COMPOSITIO MATHEMATICA, Vol. 33, Fasc. 1, 1976, pag. 69–74
Noordhoff International Publishing
Printed in the Netherlands

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 ℓ^{th} roots (ℓ 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 ℓ. (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 Bašmakov [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

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

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

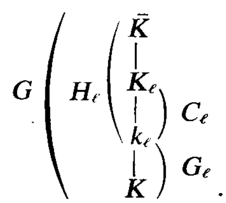
If ℓ is a prime, let

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

* Sloan Fellow. The author wishes to thank the I.H.E.S. for its hospitality.

be the character giving the action of $\mathrm{Gal}(\bar{K}/K)$ on the group of ℓ-division points of A. Let $G_\ell \subseteq \mathrm{Aut}\, A_\ell$ be the image of ρ_ℓ, 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_ℓ be the extension of K obtained by adjoining to K all ℓ^{th} roots of all the points x_i. (These roots are taken in a fixed algebraic closure $\bar{K}$ of K.) Then K_ℓ is a Galois extension of K which contains k_ℓ. Let G, H_ℓ, and C_ℓ be the Galois groups in the following diagram:



In view of the action of H_ℓ on the ℓ^{th} roots of the x_i, we may view C_ℓ 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 ℓ^{th} root r of x, and set $\varphi_x(\sigma) = \sigma r - r$ if $\sigma \in H_\ell$. It is immediate that φ_x is independent of the choice of r and that φ_x is a homomorphism which induces an isomorphism of the Galois group $\mathrm{Gal}(k_\ell(\ell^{-1}x)/k_\ell)$ with a subgroup of A_ℓ. Set $\varphi_i = \varphi_{x_i}$ $(i = 1, \ldots, n)$, and put

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

Then φ 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_ℓ with its image in B_ℓ.

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 $\Sigma\, a_i m_i$ vanishes $(a_i \in R)$.

THEOREM: *Assume that $x_1, \ldots, x_n \in A(K)$ are linearly independent over* End A. *Then $C_\ell = B_\ell$ for all but finitely many primes ℓ.*

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

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

$$(\mathrm{End}\, A)/\ell(\mathrm{End}\, A) = O/\ell O$$

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

$$G_\ell \subseteq (O/\ell O)^* = \mathrm{Aut}_{O/\ell O} A_\ell.$$

On the other hand, it is easy to see that C_ℓ is a G_ℓ-stable subgroup of B_ℓ. Indeed, this follows from the general formula

$$\varphi_x(\tau\sigma\tau^{-1}) = \tau \cdot \varphi_x(\sigma)$$

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 $\mathbf{F}_\ell[G_\ell]$ of $O/\ell O$ generated by the elements of G_ℓ 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 $\boldsymbol{Q}_\ell$-adic Tate module V_ℓ of A is free of rank 1 over $F \otimes \boldsymbol{Q}_\ell$, and since all endomorphisms of A are defined over K, V_ℓ is the direct sum of Gal $(\bar{K}/K)$-modules which are 1-dimensional over $\boldsymbol{Q}_\ell$. By the Serre-Tate lifting theory, this implies that the endomorphism algebra (End $\tilde{A}_v) \otimes \boldsymbol{Q}$ of the *reduction* of A at v is precisely equal to (End $A) \otimes \boldsymbol{Q} = F$ [5, Theorem 2, p. IV-41; Cor., p. IV-42]. Since F is commutative, Tate's theorem says that $F = \boldsymbol{Q}(\pi_v)$, where $\pi_v \in 0$ is the Frobenius endomorphism of $\tilde{A}_v$ [9, Th. 2(a), p. 140]. This implies that the ring $\boldsymbol{Z}[\pi_v]$ has finite index in O.

PROPOSITION: *If ℓ is sufficiently large, then $\boldsymbol{F}_\ell[G_\ell] = O/\ell O$.*

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

$$O/\ell O = \boldsymbol{F}_\ell[\pi_v] \subseteq \boldsymbol{F}_\ell[G_\ell] \subseteq O/\ell O$$

if ℓ is prime to $(O: \boldsymbol{Z}[\pi_v])$ 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 v for which $F = (\text{End } \tilde{A}_v) \otimes \boldsymbol{Q}$ 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

$$A(K) \xrightarrow{\text{“}\ell\text{”}} A(K) \xrightarrow{\delta} H^1(G, A_\ell)$$

obtained by taking cohomology in the short exact sequence

$$0 \to A_\ell \to A(\bar{K}) \xrightarrow{\text{"}\ell\text{"}} A(\bar{K}) \to 0.$$

("ℓ" is the map "multiplication by ℓ.")

LEMMA:

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

2. *Further, h is the composition of δ with the restriction homomorphism*

$$\mathrm{res}: H^1(G, A_\ell) \to H^1(H_\ell, A_\ell) = \mathrm{Hom}(H_\ell, A_\ell).$$

3. *The map* 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_ℓ is an ℓ-group, whereas $G_\ell \subseteq (O/\ell O)^*$ has prime-to-ℓ order.

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

$$A(K)/\ell A(K) \hookrightarrow \mathrm{Hom}(H_\ell, A_\ell).$$

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

PROOF: Clear.

PROPOSITION: *If* ℓ *is sufficiently large, then* $\varphi_1, \ldots, \varphi_n$ *are linearly independent.*

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

$$\Gamma/\ell\Gamma \xrightarrow{j} A(K)/\ell A(K)$$

is injective, where Γ is the subgroup of $A(K)$ generated over O by $x_1, \ldots, x_n$. Let

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

By the Mordell-Weil Theorem, Γ' is finitely generated, and hence the index $(\Gamma' : \Gamma)$ is finite. One sees that j is injective whenever ℓ is prime to $(\Gamma' : \Gamma)$.[1]

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

[1] 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.

REFERENCES

[1] M. BAŠMAKOV: Un théorème de finitude sur la cohomologie des courbes elliptiques. *C.R. Acad. Sci. Paris Sér. A-B 270*, A 999-A 1000 (1970).
[2] M. BAŠMAKOV: The cohomology of abelian varieties over a number field. *Russian Math. Surveys 27* (6) (1972) 25–70.
[3] J. COATES: An application of the division theory of elliptic functions to diophantine approximation. *Inventiones math. 11* (1970) 167–182.
[4] J. COATES and S. LANG: Diophantine approximation on abelian varieties with complex multiplication. (To appear).
[5] J-P. SERRE: *Abelian ℓ-adic representations and elliptic curves.* New York: Benjamin 1968.
[6] J-P. SERRE and J. TATE: Good reduction of abelian varieties. *Ann of Math. 88* (1968) 492–517.
[7] G. SHIMURA: On canonical models of arithmetic quotients of bounded symmetric domains. *Ann. of Math. 91* (1970) 144–222.
[8] G. SHIMURA and Y. TANIYAMA: Complex multiplication of abelian varieties and its applications to number theory. *Publ. Math. Soc. Japan 6* (1961).
[9] J. TATE: Endomorphisms of abelian varieties over finite fields. *Inventiones Math. 2* (1966) 134–144.

(Oblatum 9–X–1975)

Fine Hall
Princeton, N.J. 08540
USA