

ON TATE-SHAFAREVICH GROUPS OF ABELIAN VARIETIES

CRISTIAN D. GONZALEZ-AVILÉS

(Communicated by David E. Rohrlich)

To Ricardo Baeza with gratitude

ABSTRACT. Let K/F be a finite Galois extension of number fields with Galois group G , let A be an abelian variety defined over F , and let $\text{III}(A/K)$ and $\text{III}(A/F)$ denote, respectively, the Tate-Shafarevich groups of A over K and of A over F . Assuming that these groups are finite, we derive, under certain restrictions on A and K/F , a formula for the order of the subgroup of $\text{III}(A/K)$ of G -invariant elements. As a corollary, we obtain a simple formula relating the orders of $\text{III}(A/K)$, $\text{III}(A/F)$ and $\text{III}(A^\chi_F)$ when K/F is a quadratic extension and A^χ is the twist of A by the non-trivial character χ of G .

1. INTRODUCTION

This paper is the first progress report of an ongoing investigation whose aim is to determine the behavior of the Tate-Shafarevich group of an abelian variety A under extensions of the field of definition of A . To be precise, let A be an abelian variety defined over a number field F , let K/F be a finite Galois extension with Galois group G , and let $\text{III}(A/K)$ and $\text{III}(A/F)$ denote, respectively, the Tate-Shafarevich groups of A over K and of A over F . We assume throughout that these groups are finite. Then our chief aim is to find a simple relation between the orders of $\text{III}(A/K)$ and $\text{III}(A/F)$, if such a relation exists. A partial solution to this problem is implicit in a 1972 paper of Milne ([9], Corollary to Theorem 3), who obtained his result making certain assumptions on $\text{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. We have adopted a different approach here, which works well for abelian varieties A and field extensions K/F as above which satisfy the following two conditions:

- (A) $\hat{H}^p(G, A(K)) = \hat{H}^p(G, A'(K)) = 0$ for all p .
- (B) Either F is totally imaginary or both $A(F_v)$ and $A'(F_v)$ are connected for every real prime v of F .

Here A' denotes the dual abelian variety of A . Thus, for example, A could be an elliptic curve defined over \mathbb{Q} given by a Weierstrass equation of negative discriminant and K could be a finite Galois extension of \mathbb{Q} such that $A(K)$ is finite and of order prime to the degree $[K : \mathbb{Q}]$ (see Corollary V.2.3.1 of [14] and §6 of [1]). Our main result is the following.

Received by the editors May 18, 1998.

1991 *Mathematics Subject Classification*. Primary 11G40, 11G05.

The author was supported by Fondecyt grant 1981175.

Main Theorem. *Assume that conditions (A) and (B) above hold. Then*

$$\#\text{III}(A/K)^G = \#\text{III}(A/F) \cdot \prod_{v \in S} \#H^1(G_w, A(K_w)).$$

Furthermore,

$$\#H^1(G, \text{III}(A/K)) = \prod_{v \in S} \#H^2(G_w, A(K_w)).$$

Here S denotes the set of primes of F obtained by collecting together the primes that ramify in K/F and the primes of bad reduction for A/F , w is a fixed prime of K lying above v for each $v \in S$, and G_w denotes the Galois group of K_w over F_v .

The above theorem has the following corollary, which solves the problem of relating $\#\text{III}(A/K)$ to $\#\text{III}(A/F)$ in a special case.

Corollary. *Suppose that K/F is a quadratic extension and let χ denote the non-trivial character of $G = \text{Gal}(K/F)$. Assume that conditions (A) and (B) above hold for both A and its quadratic twist A^χ . Then*

$$\#\text{III}(A/K) = \#\text{III}(A/F) \cdot \#\text{III}(A^\chi/F) \cdot \prod_{v \in S} \#H^1(G_w, A(K_w)).$$

2. LOCAL COMPUTATIONS

If M is a topological abelian group, we will write M^* for the group of continuous characters of finite order of M , i.e. $M^* = \text{Hom}_{\text{cts}}(M, \mathbb{Q}/\mathbb{Z})$. Also, if G is a finite group, M is a G -module and p is any integer, then $\hat{H}^p(G, M)$ will denote the p -th Tate cohomology group of M (see §6 of [1]). In particular, if we write M_G for the largest quotient of M on which G acts trivially and $N^* : M_G \rightarrow M^G$ for the map induced by multiplication by $N = \sum_{\sigma \in G} \sigma \in \mathbb{Z}[G]$ on M , then

$$(1) \quad \hat{H}^{-1}(G, M) = \ker(N^*) \quad \text{and} \quad \hat{H}^0(G, M) = \text{coker}(N^*).$$

Let A be an abelian variety defined over a number field F . For any field $L \supset F$, we will write G_L for $\text{Gal}(\bar{L}/L)$, where \bar{L} is an algebraic closure of L . Further, we will write $H^p(L, A)$ for $H^p(G_L, A(\bar{L}))$ and A' for the dual abelian variety of A .

Now let K be a finite Galois extension of F and let G be the Galois group of K over F . For any prime w of K , we let $G_w = \text{Gal}(K_w/F_v) \subset G$ be the decomposition group of w over F , where v is the prime of F lying below w . Finally, we will write res_w for the local restriction map $H^1(F_v, A) \rightarrow H^1(K_w, A)$.

Lemma 2.1. *Let w be a prime of K and let v be the prime of F lying below w .*

(i) *If w is archimedean, then there is an exact sequence*

$$0 \rightarrow H^1(G_w, A(K_w)) \rightarrow H^1(F_v, A) \xrightarrow{\text{res}_w} H^1(K_w, A)^{G_w} \rightarrow 0.$$

(ii) *If w is non-archimedean, then there is an exact sequence*

$$0 \rightarrow H^1(G_w, A(K_w)) \rightarrow H^1(F_v, A) \xrightarrow{\text{res}_w} H^1(K_w, A)^{G_w} \rightarrow H^2(G_w, A(K_w)) \rightarrow 0.$$

Proof. Assertion (i) is easy to check. Assertion (ii) follows from the exactness of the sequence

$$H^1(G_w, A(K_w)) \hookrightarrow H^1(F_v, A) \xrightarrow{\text{res}_w} H^1(K_w, A)^{G_w} \rightarrow H^2(G_w, A(K_w)) \rightarrow H^2(F_v, A)$$

(which is the exact sequence of terms of low degree belonging to the Hochschild-Serre spectral sequence $H^p(G_w, H^q(K_w, A)) \implies H^{p+q}(F_v, A)$) and the fact that $H^2(F_v, A) = 0$ for v non-archimedean (see [5] and Corollary I.3.4 of [8]). \square

In what follows, $H^0(F_v, A')$ denotes $A'(F_v)$ unless v is archimedean, in which case it denotes $\hat{H}^0(F_v, A') = A'(F_v)/N_{\bar{F}_v/F_v}A'(\bar{F}_v)$. Similarly for $H^0(K_w, A')$.

Lemma 2.2. *Let v be any prime of F . Then the dual of the map $\bigoplus_{w|v} \text{res}_w : H^1(F_v, A) \rightarrow \bigoplus_{w|v} H^1(K_w, A)$ is the map $\prod_{w|v} H^0(K_w, A') \rightarrow H^0(F_v, A')$ induced by*

$$\prod_{w|v} A'(K_w) \rightarrow A'(F_v), \quad (x_w)_{w|v} \mapsto \sum_{w|v} N_{K_w/F_v}(x_w).$$

Proof. If v is archimedean, the verification of the above statement is straightforward, using Remark I.3.7 of [8]. If v is non-archimedean, the lemma follows easily from Tate’s local duality theory [15]. □

Now let S denote the set of primes of F obtained by collecting together all primes which ramify in K/F and all primes of bad reduction for A/F . Further, let S_∞ be the set of archimedean primes of F .

Lemma 2.3. *Let w be a prime of K and let v be the prime of F lying below w . Assume that $v \notin S \cup S_\infty$. Then for every $p \geq 1$,*

$$H^p(G_w, A(K_w)) = 0.$$

Proof. The case $p = 1$ of this result is well-known ([7], Corollary 4.4). For the general case, see Lemma 3.5 of [12]. □

Recall $G = \text{Gal}(K/F)$ and let v be any prime of F . Then $\bigoplus_{w|v} H^q(K_w, A)$ can be made into a G -module in the following natural way. For $\sigma \in G$ and $(\xi_w)_{w|v} \in \bigoplus_{w|v} H^q(K_w, A)$, let $\sigma(\xi_w)_{w|v} = (\sigma_*^{-1} \xi_{\sigma w})_{w|v}$, where $\sigma_* : H^q(K_w, A) \rightarrow H^q(K_{\sigma w}, A)$ is the homomorphism associated to the maps $G_{K_{\sigma w}} \rightarrow G_{K_w}$, $\nu \mapsto \bar{\sigma}^{-1} \nu \bar{\sigma}$, and $A(\bar{K}_w) \rightarrow A(\bar{K}_{\sigma w})$, $P \mapsto \bar{\sigma} P$, where $\bar{\sigma} : \bar{K}_w \xrightarrow{\sim} \bar{K}_{\sigma w}$ is some lifting of $\sigma : K_w \xrightarrow{\sim} K_{\sigma w}$ (see [13], p. 115). It is not difficult to see that with this G -action, $\bigoplus_{w|v} H^q(K_w, A)$ becomes a semi-local G -module in the sense of [3]. Thus we have the following

Lemma 2.4. *Let v be any prime of F . Then for every $p \geq 0$ and $q \geq 0$, there is a canonical isomorphism*

$$H^p\left(G, \bigoplus_{w|v} H^q(K_w, A)\right) \simeq H^p(G_w, H^q(K_w, A)),$$

where the w on the right denotes any prime of K lying above v .

Proof. See §2.1 of [3]. □

Let v be a prime of F . It is easy to check that the image of the map $\bigoplus_{w|v} \text{res}_w : H^1(F_v, A) \rightarrow \bigoplus_{w|v} H^1(K_w, A)$ is actually contained in $(\bigoplus_{w|v} H^1(K_w, A))^G$. Thus we have a map

$$\text{res} : \bigoplus_v H^1(F_v, A) \rightarrow \left(\bigoplus_w H^1(K_w, A)\right)^G = \bigoplus_v \left(\bigoplus_{w|v} H^1(K_w, A)\right)^G,$$

namely $\text{res} = \bigoplus_v \bigoplus_{w|v} \text{res}_w$. Now recall the sets S and S_∞ defined above.

Proposition 2.5. *There are canonical isomorphisms*

$$\begin{aligned} \ker(\text{res}) &\simeq \bigoplus_{v \in S \cup S_\infty} H^1(G_w, A(K_w)), \\ \text{coker}(\text{res}) &\simeq \bigoplus_{v \in S} H^2(G_w, A(K_w)), \end{aligned}$$

where w denotes a fixed prime of K lying above v for each $v \in S \cup S_\infty$.

Proof. It suffices to compute, for any v , the kernel and cokernel of $s \circ \bigoplus_{w|v} \text{res}_w$, where $s : (\bigoplus_{w|v} H^1(K_w, A))^G \rightarrow H^1(K_w, A)^{G_w}$ is the semi-local isomorphism of Lemma 2.4 corresponding to $p = 0$ and $q = 1$. Now the effect of s is simply to project onto the w coordinate (see [3]), from which it follows that $s \circ \bigoplus_{w|v} \text{res}_w = \text{res}_w$. The proposition now follows from Lemmas 2.1 and 2.3. \square

3. GLOBAL COMPUTATIONS

Recall $G = \text{Gal}(K/F)$. We will write $H^2(G, A(K))_{\text{tr}}$ for the kernel of the natural inflation map $H^2(G, A(K)) \rightarrow H^2(F, A)$.

Lemma 3.1. *Let $\text{Res} : H^1(F, A) \rightarrow H^1(K, A)^G$ be the global restriction map. Then*

$$\ker(\text{Res}) \simeq H^1(G, A(K)) \quad \text{and} \quad \text{coker}(\text{Res}) \simeq H^2(G, A(K))_{\text{tr}}.$$

Proof. This follows from the exactness of the sequence

$$0 \rightarrow H^1(G, A(K)) \rightarrow H^1(F, A) \xrightarrow{\text{Res}} H^1(K, A)^G \rightarrow H^2(G, A(K)) \xrightarrow{\text{inf}} H^2(F, A),$$

which is the exact sequence of terms of low degree belonging to the Hochschild-Serre spectral sequence $H^p(G, H^q(K, A)) \implies H^{p+q}(F, A)$. See [5]. \square

In the next lemma, we write $A(F_v)^\circ$ for the identity component of $A(F_v)$, where v is a real archimedean prime of F . Similar notations apply to A' .

Lemma 3.2. *Suppose that $q \geq 2$. If q is even, then there is a canonical isomorphism*

$$H^q(F, A) \simeq \bigoplus_{v \text{ real}} A(F_v)/A(F_v)^\circ.$$

When q is odd, we have a (non-canonical) isomorphism

$$H^q(F, A) \simeq \bigoplus_{v \text{ real}} A'(F_v)/A'(F_v)^\circ.$$

Proof. By Theorem I.6.26(c) of [8], the localization homomorphism $H^q(F, A) \rightarrow \bigoplus_{v \text{ real}} H^q(F_v, A)$ is an isomorphism. On the other hand, Remark I.3.7 of [8] shows that for each real prime v of F , $H^q(F_v, A)$ is isomorphic to either $\hat{H}^0(F_v, A) = A(F_v)/A(F_v)^\circ$ if q is even or to $\hat{H}^0(F_v, A') = A'(F_v)/A'(F_v)^\circ$ if q is odd. The lemma is now immediate. \square

Let $\text{III}(A/K)$ and $\text{III}(A/F)$ denote the Tate-Shafarevich groups of A over K and of A over F , respectively. These groups are defined by the exactness of the sequences

$$0 \rightarrow \text{III}(A/F) \rightarrow H^1(F, A) \xrightarrow{\lambda_F} \bigoplus_v H^1(F_v, A) \rightarrow \text{coker}(\lambda_F) \rightarrow 0$$

and

$$0 \rightarrow \text{III}(A/K) \rightarrow H^1(K, A) \xrightarrow{\lambda_K} \bigoplus_w H^1(K_w, A) \rightarrow \text{coker}(\lambda_K) \rightarrow 0,$$

where λ_F and λ_K are the natural localization maps. In what follows, we will assume true the well known conjecture that $\text{III}(A/K)$ and $\text{III}(A/F)$ are finite groups. This conjecture has been verified in some special cases by Rubin [11] and Kolyvagin [6].

In the statement of the next proposition, we view $A'(K)$ and $A'(F)$ as topological groups with the profinite topology.

Proposition 3.3. *There are canonical G -isomorphisms*

$$\text{coker}(\lambda_K) \simeq A'(K)^* \quad \text{and} \quad \text{coker}(\lambda_F) \simeq A'(F)^*.$$

Proof. This follows from the finiteness of $\text{III}(A/K)$ and $\text{III}(A/F)$. The isomorphism $\text{coker}(\lambda_K) \simeq A'(K)^*$ is induced by the map $\bigoplus_w H^1(K_w, A) \rightarrow A'(K)^*$, which is dual to the diagonal embedding $A'(K) \rightarrow \prod_w H^0(K_w, A')$, and similarly for $\text{coker}(\lambda_F)$. See Theorem I.6.13 and Remark I.6.14 of [8]. \square

Recall the map $\text{res} : \bigoplus_v H^1(F_v, A) \rightarrow (\bigoplus_w H^1(K_w, A))^G$ introduced in §2. We have the following commutative diagram:

$$\begin{array}{ccc} H^1(F, A) & \xrightarrow{\lambda_F} & \bigoplus_v H^1(F_v, A) \\ \text{Res} \downarrow & & \text{res} \downarrow \\ H^1(K, A)^G & \xrightarrow{\lambda_K} & \left(\bigoplus_w H^1(K_w, A) \right)^G. \end{array}$$

It follows that the map res induces a map

$$\rho : \text{coker}(\lambda_F) \rightarrow \text{coker}(\lambda_K)^G.$$

Proposition 3.4. *There are canonical isomorphisms*

$$\ker(\rho) \simeq \hat{H}^0(G, A'(K))^* \quad \text{and} \quad \text{coker}(\rho) \simeq \hat{H}^{-1}(G, A'(K))^*.$$

Proof. Let $N_{K/F} : A'(K) \rightarrow A'(F)$ be the global norm map. Then for any prime v of F , $N_{K/F} = \sum_{w|v} N_{K_w/F_v}$, where N_{K_w/F_v} denotes, for each $w|v$, the local norm map $A'(K_w) \rightarrow A'(F_v)$ (see Theorem I.15.3 of [10]). Thus we have a commutative diagram

$$\begin{array}{ccc} \prod_v H^0(F_v, A') & \longleftarrow & A'(F) \\ \uparrow & & \uparrow \\ \prod_v (\prod_{w|v} H^0(K_w, A'))_G & \longleftarrow & A'(K)_G, \end{array}$$

in which the horizontal maps are induced by the diagonal embeddings $A'(F) \rightarrow \prod_v H^0(F_v, A')$ and $A'(K) \rightarrow \prod_w H^0(K_w, A')$, the v -component of the left-hand vertical map is induced by the map $\prod_{w|v} H^0(K_w, A') \rightarrow H^0(F_v, A')$ of Lemma 2.2, and the right-hand vertical map is the map $N_{K/F}^* : A'(K)_G \rightarrow A'(F) = A'(K)^G$ induced by $N_{K/F}$. The dual of the above diagram is the commutative diagram

$$\begin{array}{ccc} \bigoplus_v H^1(F_v, A) & \longrightarrow & A'(F)^* \\ \downarrow & & \downarrow \\ \left(\bigoplus_w H^1(K_w, A) \right)^G & \longrightarrow & (A'(K)^*)^G, \end{array}$$

where, by Lemma 2.2, the left-hand vertical map is the map res . It follows that under the isomorphisms $\text{coker}(\lambda_K) \simeq A'(K)^*$ and $\text{coker}(\lambda_F) \simeq A'(F)^*$ of Proposition 3.3, the map $\rho : \text{coker}(\lambda_F) \rightarrow \text{coker}(\lambda_K)^G$ corresponds to the dual of $N_{K/F}^*$ (see the proof of Proposition 3.3). The lemma now follows easily from formula (1) of §2. \square

4. THE MAIN RESULT

We now make the following two assumptions on the abelian variety A and field extension K/F we are considering. These assumptions will remain in force for the rest of the paper.

- (A) $\hat{H}^p(G, A(K)) = \hat{H}^p(G, A'(K)) = 0$ for all p .
- (B) Either F is totally imaginary or both $A(F_v)$ and $A'(F_v)$ are connected for every real prime v of F .

Lemma 4.1. (i) For every archimedean prime w of K , $H^1(G_w, A(K_w)) = 0$.
 (ii) For all $q \geq 2$, $H^q(F, A) = H^q(K, A) = 0$.

Proof. Both assertions follow from assumption (B) above. See the statement and proof of Lemma 3.2. \square

Proposition 4.2. For every $p \geq 1$,

$$H^p(G, H^1(K, A)) = 0.$$

Proof. Since $H^q(K, A) = 0$ for all $q \geq 2$ by Lemma 4.1(ii), Theorem XV.5.11 of [2] applied to the Hochschild-Serre spectral sequence $H^p(G, H^q(K, A)) \implies H^{p+q}(F, A)$ yields an infinite exact sequence

$$\dots \rightarrow H^{p+1}(F, A) \rightarrow H^p(G, H^1(K, A)) \rightarrow H^{p+2}(G, A(K)) \rightarrow H^{p+2}(F, A) \rightarrow \dots$$

The proposition now follows from Lemma 4.1(ii) and assumption (A) above. \square

Now consider the commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{im}(\lambda_F) & \longrightarrow & \bigoplus_v H^1(F_v, A) & \longrightarrow & \text{coker}(\lambda_F) \longrightarrow 0 \\ & & \text{res}' \downarrow & & \text{res} \downarrow & & \rho \downarrow \\ 0 & \longrightarrow & \text{im}(\lambda_K)^G & \longrightarrow & (\bigoplus_w H^1(K_w, A))^G & \longrightarrow & \text{coker}(\lambda_K)^G, \end{array}$$

where the maps res and ρ are as defined previously, and res' is induced by res . Applying the snake lemma to this diagram yields the exact sequence

$$0 \rightarrow \ker(\text{res}') \rightarrow \ker(\text{res}) \rightarrow \ker(\rho) \rightarrow \text{coker}(\text{res}') \rightarrow \text{coker}(\text{res}) \rightarrow \text{coker}(\rho).$$

Now since $\ker(\rho) = \text{coker}(\rho) = 0$ by Proposition 3.4 and assumption (A), we conclude that there are isomorphisms

$$\ker(\text{res}') \simeq \ker(\text{res}) \quad \text{and} \quad \text{coker}(\text{res}') \simeq \text{coker}(\text{res}).$$

Proposition 4.3. There are canonical isomorphisms

$$\begin{aligned} \ker(\text{res}') &\simeq \bigoplus_{v \in S} H^1(G_w, A(K_w)), \\ \text{coker}(\text{res}') &\simeq \bigoplus_{v \in S} H^2(G_w, A(K_w)), \end{aligned}$$

where w denotes a fixed prime of K lying above v for each $v \in S$.

Proof. This follows from the preceding discussion and Proposition 2.5 together with Lemma 4.1(i). □

Theorem 4.4. *Assuming conditions (A) and (B) above, we have*

$$\#\text{III}(A/K)^G = \#\text{III}(A/F) \cdot \prod_{v \in S} \#H^1(G_w, A(K_w)),$$

where S denotes the set of primes of F obtained by collecting together the primes that ramify in K/F and the primes of bad reduction for A/F . Furthermore,

$$\#H^1(G, \text{III}(A/K)) = \prod_{v \in S} \#H^2(G_w, A(K_w)).$$

Proof. Consider the commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{III}(A/F) & \longrightarrow & H^1(F, A) & \longrightarrow & \text{im}(\lambda_F) \longrightarrow 0 \\ & & \text{Res}' \downarrow & & \text{Res} \downarrow & & \text{res}' \downarrow \\ 0 & \longrightarrow & \text{III}(A/K)^G & \longrightarrow & H^1(K, A)^G & \longrightarrow & \text{im}(\lambda_K)^G \longrightarrow \dots \end{array}$$

in which the bottom row is the long G -cohomology sequence associated with the exact sequence $0 \rightarrow \text{III}(A/K) \rightarrow H^1(K, A) \rightarrow \text{im}(\lambda_K) \rightarrow 0$, Res' is induced by the global restriction map Res , and res' is as defined above. Applying the snake lemma to the above diagram yields the exact sequence

$$\begin{aligned} 0 \rightarrow \ker(\text{Res}') &\rightarrow \ker(\text{Res}) \rightarrow \ker(\text{res}') \rightarrow \text{coker}(\text{Res}') \rightarrow \text{coker}(\text{Res}) \\ &\rightarrow \text{coker}(\text{res}') \rightarrow H^1(G, \text{III}(A/K)) \rightarrow H^1(G, H^1(K, A)). \end{aligned}$$

Now Lemma 3.1 together with assumption (A) yields $\ker(\text{Res}) = \text{coker}(\text{Res}) = 0$, while $H^1(G, H^1(K, A)) = 0$ by Proposition 4.2. It follows that Res' is injective with cokernel isomorphic to the kernel of res' , and that $H^1(G, \text{III}(A/K)) \simeq \text{coker}(\text{res}')$. The theorem now follows at once from Proposition 4.3, making use of the fact that

$$\#\text{coker}(\text{Res}')/\#\ker(\text{Res}') = \#\text{III}(A/K)^G/\#\text{III}(A/F).$$

□

In the following corollary, we write ${}_N\text{III}(A/K)$ for the kernel of the norm map $N_{K/F} : \text{III}(A/K) \rightarrow \text{III}(A/K)^G$.

Corollary 4.5. *If conditions (A) and (B) above hold, then*

$$\#\hat{H}^0(G, \text{III}(A/K)) \cdot \#\text{III}(A/K) = \#{}_N\text{III}(A/K) \cdot \#\text{III}(A/F) \cdot \prod_{v \in S} \#H^1(G_w, A(K_w)).$$

If furthermore K/F is a cyclic extension, then

$$\#\text{III}(A/K) = \#{}_N\text{III}(A/K) \cdot \#\text{III}(A/F).$$

Proof. The first assertion follows at once from the theorem and the exactness of the sequence

$$0 \rightarrow {}_N\text{III}(A/K) \rightarrow \text{III}(A/K) \xrightarrow{N_{K/F}} \text{III}(A/K)^G \rightarrow \hat{H}^0(G, \text{III}(A/K)) \rightarrow 0.$$

The second assertion follows from the first and the theorem, making use of the facts that, when G is cyclic, $\#\hat{H}^0(G, \text{III}(A/K)) = \#H^1(G, \text{III}(A/K))$ by [1], p. 109, and $\#H^1(G_w, A(K_w)) = \#H^2(G_w, A(K_w))$ if w is non-archimedean by [15], §4 (14). □

The final considerations of this paper pertain to the case of quadratic extensions K/F , and are as follows.

Suppose that K/F is a quadratic extension and let χ denote the non-trivial character of $G = \text{Gal}(K/F)$. We will write A^χ for the twist of A by χ (see §2 of [9]). Then there is an isomorphism $\psi : A_{/K} \xrightarrow{\sim} A_{/K}^\chi$ such that $\psi^\sigma = \chi(\sigma)\psi$ for $\sigma \in G$. It follows that

$$(2) \quad {}_N\text{III}(A_{/K}^\chi) \simeq \text{III}(A_{/K})^G.$$

Corollary 4.6. *Suppose that K/F is a quadratic extension and let χ denote the non-trivial character of $G = \text{Gal}(K/F)$. Assume that conditions (A) and (B) above hold for both A and A^χ . Then*

$$\#\text{III}(A_{/K}) = \#\text{III}(A_{/F}) \cdot \#\text{III}(A_{/F}^\chi) \cdot \prod_{v \in S} \#H^1(G_v, A(K_v)).$$

Proof. By Corollary 4.5 applied to A^χ and (2), we have

$$\begin{aligned} \#\text{III}(A_{/K}) &= \#\text{III}(A_{/K}^\chi) = \#{}_N\text{III}(A_{/K}^\chi) \cdot \#\text{III}(A_{/F}^\chi) \\ &= \#\text{III}(A_{/K})^G \cdot \#\text{III}(A_{/F}^\chi). \end{aligned}$$

Our result is now immediate from Theorem 4.4. \square

ACKNOWLEDGEMENTS

It is a pleasure to acknowledge the help rendered me by Jean-Louis Colliot-Thélène, who kindly provided the proof of Proposition 4.2. I also thank James S. Milne for some helpful remarks and David Rohrlich for his encouragement while I wrote this paper.

REFERENCES

- [1] Atiyah, M. and Wall, C.T.C., *Cohomology of groups*, in: Algebraic Number Theory (J.W.S. Cassels and A. Fröhlich, Eds.), pp. 94-115, Academic Press, London, 1967. MR **36**:2593.
- [2] Cartan, H. and Eilenberg, S., *Homological Algebra*, Princeton University Press, Princeton, N.J., 1956. MR **17**:1040e
- [3] Chamfy, C., *Modules semi-locaux*, In: Cohomologie Galoisienne des Modules Finis (Séminaire de l'Inst. de Math. de Lille sous la direction de G. Poitou), Dunod, Paris, 1967.
- [4] Gonzalez-Avilés, C.D., *On the conjecture of Birch and Swinnerton-Dyer*, Trans. Amer. Math. Soc. **349** (1997), 4181-4200. MR **98c**:11062
- [5] Hochschild, G.P. and Serre, J-P., *Cohomology of group extensions*, Trans. Amer. Math. Soc. **74** (1953), 110-134. MR **14**:619b
- [6] Kolyvagin, V.A., *Finiteness of $E(\mathbb{Q})$ and $\text{III}(E, \mathbb{Q})$ for a class of Weil curves*, Math. USSR, Izv. **32** (1989), 523-542. MR **89m**:11056
- [7] Mazur, K., *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183-266. MR **56**:3020
- [8] Milne, J.S., *Arithmetic Duality Theorems*, Academic Press, Orlando, FL, 1986. MR **88e**:14028
- [9] Milne, J.S., *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177-190. MR **48**:8512
- [10] O'Meara, O.T., *Introduction to Quadratic Forms*, Third Corrected Printing, Springer-Verlag, Berlin, 1973.
- [11] Rubin, K., *On Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527-560. MR **89a**:11065
- [12] Schaefer, E.F., *Class groups and Selmer groups*, J. Number Theory **56** (1996), 79-114. MR **97e**:11068
- [13] Serre, J-P., *Local Fields*, Grad. Texts in Math. 67, Springer-Verlag, New York, 1979. MR **82e**:12016

- [14] Silverman, J., *Advanced Topics in the Arithmetic of Elliptic Curves.*, Grad. Texts in Math. 151, Springer-Verlag, New York, 1994. MR **96b**:11074
- [15] Tate, J., *WC-groups over p-adic fields*, Séminaire Bourbaki, Exposé **156** (1957/58). MR **21**:4162

FACULTAD DE CIENCIAS, UNIVERSIDAD DE CHILE, CASILLA 653, SANTIAGO, CHILE
E-mail address: `cgonzale@abello.dic.uchile.cl`