PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 104, Number 3, November 1988

A REMARK ON KERNELS OF REDUCTION

ROBERT F. COLEMAN

(Communicated by Louis J. Ratliff, Jr.)

ABSTRACT. We show the group of torsion points on an Abelian variety defined over an algebraic closure of the rationals, $\bar{\mathbf{Q}}$ is generated by the kernels of reduction of all the primes of $\bar{\mathbf{Q}}$.

Let A be an Abelian variety over $\bar{\mathbf{Q}}$. For each prime $\mathfrak{p}$ of $\bar{\mathbf{Q}}$ let $K_{\mathfrak{p}}$ denote the kernel of reduction in $A(\bar{\mathbf{Q}})$ at $\mathfrak{p}$. This makes sense even at primes of bad reduction since A has a unique semi-Abelian model over the ring of integers in $\bar{\mathbf{Q}}$. For each integer n, let $A[n]$ denote the kernel of multiplication by n in $A(\bar{\mathbf{Q}})$ and $K_n = K_{A,n}$ the smallest subgroup of $A[n]$ containing $A[n] \cap K_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ of $\bar{\mathbf{Q}}$. If A is defined over a number field F, then so is K_n.

Our goal in this note is to prove

THEOREM A. *The index of K_n in $A[n]$ is bounded independently of n.*

We will need the following

THEOREM B (FALTINGS AND ZARHIN [**F**], [**Z**]). *Let F be a number field. Then in each isogency class of Abelian varieties over F there are finitely many isomorphism classes.*

We will also need the following lemmas:

LEMMA C. *Suppose A is a semi-Abelian variety over the ring of integers in a number field F whose generic fiber is Abelian. Suppose b is an endomorphism of A and p is a prime number which divides the degree of b. Then b has inseparable reduction at some prime above p.*

PROOF. Let Ω denote the module of invariant differentials on A and Λ its maximal exterior power. Let β denote the eigenvalue of b on Λ. We see that $\beta\bar{\beta} = \det b$ for any complex conjugation "$-$". It follows that there exists a prime $\mathfrak{p}$ above p dividing β and b has inseparable reduction at $\mathfrak{p}$. □

LEMMA D. *Supose A and B are semi-Abelian varieties over the ring of integers in a finite extension of $\mathbf{Q}_p$ whose generic fibers are Abelian. Suppose $a\colon A \to B$ and $b\colon B \to A$ are isogenies such that $b \circ a = dp^m$, where $(d,p) = 1$ and the kernel of a contains the kernel of reduction inside $A[p^m]$. Then the reduction of b is separable.*

PROOF. This follows immediately from the fact that the subgroup of the kernel of b lying on the connected component of B injects into the reduction of B. □

Let $A_n = A/K_n$. Let $a_n\colon A \to A_n$ denote the natural isogeny and $a_n'\colon A_n \to A$ the isogeny such that $a_n' \circ a_n = n$.

Received by the editors October 5, 1987 and, in revised form, November 20, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G10; Secondary 14K19.

LEMMA E. *Suppose* $dm = n$. *Let* $B = A_d$; *then* $K_{B,m} = a_d(K_n)$.

PROOF. Clearly

$$K_{B,m} = a_d\left(\sum \{x \in A(\bar{\mathbf{Q}})\colon mx \in K_d, x_{\mathfrak{p}} \in (K_d)_{\mathfrak{p}}\}\right),$$

where the sum runs over all primes $\mathfrak{p}$ of $\bar{\mathbf{Q}}$ and the subscript $\mathfrak{p}$ denotes reduction modulo $\mathfrak{p}$. Now $\{x \in A(\bar{\mathbf{Q}})\colon mx \in K_d,\ x_{\mathfrak{p}} \in (K_d)_{\mathfrak{p}}\}$ equals

$$\{x \in A(\bar{\mathbf{Q}})\colon nx = 0,\ \exists y \in K_d \text{ such that } (x-y) \in K_{\mathfrak{p}}\} = K_d + (A[n] \cap K_{\mathfrak{p}}).$$

Since $K_d \subseteq K_n$ it follows that $K_{B,m} = a_d(K_n)$. □

COROLLARY. *If* $dn = m$, *then* $[A[d]\colon K_d]$ *divides* $[A[n]\colon K_n]$. *If* $(d,m) = 1$, *then* $[A[n]\colon K_n] = [A[d]\colon K_d] \cdot [A[m]\colon K_m]$.

PROOF. We have immediately from the lemma

$$[B[m]\colon K_{B,m}] = [A[n]\colon K_n]/[A[d]\colon K_d].$$

This implies the first part. The second part follows from the fact that $K_n = K_m \cdot K_d$ when $(m,d) = 1$. □

PROPOSITION F. *Suppose* m *and* n *are integers such that*

$$[A[m]\colon K_m] \neq [A[n]\colon K_n],$$

then A_m *and* A_n *are not isomorphic.*

PROOF. Suppose p is a prime such that

$$\operatorname{ord}_p[A[n]\colon K_n] > \operatorname{ord}_p[A[m]\colon K_m]$$

and A_m and A_n are isomorphic. We may suppose that A is defined and has a semi-Abelian model over the ring of integers in a finite extension F of $\mathbf{Q}$. We may suppose, in addition, that there exists an isomorphism $\iota\colon A_n \to A_m$ defined over F.

Let $k = \operatorname{ord}_p m$. It follows from the previous Corollary that p^k divides n. Hence, by Lemma E, we may replace A with A_{p^k} and suppose that p does not divide m and hence does not divide $[A[m]\colon K_m]$.

Let a denote the endomorphism of A, $a'_m \circ \iota \circ a_n$. Then $\operatorname{Ker} a \supseteq K_n$ and there exists an endomorphism b of A such that $a \circ b = mn$. Since $(m,p) = 1$ it follows from Lemma D that the reduction of b (with respect to the semi-Abelian model) is separable at all primes dividing p. But the hypotheses imply that p divides the degree of b. This contradicts Lemma C and proves the Proposition. □

PROOF OF THEOREM A. We may assume without loss of generality that A is defined over a finite extension F of $\bar{\mathbf{Q}}$ and has a semi-Abelian model over the ring of integers of F. Then A_n and a_n are defined over F.

Since, all the A_n are isogenous, they lie in finitely many isomorphism classes over F. It follows from Proposition F that the set of integers $\{[A[n]\colon K_n]\colon n \in \mathbf{N}\}$ is finite. Theorem A follows immediately. □

REMARK. Let A denote the elliptic curve $y^2 = x(x-1)(x-2)$. Then $[A[2]\colon K_2] = 2$.

REFERENCES

[F] G. Faltings, *Enlicheitsätz für Abelsche Varietäten über Zahlkörpern*, Invent. Math. **74** (1983), 349–366.

[Z] Yu G. Zarhin, *A finiteness theorem for unpolarized Abelian varieties over number fields with prescribed places of bad reduction*, Invent. Math. **79** (1985), 309–321.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94530