(A_i)$ has the weights 0 and 1 with multiplicity $\dim A_i$ each, and whose weight on $\mathbb{Q}_\ell(1)$ is 1. So we can choose each χ_i such that $\langle \chi_i, \lambda \rangle$, the weight of the χ_i-eigenspace in the Hodge-Tate decomposition, is zero. Then for any weight χ which is a $\mathbb{Q}$-linear combination of the χ_i, we still have $\langle \chi, \lambda \rangle = 0$. But $\langle \mu, \lambda \rangle = 1$; hence μ is not a $\mathbb{Q}$-linear combination of the χ_i. **q.e.d.**

We finish this section with a first application of Proposition 1.4, which will not be used in the rest of the paper.

Theorem 1.6 *If G_ℓ is connected, the set of finite places v of K where the reduction of A does not possess a non-trivial supersingular abelian subvariety has Dirichlet density* 1.

Proof. By Theorem 1.2 it suffices to consider those places $v \nmid \ell$ of K for which $T_{v,\mathbb{Q}_\ell}$ is conjugate to a maximal torus S_ℓ of G_ℓ. Let v be such a place and suppose that the corresponding reduction A_v of A possesses a non-trivial supersingular abelian subvariety B_v. Then any eigenvalue of Frob_v on $V_\ell(B_v)$ has the form $\sqrt{|k_v|}$ times a root of unity, while the eigenvalue on $\mathbb{Q}_\ell(1)$ is $|k_v|$. Let χ be the weight of S_ℓ on $V_\ell(A)$ corresponding to that eigenvalue on $V_\ell(B_v) \subset V_\ell(A_v)$, and let n be the order of that root of unity. Then the values of χ^{2n} and μ^n on $\rho_\ell(\mathrm{Frob}_v)$ coincide. But by the construction of the Frobenius torus the element $\rho_\ell(\mathrm{Frob}_v)$ generates a Zariski dense subgroup of S_ℓ. Thus χ^{2n} and μ^n are equal as characters of S_ℓ, which contradicts their linear independence from Proposition 1.4. This shows that A_v does not possess a non-trivial supersingular abelian subvariety, as desired. **q.e.d.**

Corollary 1.7 *Let A be an abelian variety over a number field K. Then there exists a finite extension L of K such that for all finite places of L in a set of Dirichlet density* 1 *the reduction of A does not possess a non-trivial supersingular abelian subvariety.*

Proof. Choose an arbitrary rational prime ℓ and a finite Galois extension L of K over which G_ℓ becomes connected, and apply Theorem 1.6. **q.e.d.**

2 The ℓ-adic Galois group associated to an abelian variety with a point

Now fix a rational point of infinite order $a \in A(K)$ and set

$$\ell^{-\infty}(\mathbb{Z}a) \;:=\; \bigl\{x \in A(\bar{K}) \bigm| \exists n \geq 0 : \ell^n x \in \mathbb{Z}a\bigr\}.$$

Then we have a natural short exact sequence of discrete groups

$$0 \longrightarrow A[\ell^\infty] \longrightarrow \ell^{-\infty}(\mathbb{Z}a) \xrightarrow{a \mapsto 1} \mathbb{Z}[1/\ell] \longrightarrow 0. \tag{2.1}$$

Any choice of a compatible system of ℓ-power roots of a determines a splitting $\lambda : \mathbb{Z}[1/\ell] \to \ell^{-\infty}(\mathbb{Z}a)$ satisfying $\lambda(1) = a$. We will call such a splitting *special*. Two special splittings differ by an element of

$$\mathrm{Hom}\bigl(\mathbb{Z}[1/\ell]\,/\,\mathbb{Z}, A[\ell^\infty]\bigr) \;\cong\; \mathrm{Hom}\bigl(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A[\ell^\infty]\bigr) \;=\; T_\ell(A).$$

By contrast, two general splittings differ by an element of

$$\begin{aligned} \mathrm{Hom}\bigl(\mathbb{Z}[1/\ell], A[\ell^\infty]\bigr) \;&=\; \bigcup_{r\geq 0} \mathrm{Hom}\bigl(\mathbb{Z}[1/\ell]\,/\,\ell^r\mathbb{Z}, A[\ell^\infty]\bigr) \\ &\cong\; \bigcup_{r\geq 0} \ell^{-r}\,\mathrm{Hom}\bigl(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A[\ell^\infty]\bigr) \\ &=\; \bigcup_{r\geq 0} \ell^{-r} T_\ell(A) \;=\; V_\ell(A)\,. \end{aligned} \tag{2.2}$$

The sequence 2.1 is equivariant under the natural continuous action of $\mathrm{Gal}(\bar{K}/K)$, where the action on $\mathbb{Z}[1/\ell]$ is trivial. It is useful to describe this action via an associated Tate module. For this note that $\ell^{-\infty}(\mathbb{Z}a)/\mathbb{Z}a$ is isomorphic to $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g+1}$; hence

$$T_\ell(A,a) \;:=\; \mathrm{Hom}\bigl(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \ell^{-\infty}(\mathbb{Z}a)/\mathbb{Z}a\bigr)$$

is isomorphic to $\mathbb{Z}_\ell^{2g+1}$ and sits in a short exact sequence

$$0 \longrightarrow T_\ell(A) \longrightarrow T_\ell(A,a) \longrightarrow \mathbb{Z}_\ell \longrightarrow 0. \tag{2.3}$$

Any special splitting of 2.1 determines a splitting of 2.3, i.e., an isomorphism $T_\ell(A,a) \cong T_\ell(A) \oplus \mathbb{Z}_\ell$. We will write any such decomposition in terms of column vectors. Then the natural Galois representation on $T_\ell(A,a)$ has the form

$$\tilde{\rho}_\ell = \begin{pmatrix} \rho_\ell & * \\ 0 & 1 \end{pmatrix} :\; \mathrm{Gal}(\bar{K}/K) \longrightarrow \begin{pmatrix} \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) & T_\ell(A) \\ 0 & 1 \end{pmatrix} \cong \begin{pmatrix} \mathrm{GL}_{2g}(\mathbb{Z}_\ell) & \mathbb{Z}_\ell^{2g} \\ 0 & 1 \end{pmatrix}.$$

The construction implies that left multiplication by the same matrices also describes the Galois action on $\ell^{-\infty}(\mathbb{Z}a) \cong A[\ell^\infty] \oplus \mathbb{Z}[1/\ell]$. We are interested in the image

$$\tilde{\Gamma}_\ell \;:=\; \tilde{\rho}_\ell\bigl(\mathrm{Gal}(\bar{K}/K)\bigr) \;\subset\; \begin{pmatrix} \Gamma_\ell & T_\ell(A) \\ 0 & 1 \end{pmatrix}.$$

Letting $N_\ell := \tilde{\Gamma}_\ell \cap T_\ell(A)$ denote its intersection with the upper right corner, we obtain a natural short exact sequence

$$0 \longrightarrow N_\ell \longrightarrow \tilde{\Gamma}_\ell \longrightarrow \Gamma_\ell \longrightarrow 1. \tag{2.4}$$

As with Γ_ℓ we will study $\tilde{\Gamma}_\ell$ with the help of its Zariski closure $\tilde{G}_\ell$, which is a linear algebraic group over $\mathbb{Q}_\ell$ with a natural faithful representation on

$$V_\ell(A,a) \;:=\; T_\ell(A,a) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \;\cong\; \mathbb{Q}_\ell^{2g+1}.$$

By construction we have a natural short exact sequence

$$0 \longrightarrow U_\ell \longrightarrow \tilde{G}_\ell \longrightarrow G_\ell \longrightarrow 1$$

where U_ℓ is an algebraic subgroup of the vector group $V_\ell(A)$. Since G_ℓ is reductive by Theorem 1.1 (b), the subgroup U_ℓ is simply the unipotent radical of $\tilde{G}_\ell$.

Proposition 2.5 *$\tilde{\Gamma}_\ell$ is open in $\tilde{G}_\ell(\mathbb{Q}_\ell)$ and N_ℓ open in $U_\ell(\mathbb{Q}_\ell)$.*

Proof. By construction we have an inclusion of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_\ell(\mathbb{Q}_\ell) & \longrightarrow & \tilde{G}_\ell(\mathbb{Q}_\ell) & \longrightarrow & G_\ell(\mathbb{Q}_\ell) & \longrightarrow & 1 \\ & & \cup & & \cup & & \cup & & \\ 0 & \longrightarrow & N_\ell & \longrightarrow & \tilde{\Gamma}_\ell & \longrightarrow & \Gamma_\ell & \longrightarrow & 1\,. \end{array}$$

All these groups can be viewed as ℓ-adic Lie groups, and by a theorem of Chevalley [5, Ch. II, Cor. 7.9] the Zariski density of $\tilde{\Gamma}_\ell$ implies

$$\big[\operatorname{Lie}\tilde{G}_\ell, \operatorname{Lie}\tilde{G}_\ell\big] \;\subset\; \operatorname{Lie}\tilde{\Gamma}_\ell\,.$$

On the other hand $V_\ell(A)$ does not contain the trivial representation of G_ℓ, because all Frobenius eigenvalues have complex absolute value > 1. Thus $U_\ell \cong \operatorname{Lie} U_\ell$ does not contain the trivial representation of G_ℓ, which implies that

$$\operatorname{Lie} U_\ell \;=\; \big[\operatorname{Lie}\tilde{G}_\ell, \operatorname{Lie} U_\ell\big] \;\subset\; \big[\operatorname{Lie}\tilde{G}_\ell, \operatorname{Lie}\tilde{G}_\ell\big] \;\subset\; \operatorname{Lie}\tilde{\Gamma}_\ell\,.$$

Since moreover $\operatorname{Lie}\Gamma_\ell = \operatorname{Lie} G_\ell$ by Theorem 1.1 (c), we deduce that $\operatorname{Lie}\tilde{\Gamma}_\ell = \operatorname{Lie}\tilde{G}_\ell$. Thus $\tilde{\Gamma}_\ell$ is open in $\tilde{G}_\ell(\mathbb{Q}_\ell)$, and therefore N_ℓ is open in $U_\ell(\mathbb{Q}_\ell)$, as desired. **q.e.d.**

Proposition 2.6 *After replacing K by a suitable finite extension there exists a splitting of 2.1, not necessarily special, such that*

$$\tilde{\Gamma}_\ell \;=\; \begin{pmatrix} \Gamma_\ell & N_\ell \\ 0 & 1 \end{pmatrix}.$$

Proof. Choose any Levi decomposition $\tilde{G}_\ell = G_\ell \ltimes U_\ell$ and consider the short exact sequence

$$0 \longrightarrow V_\ell(A) \longrightarrow V_\ell(A, a) \longrightarrow \mathbb{Q}_\ell \longrightarrow 0 \tag{2.7}$$

deduced from 2.3 by tensoring with $\mathbb{Q}_\ell$. As G_ℓ is reductive, acts trivially on $\mathbb{Q}_\ell$, and non-trivially on every non-zero subspace of $V_\ell(A)$, the sequence 2.7 possesses a unique splitting that is invariant under the Levi subgroup G_ℓ. On the other hand take any splitting λ of 2.1. Then the induced splitting of 2.7 differs from the Levi invariant splitting by some element of $V_\ell(A)$. Changing λ by the same element thus shows that the Levi invariant splitting of 2.7 comes from some splitting of 2.1, though not necessarily from a special one. With respect to this splitting the decomposition $\tilde{G}_\ell = G_\ell \ltimes U_\ell$ is the same as that in terms of formal matrices

$$\tilde{G}_\ell \;=\; \begin{pmatrix} G_\ell & U_\ell \\ 0 & 1 \end{pmatrix}.$$

Finally Proposition 2.5 implies that

$$\big(G_\ell(\mathbb{Q}_\ell) \cap \tilde{\Gamma}_\ell\big) \ltimes \big(U_\ell(\mathbb{Q}_\ell) \cap \tilde{\Gamma}_\ell\big)$$

is an open subgroup of $\tilde{G}_\ell(\mathbb{Q}_\ell)$ and hence of $\tilde{\Gamma}_\ell$. After replacing K by the corresponding finite extension $\tilde{\Gamma}_\ell$ itself is such a semidirect product, as desired. **q.e.d.**

Theorem 2.8 *Let B be the identity component of the Zariski closure of $\mathbb{Z}a$. Then N_ℓ is open in $T_\ell(B) \subset T_\ell(A)$ and we have $U_\ell = V_\ell(B) \subset V_\ell(A)$.*

Proof. This is a special case of a theorem essentially due to Ribet [13] on the Kummer theory of A, itself depending on results of Faltings [8] and Serre [15] as well as the Mordell-Weil theorem, and following a method first used by Bashmakov [1]. The case we need was formulated by Bertrand [2, Th. 2] and worked out by Hindry [9, §2, Prop. 1].

We begin with two technical reductions required by this reference. First, as the Mordell-Weil group $A(K)$ is finitely generated, the given element a is an integral multiple of an indivisible element $a' \in A(K)$. Replacing a by a' does not change B, and since $\ell^{-\infty}(\mathbb{Z}a) \subset \ell^{-\infty}(\mathbb{Z}a')$ is a subgroup of finite index prime to ℓ, it also changes neither $\tilde{\Gamma}_\ell$ nor N_ℓ nor U_ℓ. Thus without loss of generality we may, and do, assume that a itself is indivisible in $A(K)$. Next let d be the number of connected components of the Zariski closure of $\mathbb{Z}a$. To prove the theorem we may, and do, replace K by its finite extension $K(A[d])$.

Now for any two integers $r \geq s \geq 0$ consider the finite quotients

$$\begin{array}{ccccc} \tilde{\Gamma}_\ell & \twoheadrightarrow & \tilde{\Gamma}_{\ell,r,s} & \subset & \mathrm{GL}_{2g}(\mathbb{Z}/\ell^r\mathbb{Z}) \ltimes T_\ell(A)/\ell^s T_\ell(A) \\ \downarrow & & \downarrow & & \downarrow \\ \Gamma_\ell & \twoheadrightarrow & \Gamma_{\ell,r} & \subset & \mathrm{GL}_{2g}(\mathbb{Z}/\ell^r\mathbb{Z}). \end{array}$$

Then the short exact sequence 2.4 maps onto a short exact sequence

$$0 \longrightarrow N_{\ell,r,s} \longrightarrow \tilde{\Gamma}_{\ell,r,s} \longrightarrow \Gamma_{\ell,r} \longrightarrow 1$$

for some subgroup $N_{\ell,r,s} \subset T_\ell(A)/\ell^s T_\ell(A) \cong A[\ell^s]$. By [9, §2, Prop. 1] this group is a subgroup of $T_\ell(B)/\ell^s T_\ell(B) \cong B[\ell^s]$ whose index is bounded independently of r and s, provided that $r \geq \mathrm{ord}_\ell(d)$. Since N_ℓ is the projective limit of the $N_{\ell,r,s}$ as both r and s go to infinity, this implies that N_ℓ is an open subgroup of $T_\ell(B)$. The second statement follows from this and Proposition 2.5. **q.e.d.**

In particular, since a has infinite order by assumption, Theorem 2.8 implies that $N_\ell \neq 0$. Another direct consequence is:

Corollary 2.9 *N_ℓ is open in $T_\ell(A)$ if and only if $U_\ell = V_\ell(A)$ if and only if $\mathbb{Z}a$ is Zariski dense in A.*

3 The ℓ-part of the reduction at v

Now consider a place $v \nmid \ell$ of K where A has good reduction A_v. Then the restriction of $\tilde{\rho}_\ell$ to any inertia group above v is trivial, and so the conjugacy class of $\rho_\ell(\mathrm{Frob}_v)$ depends only on v. We will show how this conjugacy class determines the ℓ-part of the reduction $a_v \in A_v$ of our fixed point a.

First the condition $v \nmid \ell$ implies that the reduction map induces an isomorphism

$$A[\ell^\infty] \xrightarrow{\sim} A_v(\bar{k}_v)[\ell^\infty].$$

Consider the composite homomorphism

$$\kappa_v : \ \ell^{-\infty}(\mathbb{Z}a) \subset A(\bar{K}) \longrightarrow A_v(\bar{k}_v) \longrightarrow A_v(\bar{k}_v)[\ell^\infty] \cong A[\ell^\infty],$$

where the first arrow is reduction modulo v, the second one is the projection to the ℓ-part, and the isomorphism on the right is the inverse of the reduction map. By construction its restriction to $A[\ell^\infty]$ is the identity, so κ_v induces a splitting of the sequence 2.1. It is important to note that κ_v does not in general correspond to a special splitting. Indeed, it does so if and only if $\kappa_v(a) = 0$, that is, if the ℓ-part of the reduction a_v vanishes.

By construction κ_v is equivariant under the action of Frob_v. Thus the following observation tells us that κ_v is completely determined by the element $\tilde{\rho}_\ell(\mathrm{Frob}_v) \in \tilde{\Gamma}_\ell$.

Proposition 3.1 *For every place $v \nmid \ell$ of K where A has good reduction the homomorphism κ_v is the unique* Frob_v*-equivariant splitting of the sequence 2.1.*

Proof. Any other Frob_v-equivariant splitting $\ell^{-\infty}(\mathbb{Z}a) \to A[\ell^\infty]$ differs from κ_v by a Frob_v-invariant element of $\mathrm{Hom}\big(\mathbb{Z}[1/\ell], A[\ell^\infty]\big)$. By 2.2 the latter space is isomorphic to $V_\ell(A)$. Since all eigenvalues of Frob_v on $V_\ell(A)$ have complex absolute value > 1, its subspace of Frob_v-invariants is zero. Thus κ_v is the unique Frob_v-invariant splitting. **q.e.d.**

To give a precise formula for $\kappa_v(a)$ we fix a special splitting λ of 2.1 and write

$$\tilde{\gamma}_v := \tilde{\rho}_\ell(\mathrm{Frob}_v) = \begin{pmatrix} \gamma_v & n_v \\ 0 & 1 \end{pmatrix}$$

with $\gamma_v = \rho_\ell(\mathrm{Frob}_v) \in \Gamma_\ell \subset \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ and $n_v \in T_\ell(A) \cong \mathbb{Z}_\ell^{2g}$. Since γ_v does not have the eigenvalue 1, we can invert the matrix $\gamma_v - \mathrm{id}$ over $\mathbb{Q}_\ell$ and thus define

$$m_v \ := \ (\gamma_v - \mathrm{id})^{-1} n_v \ \in \ V_\ell(A) \ \cong \ \mathbb{Q}_\ell^{2g}.$$

Let π_ℓ denote the natural composite homomorphism

$$V_\ell(A) \twoheadrightarrow V_\ell(A) \big/ T_\ell(A) \ \cong \ A[\ell^\infty].$$

Proposition 3.2 *We have $\kappa_v(a) = \pi_\ell(m_v)$. In particular the order of the ℓ-part of the reduction a_v is equal to the ℓ-part of the denominator of m_v.*

Proof. The splitting λ induces a decomposition

$$V_\ell(A, a) = V_\ell(A) \oplus \mathbb{Q}_\ell$$

which, as usual, we write in terms of column vectors. A direct calculation then shows that the eigenspace of $\tilde{\gamma}_v$ on $V_\ell(A, a)$ for the eigenvalue 1 is generated by the vector

$$\begin{pmatrix} -m_v \\ 1 \end{pmatrix}.$$

Thus again with respect to the decomposition induced by λ the map

$$\begin{array}{ccccc} \mathbb{Z}[1/\ell] & \longrightarrow & \ell^{-\infty}(\mathbb{Z}a) & = & A[\ell^\infty] \oplus \mathbb{Z}[1/\ell]\,, \\ x & \mapsto & \begin{pmatrix} -\pi_\ell(x m_v) \\ x \end{pmatrix} & & \end{array}$$

defines a $\tilde{\gamma}_v$-equivariant splitting of 2.1. The corresponding $\tilde{\gamma}_v$-equivariant splitting in the other direction

$$A[\ell^\infty] \oplus \mathbb{Z}[1/\ell] \ = \ \ell^{-\infty}(\mathbb{Z}a) \ \longrightarrow \ A[\ell^\infty]$$

is given by

$$\begin{pmatrix} b \\ x \end{pmatrix} \ = \ \begin{pmatrix} b + \pi_\ell(x m_v) \\ 0 \end{pmatrix} + \begin{pmatrix} -\pi_\ell(x m_v) \\ x \end{pmatrix} \ \mapsto \ b + \pi_\ell(x m_v)\,.$$

By Proposition 3.1 this map represents κ_v. Now since λ is a special splitting, the element $a = \lambda(1)$ corresponds to the vector

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

It follows that $\kappa_v(a) = \pi_\ell(m_v)$, as desired. **q.e.d.**

4 Density results for the ℓ-part of the reduction

In this section we derive several statements on the Dirichlet density of the set of places v at which the ℓ-part of the reduction of a has certain properties. For all these statements we can disregard the finite set S of places dividing ℓ or where A has bad reduction.

Theorem 4.1 *Let A be an abelian variety over a number field K and $a \in A(K)$ a rational point of infinite order such that $\mathbb{Z}a$ is Zariski dense in A. Consider a rational prime and a point $b \in A[\ell^\infty]$. Then for all finite places v of K in a set of Dirichlet density > 0 the ℓ-part of the reduction of a is equal to the reduction of b.*

Proof. Choose a special splitting of 2.1 and let U denote the set of elements

$$\tilde{\gamma} = \begin{pmatrix} \gamma & n \\ 0 & 1 \end{pmatrix} \in \tilde{\Gamma}_\ell \subset \begin{pmatrix} \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) & T_\ell(A) \\ 0 & 1 \end{pmatrix}$$

satisfying $\det(\gamma - \mathrm{id}) \neq 0$. Clearly this is an open subset of $\tilde{\Gamma}_\ell$. Next $\tilde{\gamma} \mapsto \pi_\ell\big((\gamma - \mathrm{id})^{-1}n\big)$ defines a continuous function from U to the discrete set $A[\ell^\infty]$. It is therefore locally constant; hence

$$U_b := \left\{ \tilde{\gamma} \in \tilde{\Gamma}_\ell \;\middle|\; \begin{array}{l} \det(\gamma - \mathrm{id}) \neq 0, \text{ and} \\ \pi_\ell\big((\gamma - \mathrm{id})^{-1}n\big) = b \end{array} \right\}$$

is an open subset of $\tilde{\Gamma}_\ell$.

Lemma 4.2 *U_b is non-empty.*

Proof. It suffices to show that the map

$$U \to V_\ell(A), \; \begin{pmatrix} \gamma & n \\ 0 & 1 \end{pmatrix} \mapsto (\gamma - \mathrm{id})^{-1}n$$

is surjective. This statement is invariant under conjugation by $V_\ell(A)$, and it suffices to prove it after replacing K by a finite extension. Thus using Proposition 2.6 we may without loss of generality assume that

$$\tilde{\Gamma}_\ell \;=\; \begin{pmatrix} \Gamma_\ell & N_\ell \\ 0 & 1 \end{pmatrix}.$$

The desired statement is then equivalent to

$$V_\ell(A) \;=\; \bigcup_{\substack{\gamma \in \Gamma_\ell \\ \det(\gamma - \mathrm{id}) \neq 0}} (\gamma - \mathrm{id})^{-1} N_\ell \,.$$

Now N_ℓ is open in $T_\ell(A)$ by Corollary 2.9; hence $\ell^r T_\ell(A) \subset N_\ell$ for some integer r. On the other hand, for every integer $s > 0$ there exists $\gamma \in \Gamma_\ell$ with $\det(\gamma - \mathrm{id}) \neq 0$

such that $\gamma \equiv \mathrm{id} \bmod \ell^s$. Indeed, any power $\rho_\ell(\mathrm{Frob}_v)^m$ for a place $v \notin S$ and m sufficiently divisible has these properties. For this element γ we then have

$$(\gamma - \mathrm{id})T_\ell(A) \ \subset\ \ell^s T_\ell(A) \ \subset\ \ell^{s-r} N_\ell$$

and hence

$$\ell^{r-s} T_\ell(A) \subset (\gamma - \mathrm{id})^{-1} N_\ell.$$

With $s \to \infty$ the desired equality follows. **q.e.d.**

Now take any element $\tilde{\gamma} \in U_b$. By openness there exists an open normal subgroup $\tilde{\Delta} \triangleleft \tilde{\Gamma}_\ell$ such that $\tilde{\gamma}\tilde{\Delta} \subset U_b$. As $\tilde{\Gamma}_\ell/\tilde{\Delta}$ is the Galois group of a finite extension of K, by the Cebotarev density theorem there exists a set of places $v \notin S$ of K of Dirichlet density > 0 for which

$$\tilde{\rho}_\ell(\mathrm{Frob}_v) \equiv \tilde{\gamma} \bmod \tilde{\Delta}.$$

But for all these v we have $\tilde{\rho}_\ell(\mathrm{Frob}_v) \in U_b$, which by Proposition 3.2 implies $\kappa_v(a) = b$. By the definition of κ_v this means that the ℓ-part of the reduction of a is equal to the reduction of b, as desired. **q.e.d.**

Corollary 4.3 *Let A be an abelian variety over a number field K and $a \in A(K)$ a rational point of infinite order such that $\mathbb{Z}a$ is Zariski dense in A. Consider a rational prime and an integer $r \geq 0$. Then for all finite places v of K in a set of Dirichlet density > 0 the ℓ-part of the reduction of a has order ℓ^r.*

Proof. Apply Theorem 4.1 to any point $b \in A[\ell^\infty]$ of order ℓ^r. (This was also partly proved by Khare and Prasad [10, §5, Lemma 4–5]. **q.e.d.**

Theorem 4.4 *For $1 \leq i \leq d$ let A_i be an abelian variety over a number field K and $a_i \in A_i(K)$ a rational point of infinite order. Let ℓ be a rational prime. Then for all finite places v of K in a set of Dirichlet density > 0 the ℓ-part of the reduction of a_i is non-trivial for every i.*

Proof. We apply the results of the preceding sections to $A := A_1 \times \ldots \times A_d$ and $a := (a_1, \ldots, a_d)$. Let $\mathrm{pr}_i :\ A \to A_i$ denote the projection to the i^{th} factor. Then as in the proof of Theorem 4.1

$$U' := \left\{ \tilde{\gamma} \in \tilde{\Gamma}_\ell \;\middle|\; \begin{array}{l} \det(\gamma - \mathrm{id}) \neq 0, \text{ and} \\ \forall i :\ \mathrm{pr}_i\, \pi_\ell\big((\gamma - \mathrm{id})^{-1} n\big) \neq 0 \end{array} \right\}$$

is an open subset of $\tilde{\Gamma}_\ell$, and it suffices to prove:

Lemma 4.5 *U' is non-empty.*

Proof. We may replace K by a finite extension. Thus using Proposition 2.6 we may without loss of generality assume that there exists $m \in V_\ell(A)$ such that

$$\tilde{\Gamma}_\ell \;=\; \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \Gamma_\ell & N_\ell \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -m \\ 0 & 1 \end{pmatrix} \;=\; \left\{ \begin{pmatrix} \gamma & n - (\gamma - \mathrm{id})m \\ 0 & 1 \end{pmatrix} \;\middle|\; \begin{array}{c} \gamma \in \Gamma_\ell \\ n \in N_\ell \end{array} \right\}.$$

We must therefore find $\gamma \in \Gamma_\ell$ and $n \in N_\ell$ such that $\det(\gamma - \mathrm{id}) \neq 0$ and

$$\mathrm{pr}_i\, \pi_\ell\big((\gamma - \mathrm{id})^{-1} n - m\big) = \mathrm{pr}_i\, \pi_\ell\Big((\gamma - \mathrm{id})^{-1}\big(n - (\gamma - \mathrm{id})m\big)\Big) \neq 0$$

for all i. This second condition is equivalent to

$$\mathrm{pr}_i\big((\gamma - \mathrm{id})^{-1} n\big) \not\equiv \mathrm{pr}_i(m) \ \bmod\ T_\ell(A_i).$$

Take any integer r so that $\ell^r m \in T_\ell(A)$. Then it suffices to have

$$\ell^r \operatorname{pr}_i\big((\gamma - \mathrm{id})^{-1}n\big) \;\notin\; T_\ell(A_i).$$

With $n = (n_1, \ldots, n_d) \in N_\ell$ this is equivalent to

$$\ell^r n_i \notin (\gamma - \mathrm{id})T_\ell(A_i). \tag{4.6}$$

Now by functoriality the image $\operatorname{pr}_i(N_\ell) \subset T_\ell(A_i)$ is the unipotent part of the ℓ-adic Galois group attached to (A_i, a_i). As a_i has infinite order, this image is non-trivial by Theorem 2.8. Since any finite number of non-trivial linear inequalities in a free $\mathbb{Z}_\ell$-module can be simultaneously satisfied, we may therefore select $n = (n_1, \ldots, n_r) \in N_\ell$ such that all $n_i \neq 0$. Then clearly 4.6 holds for any suitable $\gamma \in \Gamma_\ell$ that is sufficiently close to the identity. This proves that U' is non-empty, as desired. **q.e.d.**

Theorem 4.7 *For $1 \leq i \leq d$ let A_i be an abelian variety over a number field K and $a_i \in A_i(K)$ a rational point of infinite order. Then there exists a set of rational primes ℓ of Dirichlet density > 0 with the following property. Let $f(T) \in \mathbb{Z}[T]$ be any polynomial which is a product of cyclotomic polynomials and a power of T. For any finite place v of K let p_v denote the characteristic of the residue field and $a_{i,v}$ the reduction of a_i. Then for all finite places v of K in a set of Dirichlet density > 0 the ℓ-part of $f(p_v)a_{i,v}$ is non-trivial for every i.*

Proof. We apply the results of the preceding sections to $A := A_1 \times \ldots \times A_d$ and $a := (a_1, \ldots, a_d)$. By Corollary 1.3 there exists a set of rational primes ℓ of positive Dirichlet density for which the associated algebraic monodromy group G_ℓ splits over $\mathbb{Q}_\ell$. We will prove the theorem for any such ℓ.

Let $\mu : G_\ell \to \mathbb{G}_{m,\mathbb{Q}_\ell}$ be the multiplier character and let $\operatorname{pr}_i : A \to A_i$ denote the projection to the i^{th} factor. As in the proof of Theorem 4.1

$$U_f := \left\{ \tilde\gamma \in \tilde\Gamma_\ell \;\middle|\; \begin{array}{l} \det(\gamma - \mathrm{id}) \neq 0, \text{ and} \\ \forall i: \; f(\mu(\gamma)) \operatorname{pr}_i \pi_\ell\big((\gamma - \mathrm{id})^{-1}n\big) \neq 0 \end{array} \right\}$$

is an open subset of $\tilde\Gamma_\ell$.

Lemma 4.8 *U_f is non-empty.*

Proof. As in the proof of Lemma 4.5, after replacing K by a finite extension we may assume that

$$\tilde\Gamma_\ell \;=\; \left\{ \begin{pmatrix} \gamma & n - (\gamma - \mathrm{id})m \\ 0 & 1 \end{pmatrix} \;\middle|\; \begin{array}{c} \gamma \in \Gamma_\ell \\ n \in N_\ell \end{array} \right\}$$

for some $m \in V_\ell(A)$. We must therefore find elements $\gamma \in \Gamma_\ell$ and $n \in N_\ell$ such that $\det(\gamma - \mathrm{id}) \neq 0$ and

$$f(\mu(\gamma)) \operatorname{pr}_i \pi_\ell\big((\gamma - \mathrm{id})^{-1}n - m\big) \neq 0$$

for every i. This second condition is equivalent to

$$f(\mu(\gamma)) \operatorname{pr}_i\big((\gamma - \mathrm{id})^{-1}n\big) \not\equiv f(\mu(\gamma)) \operatorname{pr}_i(m) \mod T_\ell(A_i).$$

Taking any integer r so that $\ell^r m \in T_\ell(A)$, it suffices to have

$$\ell^r f(\mu(\gamma)) \operatorname{pr}_i\big((\gamma - \mathrm{id})^{-1}n\big) \;\notin\; T_\ell(A_i). \tag{4.9}$$

Now by the assumption on ℓ there exists a split maximal torus $S_\ell \subset G_\ell$. Every character χ of S_ℓ is then defined over $\mathbb{Q}_\ell$. For any representation W of S_ℓ let $\mathrm{pr}_\chi : W \twoheadrightarrow W_\chi$ denote the projection to the weight space associated to χ. Recall from Proposition 2.5 that N_ℓ is open in U_ℓ, which is an algebraic representation of G_ℓ and hence of S_ℓ. Thus $N_{\ell,\chi} := V_\ell(A)_\chi \cap N_\ell$ is open in the weight space $U_{\ell,\chi}$. For every χ we want to select an element $n_\chi \in N_{\ell,\chi}$ such that for all i we have $\mathrm{pr}_i(n_\chi) \neq 0$ whenever $\mathrm{pr}_i(U_{\ell,\chi}) \neq 0$. This is possible, because any finite number of non-trivial linear inequalities in a free $\mathbb{Z}_\ell$-module can be simultaneously satisfied. We will show the desired assertions with $n := \sum_\chi n_\chi \in N_\ell$ and a suitable element $\gamma \in S_\ell(\mathbb{Q}_\ell) \cap \Gamma_\ell$. To satisfy 4.9 it suffices to have

$$\forall i\ \exists \chi :\ \ell^r f(\mu(\gamma))\,\mathrm{pr}_i\big((\gamma - \mathrm{id})^{-1} n_\chi\big) \ \notin\ \mathrm{pr}_\chi\big(T_\ell(A_i)\big).$$

As n_χ is an eigenvector of γ for the eigenvalue $\chi(\gamma) \in \mathbb{Z}_\ell$, this element is equal to

$$\frac{\ell^r f(\mu(\gamma))}{\chi(\gamma) - 1} \cdot \mathrm{pr}_i(n_\chi).$$

Fix an integer s so that for all i and χ with $\mathrm{pr}_i(n_\chi) \neq 0$ we have

$$\mathrm{pr}_i(n_\chi) \ \notin\ \ell^s\,\mathrm{pr}_\chi\big(T_\ell(A_i)\big).$$

By construction this affects all pairs (i, χ) with $\mathrm{pr}_i(U_{\ell,\chi}) \neq 0$. Thus it suffices to prove the following assertion, from which the n_χ have vanished.

Sublemma 4.10 *There exists an element* $\gamma \in S_\ell(\mathbb{Q}_\ell) \cap \Gamma_\ell$ *satisfying* $\det(\gamma - \mathrm{id}) \neq 0$ *such that for every* i *there exists a character* χ *with* $\mathrm{pr}_i(U_{\ell,\chi}) \neq 0$ *and*

$$\mathrm{ord}_\ell\big(\chi(\gamma) - 1\big) \ \geq\ r + s + \mathrm{ord}_\ell\big(f(\mu(\gamma))\big).$$

Proof. For every i let $B_i \subset A_i$ be the identity component of the Zariski closure of $\mathbb{Z}a_i$. Applying Proposition 1.5 to $B := B_1 \times \ldots \times B_d$ shows that there exist weights χ_i of S_ℓ on $V_\ell(B_i) \subset V_\ell(A_i)$ so that μ is $\mathbb{Q}$-linearly independent of $\chi_1, \ldots, \chi_d$. The functoriality and Theorem 2.8 together imply that $\mathrm{pr}_i(U_\ell) = V_\ell(B_i)$. Since the projection map pr_i is S_ℓ-equivariant, we deduce that

$$\mathrm{pr}_i(U_{\ell,\chi_i}) = V_\ell(B_i)_{\chi_i} \neq 0.$$

It remains to find an element $\gamma \in S_\ell(\mathbb{Q}_\ell) \cap \Gamma_\ell$ with $\det(\gamma - \mathrm{id}) \neq 0$ and for all i

$$\mathrm{ord}_\ell\big(\chi_i(\gamma) - 1\big) \ \geq\ r + s + \mathrm{ord}_\ell\big(f(\mu(\gamma))\big). \tag{4.11}$$

The inequality 4.11 means that $\chi_i(\gamma)$ is much closer to the identity than $\mu(\gamma)$. To be precise let us first shrink Γ_ℓ so that Γ_ℓ acts trivially on $T_\ell(A) \big/ \ell^2 T_\ell(A)$. Then for every element $\gamma \in S_\ell(\mathbb{Q}_\ell) \cap \Gamma_\ell$ we have $\mu(\gamma) \equiv 1 \bmod \ell^2$. On the other hand choose an integer $k > 0$ such that all non-zero roots of $f(T)$ are roots of unity of order dividing k and have multiplicity $\leq k$. Then after multiplying $f(T)$ by some more cyclotomic polynomials we may assume that $f(T) = T^{k'}(T^k - 1)^k$ for some $k' \geq 0$. A standard calculation now shows that

$$\begin{aligned} \mathrm{ord}_\ell(f(\mu(\gamma))) &= k' \cdot \mathrm{ord}_\ell\big(\mu(\gamma)\big) + k \cdot \mathrm{ord}_\ell\big(\mu(\gamma)^k - 1\big) \\ &= k \cdot \mathrm{ord}_\ell(k) + k \cdot \mathrm{ord}_\ell\big(\mu(\gamma) - 1\big). \end{aligned}$$

Setting $t := r + s + k \cdot \mathrm{ord}_\ell(k)$ we thus need to find an element $\gamma \in S_\ell(\mathbb{Q}_\ell) \cap \Gamma_\ell$ with $\det(\gamma - \mathrm{id}) \neq 0$ and for all i

$$\mathrm{ord}_\ell\big(\chi_i(\gamma) - 1\big) \ \geq\ t + k \cdot \mathrm{ord}_\ell\big(\mu(\gamma) - 1\big). \tag{4.12}$$

To achieve this let S_ℓ^1 denote the identity component of $\mathrm{Ker}(\mu|S_\ell)$, which is a subtorus of codimension 1. Since μ is $\mathbb{Q}$-linearly independent of $\chi_1, \ldots, \chi_d$ and S_ℓ splits over $\mathbb{Q}_\ell$, there exists a subtorus S_ℓ^2 of dimension 1 inside $\bigcap_{i=1}^d \mathrm{Ker}(\chi_i|S_\ell)$ on which μ is non-trivial. We will take $\gamma = \gamma_1\gamma_2$ with $\gamma_1 \in S_\ell^1(\mathbb{Q}_\ell) \cap \Gamma_\ell$ and $\gamma_2 \in S_\ell^2(\mathbb{Q}_\ell) \cap \Gamma_\ell$. Then the left hand side of 4.12 depends only on γ_1, while the right hand side depends only on γ_2.

Theorem 1.1 (c) implies that Γ_ℓ contains an open subgroup of $S_\ell(\mathbb{Q}_\ell)$. Thus if we first select any non-trivial γ_2, the inequality 4.12 will hold for every γ_1 that is sufficiently close to the identity. Furthermore, none of the weights of S_ℓ on $V_\ell(A)$ is zero, e.g., by Proposition 1.4. Thus in any neighborhood of the identity γ_1 can be chosen such that $\gamma = \gamma_1\gamma_2$ does not have the eigenvalue 1 on $V_\ell(A)$, which means that $\det(\gamma - \mathrm{id}) \neq 0$. Thus all requirements can be simultaneously satisfied, finishing the proof of Sublemma 4.10 and hence of Lemma 4.8. **q.e.d.**

Now we return to the proof of Theorem 4.7. Since $U_f \subset \tilde{\Gamma}_\ell$ is a non-empty open subset, as in the proof of Theorem 4.1 we conclude that there exists a set of places $v \notin S$ of K of Dirichlet density > 0 for which $\tilde{\rho}_\ell(\mathrm{Frob}_v) \in U_f$. We may also assume that the associated residue fields k_v have prime order, because the remaining places form a set of Dirichlet density 0. For these places we have $\mu\rho_\ell(\mathrm{Frob}_v) = |k_v| = p_v$. The definition of U_f and Proposition 3.2 thus imply that $f(p_v)\,\mathrm{pr}_i\,\kappa_v(a) \neq 0$ for every i. By the definition of κ_v this means that the ℓ-part of $f(p_v)a_{i,v}$ is non-trivial for every i, as desired. **q.e.d.**

Remark 4.13 Theorem 4.7 is not true in general for every rational prime ℓ, even for a single abelian variety A and a single rational point $a \in A(K)$. For a counterexample suppose that A is an elliptic curve with complex multiplication over K. Then $\mathrm{End}_K(A)$ is an order in an imaginary quadratic number field F, and for any rational prime ℓ the image of Galois is an open compact subgroup of $(F \otimes \mathbb{Q}_\ell)^*$. Thus G_ℓ splits over $\mathbb{Q}_\ell$ if and only if ℓ splits in F, and in this case the proof of Theorem 4.7 goes through.

If ℓ does not split in F, we will show that the theorem is false. It is known that for every finite place $v \notin S$ with $|k_v| = p_v$ the element $\alpha_v := \rho_\ell(\mathrm{Frob}_v)$ is an algebraic integer in F with $\alpha_v\bar{\alpha}_v = p_v$ and that the cardinality of $A_v(k_v)$ is equal to $(\alpha_v - 1)(\bar{\alpha}_v - 1)$. In particular the integer $(\alpha_v - 1)(\bar{\alpha}_v - 1)$ annihilates the reduction of a. Now the fact that F has only one prime above ℓ implies that

$$\mathrm{ord}_\ell(\alpha_v - 1) \;=\; \mathrm{ord}_\ell(\bar{\alpha}_v - 1) \;\leq\; \mathrm{ord}_\ell(\alpha_v\bar{\alpha}_v - 1) \;=\; \mathrm{ord}_\ell(p_v - 1).$$

Thus with $f(T) := (T-1)^2$ we deduce that

$$\mathrm{ord}_\ell\big((\alpha_v - 1)(\bar{\alpha}_v - 1)\big) \;\leq\; 2 \cdot \mathrm{ord}_\ell(p_v - 1) \;=\; \mathrm{ord}_\ell\big(f(p_v)\big).$$

This implies that $f(p_v)$ annihilates the ℓ-part of the reduction of a. Since this is so for every $v \notin S$, we conclude that in this example Theorem 4.7 is true precisely for ℓ in a set of Dirichlet density 1/2.

5 Density results for the full reduction

In this section we derive some consequences of the density results of the preceding section which no longer refer to any particular prime ℓ.

Theorem 5.1 *For $1 \leq i \leq d$ let A_i be an abelian variety over a number field K and $a_i \in A_i(K)$ a rational point. Assume that for all finite places v of K in a set of Dirichlet density 1 the reduction of at least one a_i is annihilated by a power of the residue characteristic p_v. Then at least one $a_i = 0$.*

Proof. Suppose that some a_i is a torsion point of order n. If $n = 1$, we are done. Otherwise the order of the reduction of a_i at any finite place $v \nmid n$ is still n, and therefore not a power of p_v. Thus after removing A_i and a_i from the list the assumptions still hold. After iterating this we may assume that all a_i have infinite order; we must then derive a contradiction. Select any rational prime ℓ. Then by Theorem 4.4 for all finite places $v \nmid \ell$ of K in a set of Dirichlet density > 0 the ℓ-part of the reduction of every a_i is non-trivial. In particular, these reductions are not annihilated by a power of p_v, contradicting the given assumption. **q.e.d.**

Remark 5.2 Damian Roessler pointed out to the author that Theorem 5.1 can also be deduced from a theorem of Wong [16]. To sketch this set $A := A_1 \times \ldots \times A_d$. For any prime ℓ let $\Gamma_{\ell,1}$ denote the image of $\mathrm{Gal}(\bar{K}/K)$ in its action on the ℓ-torsion subgroup $A[\ell]$. By a theorem of Serre, which for example follows from [15, Th. 2], the group cohomology $H^1(\Gamma_{\ell,1}, A[\ell])$ vanishes for all $\ell \gg 0$. We temporarily fix any such $\ell > d$.

The assumptions in Theorem 5.1 imply that for all v in a set of Dirichlet density 1 the reduction of at least one a_i has trivial ℓ-part. Since multiplication by ℓ induces an automorphism on the prime-to-ℓ part of $A_v(k_v)$, the reduction of a_i then lies in $\ell A_v(k_v)$. Wong [16, Th. 2] deduces from this that at least one a_i is contained in $\ell A(K)$. Since this is true for every $\ell \gg 0$, and the Mordell-Weil group $A(K)$ is finitely generated, this implies that at least one a_i is torsion. As in the proof of 5.1 we now deduce that at least one $a_i = 0$, as desired.

Theorem 5.3 *For $1 \leq i \leq d$ let A_i be an abelian variety over a number field K and $a_i \in A_i(K)$ a rational point. Let $f(T) \in \mathbb{Z}[T]$ be any polynomial which is a product of cyclotomic polynomials and a power of T. For any finite place v of K let p_v denote the characteristic of the residue field and $a_{i,v}$ the reduction of a_i. Assume that for all finite places v of K in a set of Dirichlet density 1 at least one $a_{i,v}$ is annihilated by $f(p_v)$. Then at least one a_i is a torsion point.*

Proof. Suppose that every a_i has infinite order. Then by Theorem 4.7 there exists a rational prime ℓ such that for all finite places v of K in a set of Dirichlet density > 0 the ℓ-part of every $f(p_v)a_{i,v}$ is non-trivial. In particular, these $a_{i,v}$ are not annihilated by $f(p_v)$, contradicting the given assumption. Thus the order of at least one a_i is finite. **q.e.d.**

References

[1] Bashmakov, M.: The cohomology of abelian varieties over a number field. *Russian Math. Surveys* **27** (6) (1977), 25–70.

[2] Bertrand, D.: Galois representations and transcendental numbers. *New advances in transcendence theory (Durham, 1986)*, Cambridge: Cambridge Univ. Press (1988), 37–55.

[3] Bogomolov, F. A.: Points of finite order on abelian varieties. (Russian) *Izv. Akad. Nauk SSSR* Ser. Mat. **44** (1980), 782–804, 973 = *Math. USSR Izvestija* **17** (1981), 55-72.

[4] Bogomolov, F. A.: Sur l'algébricité des représentations ℓ-adiques. *C. R. Acad. Sci. Paris Sér. A-B* **290**, no. 15 (1980) A701–A703.

[5] Borel, A.: *Linear Algebraic Groups.* GTM **126**, New York etc.: Springer (1991).

[6] Corrales-Rodrigáñez, C., Schoof, R.: The Support Problem and Its Elliptic Analogue. *J. Number Th.* **64** (1997), 276–290.

[7] Deligne, P.: Théorie de Hodge, III. *Publ. Math. IHES* **44** (1974), 5–77.

[8] Faltings, G.: Finiteness Theorems for Abelian Varieties over Number Fields. *Arithmetic Geometry, G. Cornell, J. H. Silverman (Eds.)*, New York etc.: Springer (1986), 9–27.

[9] Hindry, M.: Autour d'une conjecture de Serge Lang. *Invent. math.* **94** (1988), 575–603.

[10] Khare, C., Prasad, D.: Reduction of Homomorphisms mod p and algebraicity. *Preprint* (18 p.) `arXiv:math.NT/0211004 v1 1 Nov 2002.`

[11] Larsen, M. J.: The Support Problem For Abelian Varieties. *Preprint* (7 p.) `arXiv:math.NT/0211118 v3 28 Feb 2003.`

[12] Pink, R., Roessler, D.: A Conjecture of Beauville and Catanese Revisited. *Preprint* November 27, 2003, 13p.

[13] Ribet, K.: Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.* **46** No. 4 (1979), 745–761.

[14] Serre, J.-P.: Lettre à Ken Ribet du 1/1/1981. *Oeuvres vol. IV,* Berlin etc.: Springer (2000), 1–17.

[15] Serre, J.-P.: Résumé des cours de 1985–1986. *Annuaire du Collège de France* (1986), 95–99 = *Oeuvres vol. IV,* Berlin etc.: Springer (2000), 33–37.

[16] Wong, S.: Power Residues on Abelian Varieties. *Manuscripta math.* **102** (2000) 129–137.