DIVIDING RATIONAL POINTS ON ABELIAN
VARIETIES OF CM-TYPE

Kenneth A. Ribet*

This note has to do with the general problem of Galois representations arising from abelian varieties of CM-type. More particularly, we wish to see what happens when one takes the $\ell^n$ roots ($\ell$ a varying prime) of a fixed set of rational points on a simple abelian variety $A$ of CM-type. Provided that the rational points are independent over the endomorphism ring of $A$, the Galois groups that one obtains are as large as possible for all but finitely many $\ell$. (See the theorem below for a precise statement.)

This result has recently been applied by Coates and Lang in a study involving diophantine approximation [4]. Similar results were previously obtained by Ba\v{s}makov [1, 2], who studied elliptic curves (both with and without complex multiplication). A special case was also discussed in [3].

1. Statement of the result, and beginning of the proof

Let $A$ be an abelian variety over a number field $K$. We assume that all endomorphisms of $A$ are defined over $K$ and that the algebra

$$F = (\text{End} A) \otimes Q$$

is a field of degree $2 \cdot \dim A$. Thus $A$ is simple and of CM-type.

If $\ell$ is a prime, let

$$\rho_\ell : \text{Gal} (\bar{K}/K) \to \text{Aut} A_\ell$$

* Sloan Fellow. The author wishes to thank the I.H.E.S. for its hospitality.
be the character giving the action of $\text{Gal}(\overline{K}/K)$ on the group of $\ell$-division points of $A$. Let $G_\ell \subseteq \text{Aut} A_\ell$ be the image of $\rho_\ell$ and let $k_\ell = K(A_\ell)$ be the corresponding Galois extension of $K$.

Now let $x_1, \ldots, x_n$ be elements of the group $A(K)$ of $K$-rational points of $A$. Let $K_\ell$ be the extension of $K$ obtained by adjoining to $K$ all $\ell^n$ roots of all the points $x_i$ (these roots are taken in a fixed algebraic closure $\overline{K}$ of $K$). Then $K_\ell$ is a Galois extension of $K$ which contains $k_\ell$. Let $G$, $H_\ell$, and $C_\ell$ be the Galois groups in the following diagram:

$$
G \xrightarrow{H_\ell} \frac{\overline{K}}{K} \xrightarrow{k_\ell} \frac{C_\ell}{k_\ell} \xrightarrow{G_\ell} K
$$

In view of the action of $H_\ell$ on the $\ell^n$ roots of the $x_i$, we may view $C_\ell$ as a subgroup of the abelian group

$$B_\ell = A_\ell \times \cdots \times A_\ell \ (n \text{ times}).$$

In fact, for any $x \in A(K)$, we define a continuous homomorphism

$$\varphi_x : H_\ell \to A_\ell$$

as follows: take any $\ell^n$ root $r$ of $x$, and set $\varphi_x(\sigma) = \sigma r - r$ if $\sigma \in H_\ell$. It is immediate that $\varphi_x$ is independent of the choice of $r$ and that $\varphi_x$ is a homomorphism which induces an isomorphism of the Galois group $\text{Gal}(k_\ell(\ell^{-1}x)/k_\ell)$ with a subgroup of $A_\ell$. Set $\varphi_i = \varphi_{x_i} \ (i = 1, \ldots, n)$, and put

$$\varphi = \varphi_1 \times \cdots \times \varphi_n.$$

Then $\varphi$ is a continuous homomorphism $H_\ell \to B_\ell$ which induces an injection $C_\ell \hookrightarrow B_\ell$. It is sometimes useful to identify $C_\ell$ with its image in $B_\ell$.

Before stating the theorem, we make one more remark on terminology. If $M$ is a module over a ring $R$ and if $m_1, \ldots, m_n \in M$, we say that $m_1, \ldots, m_n$ are linearly independent (over $R$) if no non-trivial linear combination $\sum a_i m_i$ vanishes ($a_i \in R$).
THEOREM: Assume that \( x_1, \ldots, x_n \in A(K) \) are linearly independent over \( \text{End} \ A \). Then \( C_\ell = B_\ell \) for all but finitely many primes \( \ell \).

We shall show, first of all, that \( B_\ell = C_\ell \) whenever \( \ell \) satisfies a certain pair of conditions. Then, in the remaining two sections, we will show that each condition is satisfied provided that \( \ell \) is sufficiently large.

Let \( O \) be the integer ring of \( F \). One knows that \( \text{End} \ A = \text{End}_K A \) is a subring of \( \text{finite index in} \ O \). We shall always assume that our primes \( \ell \) are unramified in \( F \) and prime to the index \( (O : \text{End} A) \). This condition, satisfied by all but finitely many \( \ell \), implies that

\[
(\text{End} \ A)/\ell(\text{End} \ A) = O/\ell O
\]

is a product of fields and that \( A_\ell \) is free of rank 1 over \( (\text{End} \ A)/\ell(\text{End} \ A) \) [6, pp. 501–502]. Then we have

\[
G_\ell \subseteq (O/\ell O)^* = \text{Aut}_{O/\ell O} A_\ell.
\]

On the other hand, it is easy to see that \( C_\ell \) is a \( G_\ell \)-stable subgroup of \( B_\ell \). Indeed, this follows from the general formula

\[
\varphi_\sigma(\tau \sigma \tau^{-1}) = \tau \cdot \varphi_\sigma(\sigma)
\]

valid for \( x \in A(K), \tau \in G, \sigma \in H_\ell \).

LEMMA: Let \( R \) be a product of fields, and let \( V \) be a free rank-1 module over \( R \). Suppose that \( C \) is an \( R \)-submodule of \( B = V \times \cdots \times V \) (n times) which is strictly smaller than \( B \). Then there are elements \( t_1, \ldots, t_n \) of \( R \), not all 0, such that

\[
\sum t_i v_i = 0
\]

for all \( (v_1, \ldots, v_n) \in C \).

PROOF: Clear.

COROLLARY: We have \( C_\ell = B_\ell \) whenever the following two conditions are verified:

(i) The subring \( \mathbb{F}_\ell[G_\ell] \) of \( O/\ell O \) generated by the elements of \( G_\ell \) is in fact all of \( O/\ell O \).

(ii) The homomorphisms \( \varphi_1, \ldots, \varphi_n : H_\ell \to A_\ell \) are linearly independent over \( O/\ell O \).
PROOF: Given condition (i), we apply the lemma with $R = O/\ell O$, $C = C_\ell$, $B = B_\ell$.

2. Galois action on points of finite order (verification of (i))

Let $p$ be any rational prime which splits completely in the multiplication field $F$ and such that $A$ has good reduction at some prime of $K$ lying over $p$. Let $v$ be such a prime. Since the $Q_v$-adic Tate module $V_v$ of $A$ is free of rank 1 over $F \otimes Q_v$ and since all endomorphisms of $A$ are defined over $K$, $V_v$ is the direct sum of $\text{Gal}(\bar{K}/K)$-modules which are 1-dimensional over $Q_v$. By the Serre-Tate lifting theory, this implies that the endomorphism algebra $(\text{End } A_v) \otimes Q$ of the reduction of $A$ at $v$ is precisely equal to $(\text{End } A) \otimes Q = F$ [5, Theorem 2, p. IV-41; Cor., p. IV-42]. Since $F$ is commutative, Tate’s theorem says that $F = Q(\pi_v)$, where $\pi_v \in 0$ is the Frobenius endomorphism of $A_v$ [9, Th. 2(a), p. 140]. This implies that the ring $\mathbb{Z}[\pi_v]$ has finite index in $O$.

PROPOSITION: If $\ell$ is sufficiently large, then $F_\ell[G_\ell] = O/\ell O$.

PROOF: From the above discussion we see that $F_\ell[\pi_v] = O/\ell O$ whenever $\ell$ is prime to the index of $\mathbb{Z}[\pi_v]$ in $O$. But if $\ell \neq p$ then $\pi_v$ (or rather its image in $O/\ell O$) belongs to $G_\ell$: it is the image in $G_\ell$ of any Frobenius element for $v$ in $\text{Gal}(\bar{K}/K)$. We have then

$$O/\ell O = F_\ell[\pi_v] \subseteq F_\ell[G_\ell] \subseteq O/\ell O$$

if $\ell$ is prime to $(O: \mathbb{Z}[\pi_v])$ and different from $p$.

REMARK: Shimura has given an alternate proof of this proposition based on the theory of complex multiplication [8, Th. 1, p. 110], [7, Prop. 1.9]. As a compromise, one may obtain primes $\ell$ for which $F = (\text{End } A_v) \otimes Q$ by using [8, Th. 2, p. 114] and then employ Tate’s Theorem as above.

3. Application of the Mordell-Weil theorem (verification of (ii))

We consider the sequence

$$A(K) \xrightarrow{\cdot m} A(K) \xrightarrow{\pi_v} H^1(G, A_\ell)$$
obtained by taking cohomology in the short exact sequence

\[ 0 \rightarrow A_{\ell} \rightarrow A(\bar{K}) \xrightarrow{\ell} A(\bar{K}) \rightarrow 0. \]

("\(\ell\)" is the map "multiplication by \(\ell\`).")

**Lemma:**

1. The map \(h : A(K) \rightarrow \text{Hom}(H_{\ell}, A_{\ell})\) defined by \(x \mapsto \varphi_x\) is \((\text{End} A)\)-linear.

2. Further, \(h\) is the composition of \(\delta\) with the restriction homomorphism

\[ \text{res} : H^1(G, A_{\ell}) \rightarrow H^1(H_{\ell}, A_{\ell}) = \text{Hom}(H_{\ell}, A_{\ell}). \]

3. The map \(\text{res}\) is injective.

**Proof:** The first two statements are proved by a direct computation, which we omit. The third follows from the restriction-inflation sequence together with the vanishing of

\[ H^1(G/H_{\ell}, A_{\ell}) = H^1(G_{\ell}, A_{\ell}). \]

This cohomology group vanishes because \(A_{\ell}\) is an \(\ell\)-group, whereas \(G_{\ell} \subseteq (O/\ell O)^*\) has prime-to-\(\ell\) order.

**Corollary:** The map \(h\) induces an \((O/\ell O)\)-linear injection

\[ A(K)/\ell A(K) \hookrightarrow \text{Hom}(H_{\ell}, A_{\ell}). \]

Hence \(\varphi_1, \ldots, \varphi_n\) are linearly independent if and only if the images \(\tilde{s}_1, \ldots, \tilde{s}_n\) of \(x_1, \ldots, x_n\) in \(A(K)/\ell A(K)\) are linearly independent over \(O/\ell O\).

**Proof:** Clear.

**Proposition:** If \(\ell\) is sufficiently large, then \(\varphi_1, \ldots, \varphi_n\) are linearly independent.

**Proof:** Because of the corollary, it suffices to prove that the map

\[ \Gamma/\ell \Gamma \rightarrow A(K)/\ell A(K) \]
is injective, where $\Gamma$ is the subgroup of $A(K)$ generated over $O$ by $x_1, \ldots, x_n$. Let

$$I'' = \{ y \in A(K) | my \in \Gamma \text{ for some } m \in \mathbb{Z} \}.$$

By the Mordell-Weil Theorem, $I''$ is finitely generated, and hence the index $(I'':\Gamma)$ is finite. One sees that $j$ is injective whenever $\ell$ is prime to $(I'':\Gamma)$.\footnote{Cassels remarks that one may avoid the use of the Mordell-Weil theorem here by using properties of heights and a trick from diophantine approximation.}

As noted above, the theorem follows from the corollary of §1 together with the above proposition and the proposition of §2.

References