

APPENDIX: TORSION POINTS OF ABELIAN VARIETIES IN CYCLOTOMIC EXTENSIONS

Autor(en): **Ribet, Kenneth A.**

Objektyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **27 (1981)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **29.05.2024**

Persistenter Link: <https://doi.org/10.5169/seals-51754>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

APPENDIX: TORSION POINTS OF ABELIAN VARIETIES IN CYCLOTOMIC EXTENSIONS

by Kenneth A. RIBET ¹⁾

Let k be a number field, and let \bar{k} be an algebraic closure for k . For each prime p , let K_p be the subfield of k obtained by adjoining to k all p -power roots of unity in \bar{k} . Let K be the compositum of all of the K_p , i.e., the field obtained by adjoining to k all roots of unity in \bar{k} .

Suppose that A is an abelian variety over k . Mazur has raised the question of whether the groups $A(K_p)$ are finitely generated [4]. In this connection, H. Imai [1] and J.-P. Serre [5] proved (independently) that the *torsion subgroup* of $A(K_p)$ is finite for each p . The aim of this appendix is to prove that more precisely one has the following theorem, cf. [3], §II, Remark 3.

THEOREM 1. *The torsion subgroup $A(K)_{\text{tors}}$ of $A(K)$ is finite.*

Let G be the Galois group $\text{Gal}(\bar{k}/k)$ and let H be its subgroup $\text{Gal}(\bar{k}/K)$. For each positive integer n , let $A[n]$ be the kernel of multiplication by n in $A(\bar{k})$. For each prime p , let V_p be the \mathbf{Q}_p -adic Tate module attached to A . If M is one of these modules, we denote by M^H the set of elements of M left fixed by H . Since H is normal in G , M^H is stable under the action of G on M .

Because of the structure of the torsion subgroup of $A(\bar{k})$, one sees easily that Theorem 1 is equivalent to the conjunction of the following two statements:

THEOREM 2. *For all but finitely many primes p , we have $A[p]^H = 0$.*

THEOREM 3. *For each prime p , we have $V_p^H = 0$.*

Indeed, Theorem 2 asserts the vanishing of the p -primary part of $A(K)_{\text{tors}}$, while Theorem 3 asserts the finiteness of this p -primary part.

¹⁾ Partially supported by National Science Foundation contract number MCS 80-02317.

In proving these statements, we visibly have the right to replace k by a finite extension of k . Therefore, using ([SGA 71], IX, 3.6) we can (and will) assume that A/k is semistable. Next, consider the largest subextension k' of K/k which is unramified at all finite places of k .

LEMMA. *For each prime p , let L_p be the largest extension of k in K which is unramified at all places of k except for primes dividing p and the infinite places of k . Then L_p is the compositum $k'K_p$.*

Proof. Let A be the Galois group $\text{Gal}(K/k)$, viewed as a subgroup of $\hat{\mathbf{Z}}^*$. We consider $\hat{\mathbf{Z}}^*$ as the direct product of its two subgroups \mathbf{Z}_p^* and $\prod_{l \neq p} \mathbf{Z}_l^*$. Let I (resp. J) be the subgroup of A generated by the inertia groups of A for primes of k which divide p (resp. which do not divide p). Then I is a subgroup of \mathbf{Z}_p^* , while J is a subgroup of $\prod_{l \neq p} \mathbf{Z}_l^*$. The product $I \times J$ is the subgroup of A generated by all inertia groups of A . We have $J = \text{Gal}(\bar{k}/L_p)$, $I \times J = \text{Gal}(\bar{k}/k')$, and $\text{Gal}(\bar{k}/K_p) = A \cap \left(\prod_{l \neq p} \mathbf{Z}_l^*\right)$. Now $\text{Gal}(\bar{k}/k'K_p)$ is the intersection of the two Galois groups $\text{Gal}(\bar{k}/k')$ and $\text{Gal}(\bar{k}/K_p)$. Putting these facts together, we prove the desired assertion.

We now replace k by its finite extension k' . With this replacement made, K_p becomes equal to L_p . Furthermore, for odd primes p , the largest extension of k in K which is unramified outside p and infinity and which has degree prime to p is the field obtained by adjoining to k the p -th roots of unity in \bar{k} .

Proof of Theorem 2. We shall consider only primes p which are odd, unramified in k , and such that A has good reduction at at least one prime of k dividing p . Let p be such a prime and v a prime of k over p at which A has good reduction. Suppose that the G -module $A[p]^H$ is non-zero, and let W be a simple G -submodule of this module. The algebra $\text{End}_G W$ is a finite field \mathbf{F} , and the action of G on W is given by a character

$$\phi: G \rightarrow \mathbf{F}^*$$

since the action of G on $A[p]^H$ is abelian. (Here the point is simply that G/H is an abelian group.) In particular, the image of G in $\text{Aut}(A[p])$ has order prime to p . On the other hand, the character ϕ is unramified at primes of k not dividing p because A/k is semistable. By the discussion following the lemma, we know that ϕ factors through the quotient $\text{Gal}(k(\mu_p)/k)$ of G ; here, μ_p denotes the group of p -th roots of unity. In particular, ϕ must have order dividing $p - 1$, so that its

values lie in the prime field \mathbf{F}_p . Since W was chosen to be simple, its dimension over \mathbf{F}_p must be 1; i.e., W is a group of order p .

Let $\chi: G \rightarrow \mathbf{F}_p^*$ be the mod p cyclotomic character, i.e., the character giving the action of G on μ_p . Since ϕ factors through $\text{Gal}(k(\mu_p)/k)$, we may write ϕ in the form χ^n , where n is an integer mod $(p-1)$. We claim that n can only be 0 or 1.

To verify this claim, it is enough to check that it is true after we replace G by an inertia group I in G for the prime v , since χ is totally ramified at v . We remark that W is the I -module associated to a finite flat commutative group scheme \mathcal{W} over the ring of integers of the completion of k at v , since v is such that A has good reduction at v . Because \mathcal{W} has order p , the classification of Tate-Oort ([8], especially pp. 15-16) applies to \mathcal{W} . Because v is absolutely unramified, the classification shows immediately that \mathcal{W} is either étale or the dual of an étale group. In the former case, I acts trivially on W ; in the latter case, I acts on W via χ . This completes the verification of the claim.

Thus, if Theorem 2 is false, there are infinitely many primes p for which $A[p]$ contains a G -submodule isomorphic to either $\mathbf{Z}/p\mathbf{Z}$ or to μ_p . Of course, the former case can occur only a finite number of times, since $A(k)$ is finite. One way to rule out the latter case is to argue that whenever μ_p is a submodule of $A[p]$, the group $\mathbf{Z}/p\mathbf{Z}$ is a quotient of the dual of $A[p]$, which is the kernel of multiplication by p on the abelian variety A^\vee dual to A . In other words, if μ_p occurs as a submodule of $A[p]$, then there is an abelian variety isogenous to A^\vee (and therefore in fact to A) which has a rational point of order p over k . Therefore p is a divisor of the order of a finite group that may be specified in advance, viz. the group of rational points of any reduction of A at a good unramified prime of k of residue characteristic different from 2. (See the appendix to Katz's recent paper [2] for a discussion of this point.)

Proof of Theorem 3. Suppose that p is a prime such that V_p^H is non-zero. We again choose W to be an irreducible G -submodule (i.e., $\mathbf{Q}_p[G]$ -submodule) of V_p^H . Because the action of G on W is abelian, and because W is simple, each element of G acts semisimply on W . Since A/k is semistable, it follows that the homomorphism

$$\rho: G \rightarrow \text{Aut}(W)$$

giving the action of G on W is unramified at all primes of k not dividing p . Therefore, ρ factors through $\text{Gal}(K_p/k)$ in view of the lemma and the subsequent replacement $k \rightarrow k'$. In other words, starting from the hypothesis that the p -torsion subgroup of $A(K)$ is infinite, we have deduced that the p -torsion subgroup of $A(K_p)$ is infinite.

Of course, this situation is ruled out by the theorem of Imai and Serre mentioned above. Nevertheless, we will sketch for the reader's convenience an argument which leads to a contradiction. Let v be a place of k dividing p , and let $D \subset G$ be a decomposition group for v . By ([SGA 71], IX, Prop. 5.6), the D -module V_p is an extension of D -modules attached to p -divisible groups over the integer ring of the completion of k at v . Because of Tate's theory [7], the semisimplification V_p^{ss} of the D -module V_p has a Hodge-Tate decomposition. (Here we should remark that submodules and quotients of Hodge-Tate modules are again Hodge-Tate.) Since W is semisimple as a D -module (because semisimple and *abelian* as a G -module), W may be viewed as a submodule of V_p^{ss} . Therefore, W is a Hodge-Tate module.

By ([6], III, Appendix), we know that ρ is a locally algebraic abelian representation of G . Using this information, plus the fact that ρ factors through $\text{Gal}(K_p/k)$, we find that there is an open subgroup G_0 of G with the following property: the restriction of ρ to G_0 is the direct sum of 1-dimensional representations, each described by an integral power χ_p^n of the standard cyclotomic character $\chi_p: G \rightarrow \mathbf{Z}_p^*$. After replacing k by a finite extension, we may assume that G_0 is G . Take a prime w of k which is prime to p and such that A has good reduction at w . Let $g \in G$ be a Frobenius element for w . The eigenvalues of $\rho(g)$ will be integral powers of $\chi_p(g)$, i.e., of the norm Nw of w . However, by a well known theorem of Weil, these eigenvalues all have archimedian absolute values equal to $(Nw)^{1/2}$. This contradiction completes the proof of Theorem 3.

REFERENCES

- [1] IMAI, H. A remark on the rational points of abelian varieties with values in cyclotomic \mathbb{Z}_p extensions. *Proc. Japan Acad.* 51 (1975), 12-16.
- [2] KATZ, N. Galois properties of torsion points on abelian varieties. *Invent. Math.* 62 (1981), 481-502.
- [3] KATZ, N. and S. LANG. Finiteness theorems in geometric classfield theory.
- [4] MAZUR, B. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* 18 (1972), 183-266.
- [5] SERRE, J.-P. Letters to B. Mazur, January, 1974.
- [6] ——— *Abelian l -adic Representations and Elliptic Curves*. New York: Benjamin 1968.
- [7] TATE, J. p -divisible groups. In: *Proceedings of a Conference on Local Fields*. Berlin-Heidelberg-New York: Springer-Verlag 1967.
- [8] TATE, J. and F. OORT. Group schemes of prime order. *Ann. scient. Éc. Norm. Sup.*, 4^e série 3 (1970), 1-21.
- [SGA 71] *Groupes de Monodromie en Géométrie Algébrique* (séminaire dirigé par A. Grothendieck avec la collaboration de M. Raynaud et D. S. Rim). *Lecture Notes in Math.* 288 (1972).

(Reçu le 20 janvier 1981)

Kenneth A. Ribet

U.C. Berkeley
Mathematics Department
Berkeley, Ca. 94720
USA

Vide-leer-empty