4. A Remark on the Rational Points of Abelian Varieties with Values in Cyclotomic Z_p-Extensions

By Hideo IMAI
Department of Mathematics, Tokyo Institute of Technology

(Comm. by Kunihiko KODAIRA, M. J. A., Jan. 13, 1975)

Let K be an algebraic number field of finite degree, p a prime integer, L/K a $\boldsymbol{Z}_p$-extension (or Γ-extension), and let A be an abelian variety defined over K. With these settings, recently Mazur [3] investigated the problem concerning the finite generatedness of the group of rational points $A(L)$. He obtained some sufficient conditions for affirmative solution of this problem. In this note we prove that the torsion part of $A(L)$ is finite if L/K is cyclotomic and if A has good reduction at some prime dividing p. In fact we prove a more general theorem:

Theorem. *Let K be a finite extension field of $\boldsymbol{Q}_p$, L the smallest field containing K and all p-power roots of* 1, *and let A be an abelian variety defined over K which has good reduction. Then the torsion part of $A(L)$ is finite.*

Proof. First we show that there is a finite extension K'/K contained in L such that L/K' is a totally ramified extension. In fact, take a finite extension $E/\boldsymbol{Q}$ such that $E\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p=E\boldsymbol{Q}_p=K$ (cf. Lang, Algebraic Number Theory, Chap. II, § 2, Proposition 4, Corollary). Let F be the smallest field containing E and all p-power roots of 1. From [1], § 7 and [3], § 2(c), there is a finite extension E'/E contained in F such that for some prime v of E' dividing p, F/E' is totally ramified at v. Then, putting K' to be the completion of E' at v, we obtain the desired field. From now on, taking K' instead of K, we assume that L/K is totally ramified. Now denote by $A(L)^{(p')}$ the p'-primary part of $A(L)$, and take $y\in A(L)^{(p')}$. If p' is relatively prime to p, then, by [8], Theorem 1, $K(y)/K$ is an unramified extension, and this means $y\in A(K)^{(p')}$. Hence $A(L)^{(p')}$ is contained in $A(K)^{(p')}$ and, from the well known fact that the torsion part of $A(K)$ is finite, we conclude that $A(L)^{(p')}$ is finite for all primes p' distinct from p and is zero for almost all p'. Therefore it is sufficient to consider the p-part $A(L)^{(p)}$.

We denote by $T_p(A)$ the Tate-module of A, $T_p(A(L))$ the fixed points of $T_p(A)$ under $\mathrm{Gal}(\bar{K}/L)$, where $\bar{K}$ is the algebraic closure of K. By the elementary divisor theorem, under suitable basis we can write these modules as: $T_p(A)=\boldsymbol{Z}_p\oplus\cdots\oplus\boldsymbol{Z}_p$, $T_p(A(L))=p^{a_1}\boldsymbol{Z}_p\oplus\cdots\oplus p^{a_n}$

$Z_p \oplus 0 \oplus \cdots \oplus 0$, where a_i are non-negative integers. We claim that all $a_1, \cdots, a_n$ are 0, i.e., $T_p(A(L))$ is a Z_p-direct summand of $T_p(A)$. To show this, it is sufficient to remark that, if $\sigma(p^a x) = p^a x$ for $\sigma \in \mathrm{Aut}_{Z_p}(T_p(A))$, $a \geqq 0$, $x \in T_p(A)$, then we have $\sigma x = x$, since $T_p(A)$ is torsion free.

Now we have the following equivalences:

$A(L)^{(p)}$ is an infinite group

$\Longleftrightarrow$ for any positive integer n, there exists an element $x_n \in A(L)$ of order p^n

$\Longleftrightarrow$ $T_p(A(L)) \neq 0$.

To see the second equivalence, we consider the projective system consisting of the sets $A_n = \{x \in A(L) \mid x \text{ is of order } p^n\}$ and the maps $p: A_n \rightarrow A_{n-1}$ which are induced from multiplication by p. As the projective limit of non-empty finite sets is non-empty (see, e.g., Serre, Cohomologie Galoisienne, § 1.4, Lemme 3), the second assertion implies the third. The converse is trivial.

Let $G = \mathrm{Gal}(L/K)$, and let $\rho: G \rightarrow \mathrm{Aut}_{Q_p} V_p(A(L))$ be the p-adic representation corresponding to $V_p(A(L)) = T_p(A(L)) \otimes_{Z_p} Q_p$, and denote by $\mathfrak{g}$ the Lie algebra of $\rho(G)$. As $T_p(A(L))$ is a Z_p-direct summand of $T_p(A)$, it may be viewed as the Tate-module of some p-divisible group over the integer ring of K, according to [9], § 4, Proposition 12. Hence we can use the Hodge-Tate decomposition for such modules (cf. [9], § 4 or [7], § 5). That is, putting $X = V_p(A(L)) \otimes_{Q_p} C$, where C is the completion of $\bar{K}$, X may be decomposed as:

$$X = X(0) \oplus X(1) \qquad \text{where } X(i) = X^{(i)} \otimes_K C,$$

and $X^{(i)} = \{x \in X \mid gx = \chi(g)^i x, \text{ for } g \in \mathrm{Gal}(\bar{K}/K)\}$, with $\chi: \mathrm{Gal}(\bar{K}/K) \rightarrow Z_p^\times$ the homomorphism such that $g\zeta = \zeta^{\chi(g)}$ for $g \in \mathrm{Gal}(\bar{K}/K)$, and for all p-power roots ζ of 1.

Now let F be the completion of the maximal unramified extension of K. Then, as the representation ρ may also be considered as the representation of $\mathrm{Gal}(\bar{F}/F)$, by [5], Theorem 1, we obtain the following characterization of the Lie algebra $\mathfrak{g}$: $\mathfrak{g}$ is the smallest subspace of $\mathrm{End}_{Q_p} V_p(A(L))$ defined over Q_p such that $\mathfrak{g} \otimes_{Q_p} C$ contains Φ ($\Phi \in \mathrm{End}_C X$ is the element such that $\Phi x = ix$ for $x \in X(i)$. Here we note that the decomposition of X with base field F is essentially the same as the decomposition $X = X(0) \oplus X(1)$, by [6], Chap. III, Appendix, Theorem 1). As G contains a subgroup of finite index which is isomorphic to Z_p, we have $\dim_{Q_p} \mathfrak{g} \leqq 1$. Hence we see that Φ is defined over Q_p. That is, $V_p(A(L)) = V_p(0) \oplus V_p(1)$ where $V_p(i) = \{x \in V_p(A(L)) \mid \Phi x = ix\}$. (In fact, we write $x \in V_p(A(L))$ as $x = (x - \Phi x) + \Phi x$, and note that $x - \Phi x$, Φx are in $V_p(A(L))$ since Φ is defined over Q_p, and these are elements of $V_p(0)$, $V_p(1)$ (respectively) since Φ is idempotent.) Note that $V_p(i)=V_p(A(L))\cap X(i)$, hence $V_p(i)$ is a G-module.

If $V_p(0)\neq 0$, then the group $\rho(G)$ restricted to $V_p(0)$ is a finite group, since its Lie algebra is 0. Hence, by extending K finitely, we see that $\mathrm{Gal}(L/K)$ acts trivially on $V_p(0)$. But this means $V_p(A(K))\neq 0$, and this contradicts the fact that torsion part of $A(K)$ is finite.

If $V_p(A(L))=V_p(1)\neq 0$, then the Lie algebra $\mathfrak{g}$ is represented in the diagonal form

$$\left\{\begin{pmatrix} x & & 0 \\ & \ddots & \\ 0 & & x \end{pmatrix} \middle| \, x\in \boldsymbol{Q}_p\right\}.$$

Hence, by extending K finitely, $\mathrm{Gal}(L/K)$ is represented by a character $\mathrm{Gal}(L/K)\to \boldsymbol{Z}_p^\times$. From the Hodge-Tate decomposition, we see that this character is equal to χ. Now let D be the integer ring of K, k its residue field, F the completion of the maximal unramified extension of K, and let R be the integer ring of F. Let $\boldsymbol{G}_m(p)$, $A(p)$ be the p-divisible groups over D obtained from the multiplicative group, and from the abelian variety A (respectively). Then, since $T_p(\boldsymbol{G}_m(p))\cong \boldsymbol{Z}_p$, $T_p(A(L))\cong \boldsymbol{Z}_p^n$ (for some n), and since $\mathrm{Gal}(L/K)$ is represented by the character χ on $T_p(A(L))$, we have a $\mathrm{Gal}(L/K)$-homomorphism (hence also a $\mathrm{Gal}(\bar{K}/K)$-homomorphism) $T_p(\boldsymbol{G}_m(p))\to T_p(A(L))\subset T_p(A)$ whose image is a non-trivial $\boldsymbol{Z}_p$-direct summand of $T_p(A)$. By [9], § 4.2, Theorem 4, Corollary 1, we have a morphism $\pi:\boldsymbol{G}_m(p)\to A(p)$ corresponding to the above homomorphism. We need the following lemma.

Lemma. *Let $A(p)$ be (any) p-divisible group over D. Let $\pi:\boldsymbol{G}_m(p)\to A(p)$ be a morphism of p-divisible groups such that, considered on Tate-modules, the image of π is a $\boldsymbol{Z}_p$-direct summand of $T_p(A(p))$. Then π is a closed immersion.*

Granting the lemma, we proceed as follows. Reduce the morphism π modulo the maximal ideal, then we obtain a closed immersion $\pi_k:\boldsymbol{G}_m(p)_k\to A(p)_k$. Consider the Frobenius endomorphism Fr on these groups (cf. [3], § 4(e)). Then, from loc. cit., the eigenvalue of Fr on $\boldsymbol{G}_m(p)_k$ (which is equal to q the number of the elements of k) is among the eigenvalues of Fr on $A(p)_k$ (whose complex absolute values are equal to $\sqrt{q}$), and this is a contradiction. From these contradictions we conclude that $V_p(A(L))=0$, i.e., $A(L)^{(p)}$ is a finite group.

Lastly we prove the lemma. As $\boldsymbol{G}_m(p)$ is a connected-étale group (i.e., it is a connected p-divisible group whose dual is étale), π factors as

$$\boldsymbol{G}_m(p)\xrightarrow{\pi'}A(p)^0\xrightarrow{i'}A(p),$$

where $A(p)^0$ is the connected component of $A(p)$. Then, considering the Cartier dual, we see that ${}^t\pi'$ factors as

$${}^t(A(p)^0)\xrightarrow{i''}({}^t(A(p)^0))^{et}\xrightarrow{\pi''}{}^t\boldsymbol{G}_m(p),$$

where the superscript t denotes the Cartier dual (cf. [9], § 2). Hence π is equal to the composite of

$$G_m(p) \xrightarrow{\pi^*} A(p)^{0,et} \xrightarrow{{}^t i''} A(p)^0 \xrightarrow{i'} A(p),$$

where $\pi^* = {}^t\pi''$ and $A(p)^{0,et} = {}^t(({}^t(A(p)^0))^{et})$. Now consider the finite groups (G_ν), (H_ν) defining ${}^t(A(p)^0)$, $({}^t(A(p)^0))^{et}$ (respectively), and write $G_\nu = \operatorname{Spec} A_\nu$, $H_\nu = \operatorname{Spec} B_\nu$. Then B_ν is the maximal étale subalgebra of A_ν (cf. [9], § 1.4). Here we show that B_ν is a D-direct summand of A_ν. In fact, as A_ν, B_ν are direct products of local rings, for this purpose we may assume that A_ν, B_ν are local rings. As B_ν is unramified over D, it is a discrete valuation ring. Consider the exact sequence of D-modules $0 \to B_\nu \to A_\nu \to A_\nu/B_\nu \to 0$. As A_ν is a free D-module, this sequence splits if and only if A_ν/B_ν is a free D-module. Suppose that A_ν/B_ν is not free. Then there exists an $x \in A_\nu$ such that $x \notin B_\nu$ and $\gamma^n x \in B_\nu$ (for some $n > 0$), where γ is a prime element of D (hence also a prime element of B_ν). As A_ν is contained in $A_\nu \otimes_D K$, and as the latter algebra is a field since $G_\nu \times_D K$ is reduced (cf. [4], Chap. III, § 11, Theorem), the above fact means that A_ν contains the fraction field of B_ν. But this implies that A_ν is not of finite type as D-module. This is a contradiction. Hence B_ν is a D-direct summand of A_ν. Now consider the D-linear duals of A_ν, B_ν. The above fact shows that ${}^t i''$ is a closed immersion. Hence to show that π is a closed immersion it is enough to show that π^* is a closed immersion. To show this, it is enough to show that $\pi^*_R : G_m(p)_R \to A(p)^{0,et}_R$ is a closed immersion, where the subscript R indicates the scalar extension to R (in fact, let $(\operatorname{Spec} A_\nu)$, $(\operatorname{Spec} B_\nu)$ be the finite groups defining $G_m(p)$, $A(p)^{0,et}$ (respectively), then by Nakayama's lemma we have the following equivalences: π^* is a closed immersion$\Leftrightarrow B_\nu \to A_\nu$ is surjective$\Leftrightarrow B_\nu \otimes k \to A_\nu \otimes k$ is surjective$\Leftrightarrow B_\nu \otimes \bar{k} \to A_\nu \otimes \bar{k}$ is surjective$\Leftrightarrow \pi^*_R$ is a closed immersion). Now from the fact that for finite group scheme G over D, G^{et} is determined by $G(\bar{k})$ with $\operatorname{Gal}(\bar{k}/k)$-action (cf. [9], § 1.4), we see that $A(p)^{0,et}$ is a connected-étale p-divisible group. Since over an algebraically closed field of characteristic p, the finite connected-étale groups are direct products of μ_{p^ν}'s (cf. [4], Chap. 3, § 14), from [3], § 4(d), Lemma 4.26, we see $(A(p)^{0,et})_R \cong (G_m(p)_R)^g$ for suitable g, and we identify these groups. Now let $\sigma : G_m(p)_R \to (G_m(p)_R)^g$ be the morphism corresponding to the first factor. Considered on the Tate-modules, the images of π^*_R and σ are Z_p-direct summands of $T_p(G_m(p)^g_R)$. Hence there exists a $\theta \in \operatorname{Aut}_{Z_p} T_p(G_m(p)^g_R) = \operatorname{Aut}_{\operatorname{Gal}(\bar{F}/F)} T_p(G_m(p)^g_R)$ such that $\pi^*_R = \theta \circ \sigma$. From [9], § 4.2, Theorem 4, Corollary 1, θ is induced by an automorphism of $(G_m(p)_R)^g$. As σ is a closed immersion, this completes the proof.

Added in proof. From the above theorem it follows in global case that if K is an algebraic number field of finite degree, L the cyclotomic

Z_p-extension, and if A is an abelian variety defined over K with good reduction at some prime dividing p, then the torsion part of $A(L)$ is finite. After he had completed this paper, the author was informed that in the global case Serre proved a more general theorem by a different way.

References

[1] K. Iwasawa: On Γ-extensions of algebraic number fields. Bull. Amer. Math. Soc., **65**, 183–226 (1959).

[2] Ju. Manin: Cyclotomic fields and modular curves. Russ. Math. Surveys, **26**, 7–78 (1971).

[3] B. Mazur: Rational points of abelian varieties with values in towers of number fields. Inventiones math., **18**, 183–266 (1972).

[4] D. Mumford: Abelian Varieties. Oxford Univ. Press, London (1970).

[5] S. Sen: Lie algebras of Galois groups arising from Hodge-Tate modules. Ann. of Math., **97**, 160–170 (1973).

[6] J.-P. Serre: Abelian l-adic representations and elliptic curves. Benjamin Inc. New York (1968).

[7] ——: Sur les groupes de Galois attachés aux groupes p-divisibles. Proceedings of a Conference on Local Fields, pp. 118–131. Springer, Berlin-Heidelberg-New York (1967).

[8] J.-P. Serre and J. Tate: Good reduction of abelian varieties. Ann. of Math., **88**, 492–517 (1968).

[9] J. Tate: p-Divisible Groups. Proceedings of a Conference on Local Fields, pp. 158–183. Springer, Berlin-Heidelberg-New York (1967).