On the Universal Norms of Some Abelian Varieties Over Local Fields

Hideo IMAI

*Graduate School of Information Sciences, Tohoku University,
Aoba-ku, Sendai 980-77, Japan*

Let F be a finite extension field of $\mathbf{Q}_p$, A an abelian variety defined over F with ordinary good reduction and with sufficiently many endomorphisms (see the theorem below for a precise statement). In this paper we prove that there exists unique Galois extension M of F such that for a Galois extension K of F, the group $N_{K/F}(A)$ of universal norms is finite if and only if K contains M. Our result generalizes that of J. Coates and R. Greenberg [1] which concerns the case of elliptic curves.

KEYWORDS: abelian variety, universal norm

1. Introduction

The problem concerning the universal norms of an abelian variety A for an extension K/F of local fields was first treated by B. Mazur in [2]. In that paper he considered the case when A has ordinary good reduction and the extension K/F is a ramified $\mathbf{Z}_p$-extension. Using the theory of pro-algebraic groups, he obtained the results which state that the group of universal norms $N_{K/F}(A)$ is of finite index in $A(F)$, and under some conditions he determined the structure of the group $A(F)/N_{K/F}(A)$ (cf. [2], Proposition 4.42). Recently, in [1], J. Coates and R. Greenberg took up this problem again. Their method differs from that used by B. Mazur, and is mainly the ramification theory of local fields which was previously used by J. Tate in [3]. This method enabled them to treat more general extensions than those treated by B. Mazur. In particular, they proved that when A is an elliptic curve defined over $\mathbf{Q}_p$ with ordinary good reduction, there exists unique Galois extension M over $\mathbf{Q}_p$ such that, for a Galois extension K of $\mathbf{Q}_p$, $N_{K/\mathbf{Q}_p}(A)$ is finite if and only if K contains M (cf. [1], Proposition 5.8). In this paper we generalize this fact to (some) abelian varieties.

2. Main result

Let p be a prime number, $\mathbf{Q}_p$ the p-adic rational number field and $\bar{\mathbf{Q}}_p$ a fixed algebraic closure of $\mathbf{Q}_p$. Let F be a finite extension of $\mathbf{Q}_p$ lying inside $\bar{\mathbf{Q}}_p$, $\mathcal{O}_F$ the integer ring of F, m_F the maximal ideal of $\mathcal{O}_F$ and k_F the residue field of $\mathcal{O}_F$. Let A be an abelian variety of dimension g defined over F and A^t the dual abelian variety of A. If X is a torsion abelian group, we write $X(p)$ for its p-primary subgroup and if X is a profinite abelian group, we write X_p for its maximal pro-p subgroup.

Let $G_F = G(\bar{\mathbf{Q}}_p/F)$ be the Galois group of $\bar{\mathbf{Q}}_p$ over F and for a continuous G_F-module X, $H^i(F, X) = H^i(G_F, X)$ be its continuous cohomology group. For any extension K of F contained in $\bar{\mathbf{Q}}_p$, let

$$r_{K/F}: H^1(F, A(\bar{\mathbf{Q}}_p))(p) \to H^1(K, A(\bar{\mathbf{Q}}_p))(p)$$

be the restriction homomorphism.

We define the universal norms of A^t for the extension K/F as

$$N_{K/F}(A^t) = \bigcap_{F'} N_{F'/F}(A^t(F'))$$

where F' runs over all finite extensions of F contained in K, and $N_{F'/F}$ denotes the norm map from F' to F on A^t.

Then Tate duality asserts that $A^t(F)_p$ is canonically dual to $H^1(F, A(\bar{\mathbf{Q}}_p))(p)$. Moreover, $N_{K/F}(A^t)_p$ is the exact orthogonal complement of $\mathrm{Ker}\,(r_{K/F})$ in this duality. Thus, $\mathrm{Im}\,(r_{K/F})$ is canonically dual to $N_{K/F}(A^t)_p$.

Now suppose A has ordinary good reduction modulo m_F.

Let $\tilde{A}$ be the reduction of $A \bmod m_F$ and $D = \tilde{A}[p^\infty]$ the p-primary subgroup of $\tilde{A}(k_F^{\mathrm{sep}})$. Then D is a $\mathbf{Z}_p$-module co-free of corank g. From the action of G_F on D we obtain an unramified homomorphism

$$\phi: G_F \to \mathrm{Aut}\,(D).$$

Let L be the fixed field of the kernel of ϕ, then L is an unramified extension of F and $G(L/F)$ is isomorphic to the Galois group of its residue field extensions. Hence $G(L/F)$ is topologically cyclic, and $G(L/F) \simeq \Delta \times \Gamma$,

where $\Gamma \simeq \mathbf{Z}_p$ and Δ is a finite group of order prime to p.

Lemma *Under the above notations the restriction map*

$$\rho_{L/F}: H^1(F, D) \to H^1(L, D) = \mathrm{Hom}\,(G_L, D)$$

is injective.

Proof. From the inflation-restriction exact sequence we have

$$\mathrm{Ker}\,(\rho_{L/F}) \simeq H^1(G(L/F), D^{G_L}) = H^1(G(L/F), D).$$

Let γ be a topological generator of $G(L/F)$, and $\gamma' \in \mathrm{Aut}\,(D)$ the image of γ under the map ϕ (note that ϕ factors through $G(L/F)$).

Now $\mathrm{Ker}\,(\gamma' - 1) = \tilde{A}(k_F)[p^\infty]$ is a finite group. As D is isomorphic to $(\mathbf{Q}_p/\mathbf{Z}_p)^g$, this implies that the map $g' - 1: D \to D$ is surjective. Hence $H^1(G(L/F), D) = 0$. ∎

Remark. As p-cohomological dimension of $G(L/F)$ is 1 and D is torsion, we have $H^2(G(L/F), D) = 0$. So the map in lemma gives in fact an isomorphism $H^1(F, D) \simeq H^1(L, D)^{G(L/F)} = \mathrm{Hom}_{G(L/F)}(G_L, D)$.

As above D is a G_F-module of $\mathbf{Z}_p$-corank g and $H^0(F, D)$ is finite. From the Weil pairing and local duality, we see that $H^2(F, A[p^\infty])$ is canonically dual to $H^0(F, T_p(A')) = 0$, so $H^2(F, A[p^\infty]) = 0$. Let C be the kernel of the reduction map on $A[p^\infty]$, then we have the following exact sequence of G_F-modules

$$0 \to C \to A[p^\infty] \to D \to 0.$$

Taking G_F-cohomology of the above exact sequence and recalling that G_F has cohomological dimension equal to 2, we deduce that $H^2(F, D) = 0$. From the Euler-Poincare characteristic of D over F we have

$$\mathrm{corank}_{\mathbf{Z}_p} H^1(F, D) = g[F: \mathbf{Q}_p].$$

Let $H^1(F, D)_{\mathrm{div}}$ be the maximal divisible subgroup of $H^1(F, D)$, and $Y = \rho_{L/F}(H^1(F, D)_{\mathrm{div}})$ be its image in $H^1(G_L, D) = \mathrm{Hom}\,(G_L, D)$. From the lemma, we see

$$Y \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^{g[F:\mathbf{Q}_p]}.$$

Let $H \subseteq G_L$ be the subgroup whose elements are annihilated by Y:

$$H = \{\sigma \in G_L \,|\, f(\sigma) = 0 \quad (\forall f \in Y)\}.$$

Let $M \subset \bar{\mathbf{Q}}_p$ be the fixed field of H. Then we have a natural injection

$$Y \hookrightarrow \mathrm{Hom}\,(G(M/L), D).$$

From the construction, M is an abelian extension of L, $\mathrm{rank}_{\mathbf{Z}_p} G(M/L) \geq [F: \mathbf{Q}_p]$, and as Y is a submodule of $\mathrm{Hom}_{G_F}(G_L, D)$, M is Galois over F. It is plain that the extension M over L is ramified, and so is infinitely wildly ramified (M contains a $\mathbf{Z}_p^{[F:\mathbf{Q}_p]}$-extension of L). Note also that M is determined only by the reduction $\tilde{A}$ of A.

Now we can state our main result.

Theorem *Let A be an abelian variety of dimension g defined over F with ordinary good reduction. Suppose $\mathrm{End}\,(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ contains a number field E of degree g in which p does not split. Let K be a Galois extension of F and let M be the field defined as above. Then $N_{K/F}(A')$ is finite if and only if $K \supseteq M$.*

Before proving the theorem, we recall some basic facts on the cohomology groups related to A, which were proved in [1].

Let $\mathcal{F}$ be the formal group over $\mathcal{O}_F$ attached to the Neron model of A over $\mathcal{O}_F$, $\bar{m}$ the maximal ideal of the integer ring of $\bar{\mathbf{Q}}_p$. $\mathcal{F}$ may be written by a family $f(X, Y) = (f_i(X, Y))$ of g formal power series in $2g$ variables X_i, $Y_i (i = 1, 2, \cdots, g)$, with coefficients in $\mathcal{O}_F$.

Let K be any field with $F \subseteq K \subseteq \bar{\mathbf{Q}}_p$. We define $\mathcal{F}(m_K)$ to be the set m_K^g, endowed with the abelian group low
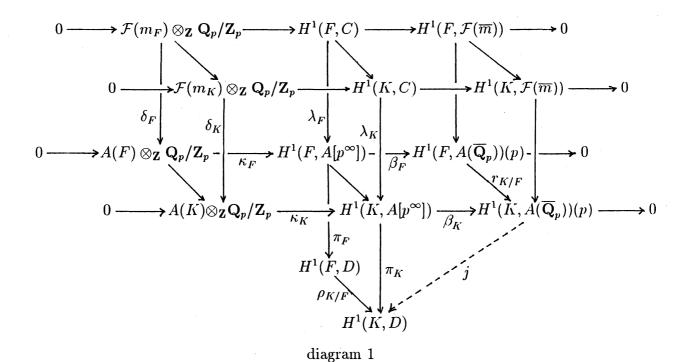
$$x \otimes y = f(x, y);$$

even though K is not in general complete, the power series on the right converge to an element of m_K^g, because of our hypothesis that the coefficients of $\mathcal{F}$ belong to F a finite extension field of $\mathbf{Q}_p$.

The formal group $\mathcal{F}$ is often described as the kernel of the reduction map on A, and we have the following exact sequences:

$$0 \to \mathcal{F}(\bar{m}) \to A(\bar{\mathbf{Q}}_p) \to \tilde{A}(k_F^{\mathrm{sep}}) \to 0$$

$$0 \to C \to A[p^\infty] \to D \to 0.$$

From these sequences and the Kummer sequence, we have the following diagram of exact sequences for any field K with $F \subseteq K \subseteq \bar{\mathbf{Q}}_p$ (cf. the diagram (4.8) of [1], p. 152).

$$0 \longrightarrow \mathcal{F}(m_F) \otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow H^1(F, C) \longrightarrow H^1(F, \mathcal{F}(\overline{m})) \longrightarrow 0$$

$$0 \longrightarrow \mathcal{F}(m_K) \otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow H^1(K, C) \longrightarrow H^1(K, \mathcal{F}(\overline{m})) \longrightarrow 0$$

$$0 \longrightarrow A(F) \otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{\ \kappa_F\ } H^1(F, A[p^\infty]) \xrightarrow{\ \beta_F\ } H^1(F, A(\overline{\mathbf{Q}}_p))(p) \longrightarrow 0$$

$$0 \longrightarrow A(K) \otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{\ \kappa_K\ } H^1(K, A[p^\infty]) \xrightarrow{\ \beta_K\ } H^1(K, A(\overline{\mathbf{Q}}_p))(p) \longrightarrow 0$$

with maps δ_F, δ_K, λ_F, λ_K, $r_{K/F}$, and $H^1(F, D)$, π_F, π_K, $\rho_{K/F}$, j, $H^1(K, D)$.

diagram 1

About this diagram, the following facts are known: As $\mathcal{F}(m_F)$ is a finite index subgroup of $A(F)$, δ_F is surjective, hence δ_K is also surjective. The surjectivity of δ_K implies Im $(\kappa_K) \subseteq$ Im (λ_K), and this implies Ker $(\beta_K) \subseteq$ Ker (π_K), so the dotted homomorphism j is defined.

If A has ordinary good reduction and if K is infinitely wildly ramified over F, then the equality Im $(\kappa_K) =$ Im (λ_K) holds (cf. [1], Proposition 4.7), and in this case j is injective. If A has potential good reduction, then π_F is surjective (cf. [1], Proposition 5.3).

Proof of the theorem. By a well-known theorem of Mattuck, we have an isomorphism

$$A'(F) \simeq \mathbf{Z}_p^{g[F:\mathbf{Q}_p]} \times \text{(a finite group)}.$$

Let F' be any finite extension of F which is contained in K. Then $N_{F'/F}(A'(F'))$ is a closed subgroup of $A'(F)$, because $N_{F'/F}$ is continuous and $A'(F')$ is compact. Hence $N_{K/F}(A')$ is also a closed subgroup of $A'(F)$, so must be of the form $N_{K/F}(A') \simeq \mathbf{Z}_p^u \times$ (a finite group). So $N_{K/F}(A')$ is finite if and only if $N_{K/F}(A')_p$ is finite. Suppose first that $M \subseteq K$, then the restriction map factors as follows

$$\rho_{K/F}: H^1(F, D) \hookrightarrow H^1(L, D) = \text{Hom}(G_L, D) \to H^1(M, D) \to H^1(K, D).$$

By definition, $H^1(F, D)_{\text{div}}$ maps to 0 in $H^1(M, D)$.

We also see from the above factorization, for field K containing L, K contains M if and only if Ker $(\rho_{K/F})$ contains $H^1(F, D)_{\text{div}}$.

As M is infinitely wildly ramified over F, the diagram 1, the injectivity of j and the surjectivity of π_F imply the following (here $X^\wedge$ is the Pontrjagin dual of an abelian group X):

$$N_{K/F}(A')_p \simeq (\text{Im}(r_{K/F}))^\wedge = (\text{Im}(j \circ r_{K/F} \circ \beta_F))^\wedge = (\text{Im}(\rho_{K/F} \circ \pi_F))^\wedge = (\text{Im}(\rho_{K/F}))^\wedge$$
$$\simeq (H^1(F, D)/\text{Ker}(\rho_{K/F}))^\wedge \simeq \text{(a subgroup of } (H^1(F, D)/H^1(F, D)_{\text{div}})^\wedge).$$

The last group is finite.

Conversely assume that $N_{K/F}(A')$ is finite. Then K must be infinitely wildly ramified over F by [1], Lemma 5.1. Hence in the diagram 1 the map j is injective. From the diagram 1 and surjectivity of π_F, we have as before

$$N_{K/F}(A') \simeq (H^1(F, D)/\text{Ker}(\rho_{K/F}))^\wedge,$$

and the finiteness of this group implies Ker $(\rho_{K/F}) \supseteq H^1(F, D)_{\text{div}}$.

As Ker $(\rho_{K/F}) = H^1(G(K/F), D(K))$, this implies in particular that $D(K)$ is infinite (note that $\mathbf{Z}_p$-corank of $H^1(F, D)$ is not 0).

Now from the hypothesis $E \otimes_{\mathbf{Q}} \mathbf{Q}_p$ is an extension field of $\mathbf{Q}_p$ of degree g.

Consider the p-adic Tate module $T_p(D) = \text{proj} \lim D[p^n]$ associated to D and the p-adic space $V_p(D) = T_p(D) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.

$V_p(D)$ is a $E \otimes_{\mathbf{Q}} \mathbf{Q}_p$-vector space of dimension 1 on which G_K acts continuously.

From the infiniteness of $D(K)$ we have $T_p(D)^{G_K} \neq 0$ and from this we have $V_p(D)^{G_K} = V_p(D)$. Hence $\tilde{A}[p^\infty]$ $= D(K)$ and $K \supseteq L$. From Ker $(\rho_{K/F}) \supseteq H^1(F, D)_{\mathrm{div}}$, we have $K \supseteq M$. This completes the proof. ∎

REFERENCES

[1]   J. Coates and R. Greenberg: Kummer theory for abelian varieties over local fields. Invent. math. **124**, 129–174 (1996)

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

[3]   J. Tate: p-divisible groups, Proceedings of a conference on local fields (Driebergen, 1966), 159–183, Springer, 1967