# ON TATE-SHAFAREVICH GROUPS OF ABELIAN VARIETIES 

CRISTIAN D. GONZALEZ-AVILÉS<br>(Communicated by David E. Rohrlich)<br>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 $\amalg\left(A_{/ K}\right)$ and $\amalg\left(A_{/ F}\right)$ 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 $\amalg\left(A_{/ K}\right)$ of $G$-invariant elements. As a corollary, we obtain a simple formula relating the orders of $\amalg\left(A_{/ K}\right), ~\left(A_{/ F}\right)$ and $\amalg\left(A_{/ F}^{\chi}\right)$ when $K / F$ is a quadratic extension and $A^{\chi}$ is the twist of $A$ by the non-trivial character $\chi$ 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 $Щ\left(A_{/ K}\right)$ and $\amalg\left(A_{/ F}\right)$ 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 $\amalg\left(A_{/ K}\right)$ and $Щ\left(A_{/ F}\right)$, 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 $\operatorname{End}_{K}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. 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) $\hat{H}^{p}(G, A(K))=\hat{H}^{p}\left(G, A^{\prime}(K)\right)=0$ for all $p$.
(B) Either $F$ is totally imaginary or both $A\left(F_{v}\right)$ and $A^{\prime}\left(F_{v}\right)$ are connected for every real prime $v$ of $F$.
Here $A^{\prime}$ 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 $\S 6$ of [1]). Our main result is the following.

[^0]Main Theorem. Assume that conditions ( $A$ ) and ( $B$ ) above hold. Then

$$
\# Щ\left(A_{/ K}\right)^{G}=\# \amalg\left(A_{/ F}\right) \cdot \prod_{v \in S} \# H^{1}\left(G_{w}, A\left(K_{w}\right)\right) .
$$

Furthermore,

$$
\# H^{1}\left(G, Щ\left(A_{/ K}\right)\right)=\prod_{v \in S} \# H^{2}\left(G_{w}, A\left(K_{w}\right)\right)
$$

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 $\# \amalg\left(A_{/ K}\right)$ to $\# \amalg\left(A_{/ F}\right)$ in a special case.
Corollary. Suppose that $K / F$ is a quadratic extension and let $\chi$ denote the nontrivial character of $G=\operatorname{Gal}(K / F)$. Assume that conditions ( $A$ ) and (B) above hold for both $A$ and its quadratic twist $A^{\chi}$. Then

$$
\# \amalg\left(A_{/ K}\right)=\# \amalg\left(A_{/ F}\right) \cdot \# \amalg\left(A_{/ F}^{\chi}\right) \cdot \prod_{v \in S} \# H^{1}\left(G_{w}, A\left(K_{w}\right)\right)
$$

## 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. $M^{*}=\operatorname{Hom}_{\operatorname{cts}}(M, \mathbb{Q} / \mathbb{Z})$. 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 $\S 6$ of [1]). In particular, if we write $M_{G}$ for the largest quotient of $M$ on which $G$ acts trivially and $N^{\star}: M_{G} \rightarrow M^{G}$ for the map induced by multiplication by $N=\sum_{\sigma \in G} \sigma \in \mathbb{Z}[G]$ on $M$, then

$$
\begin{equation*}
\hat{H}^{-1}(G, M)=\operatorname{ker}\left(N^{\star}\right) \quad \text { and } \quad \hat{H}^{0}(G, M)=\operatorname{coker}\left(N^{\star}\right) \tag{1}
\end{equation*}
$$

Let $A$ be an abelian variety defined over a number field $F$. For any field $L \supset F$, we will write $G_{L}$ for $\operatorname{Gal}(\bar{L} / L)$, where $\bar{L}$ is an algebraic closure of $L$. Further, we will write $H^{p}(L, A)$ for $H^{p}\left(G_{L}, A(\bar{L})\right)$ and $A^{\prime}$ 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 $G_{w}=\operatorname{Gal}\left(K_{w} / F_{v}\right) \subset G$ be the decomposition group of $w$ over $F$, where $v$ is the prime of $F$ lying below $w$. Finally, we will write $\operatorname{res}_{w}$ for the local restriction map $H^{1}\left(F_{v}, A\right) \rightarrow H^{1}\left(K_{w}, A\right)$.
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

$$
0 \rightarrow H^{1}\left(G_{w}, A\left(K_{w}\right)\right) \rightarrow H^{1}\left(F_{v}, A\right) \xrightarrow{\mathrm{res}_{w}} H^{1}\left(K_{w}, A\right)^{G_{w}} \rightarrow 0
$$

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

$$
0 \rightarrow H^{1}\left(G_{w}, A\left(K_{w}\right)\right) \rightarrow H^{1}\left(F_{v}, A\right) \xrightarrow{\operatorname{res}_{w}} H^{1}\left(K_{w}, A\right)^{G_{w}} \rightarrow H^{2}\left(G_{w}, A\left(K_{w}\right)\right) \rightarrow 0
$$

Proof. Assertion (i) is easy to check. Assertion (ii) follows from the exactness of the sequence
$H^{1}\left(G_{w}, A\left(K_{w}\right)\right) \hookrightarrow H^{1}\left(F_{v}, A\right) \xrightarrow{\mathrm{res}_{w}} H^{1}\left(K_{w}, A\right)^{G_{w}} \rightarrow H^{2}\left(G_{w}, A\left(K_{w}\right)\right) \rightarrow H^{2}\left(F_{v}, A\right)$
(which is the exact sequence of terms of low degree belonging to the HochschildSerre spectral sequence $\left.H^{p}\left(G_{w}, H^{q}\left(K_{w}, A\right)\right) \Longrightarrow H^{p+q}\left(F_{v}, A\right)\right)$ and the fact that $H^{2}\left(F_{v}, A\right)=0$ for $v$ non-archimedean (see [5] and Corollary I.3.4 of [8]).

In what follows, $H^{0}\left(F_{v}, A^{\prime}\right)$ denotes $A^{\prime}\left(F_{v}\right)$ unless $v$ is archimedean, in which case it denotes $\hat{H}^{0}\left(F_{v}, A^{\prime}\right)=A^{\prime}\left(F_{v}\right) / N_{\bar{F}_{v} / F_{v}} A^{\prime}\left(\bar{F}_{v}\right)$. Similarly for $H^{0}\left(K_{w}, A^{\prime}\right)$.
Lemma 2.2. Let $v$ be any prime of $F$. Then the dual of the map $\bigoplus_{w \mid v} \operatorname{res}_{w}$ : $H^{1}\left(F_{v}, A\right) \rightarrow \bigoplus_{w \mid v} H^{1}\left(K_{w}, A\right)$ is the map $\prod_{w \mid v} H^{0}\left(K_{w}, A^{\prime}\right) \rightarrow H^{0}\left(F_{v}, A^{\prime}\right)$ induced by

$$
\prod_{w \mid v} A^{\prime}\left(K_{w}\right) \rightarrow A^{\prime}\left(F_{v}\right), \quad\left(x_{w}\right)_{w \mid v} \mapsto \sum_{w \mid v} N_{K_{w} / F_{v}}\left(x_{w}\right)
$$

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 $S_{\infty}$ 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 $p \geq 1$,

$$
H^{p}\left(G_{w}, A\left(K_{w}\right)\right)=0
$$

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 $G=\operatorname{Gal}(K / F)$ and let $v$ be any prime of $F$. Then $\bigoplus_{w \mid v} H^{q}\left(K_{w}, A\right)$ can be made into a $G$-module in the following natural way. For $\sigma \in G$ and $\left(\xi_{w}\right)_{w \mid v} \in \bigoplus_{w \mid v} H^{q}\left(K_{w}, A\right)$, let $\sigma\left(\xi_{w}\right)_{w \mid v}=\left(\sigma_{*}^{-1} \xi_{\sigma w}\right)_{w \mid v}$, where $\sigma_{*}: H^{q}\left(K_{w}, A\right) \rightarrow$ $H^{q}\left(K_{\sigma w}, A\right)$ is the homomorphism associated to the maps $G_{K_{\sigma w}} \rightarrow G_{K_{w}}, \nu \mapsto$ $\bar{\sigma}^{-1} \nu \bar{\sigma}$, and $A\left(\bar{K}_{w}\right) \rightarrow A\left(\bar{K}_{\sigma w}\right), P \mapsto \bar{\sigma} P$, 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, $\bigoplus_{w \mid v} H^{q}\left(K_{w}, A\right)$ 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

$$
H^{p}\left(G, \bigoplus_{w \mid v} H^{q}\left(K_{w}, A\right)\right) \simeq H^{p}\left(G_{w}, H^{q}\left(K_{w}, A\right)\right)
$$

where the $w$ on the right denotes any prime of $K$ lying above $v$.
Proof. See $\S 2.1$ of [3].
Let $v$ be a prime of $F$. It is easy to check that the image of the map $\bigoplus_{w \mid v} \operatorname{res}_{w}$ : $H^{1}\left(F_{v}, A\right) \rightarrow \bigoplus_{w \mid v} H^{1}\left(K_{w}, A\right)$ is actually contained in $\left(\bigoplus_{w \mid v} H^{1}\left(K_{w}, A\right)\right)^{G}$. Thus we have a map

$$
\text { res }: \bigoplus_{v} H^{1}\left(F_{v}, A\right) \rightarrow\left(\bigoplus_{w} H^{1}\left(K_{w}, A\right)\right)^{G}=\bigoplus_{v}\left(\bigoplus_{w \mid v} H^{1}\left(K_{w}, A\right)\right)^{G}
$$

namely res $=\bigoplus_{v} \bigoplus_{w \mid v} \operatorname{res}_{w}$. Now recall the sets $S$ and $S_{\infty}$ defined above.

Proposition 2.5. There are canonical isomorphisms

$$
\begin{aligned}
\operatorname{ker}(\mathrm{res}) & \simeq \bigoplus_{v \in S \cup S_{\infty}} H^{1}\left(G_{w}, A\left(K_{w}\right)\right) \\
\operatorname{coker}(\mathrm{res}) & \simeq \bigoplus_{v \in S} H^{2}\left(G_{w}, A\left(K_{w}\right)\right)
\end{aligned}
$$

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 $s \circ \bigoplus_{w \mid v} \mathrm{res}_{w}$, where $s:\left(\bigoplus_{w \mid v} H^{1}\left(K_{w}, A\right)\right)^{G} \rightarrow H^{1}\left(K_{w}, A\right)^{G_{w}}$ 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 $s \circ \bigoplus_{w \mid v} \operatorname{res}_{w}=\operatorname{res}_{w}$. The proposition now follows from Lemmas 2.1 and 2.3.

## 3. Global computations

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

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

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

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 $H^{p}\left(G, H^{q}(K, A)\right) \Longrightarrow H^{p+q}(F, A)$. See [5].

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

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

$$
H^{q}(F, A) \simeq \bigoplus_{v \text { real }} A\left(F_{v}\right) / A\left(F_{v}\right)^{\circ}
$$

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

$$
H^{q}(F, A) \simeq \bigoplus_{v \text { real }} A^{\prime}\left(F_{v}\right) / A^{\prime}\left(F_{v}\right)^{\circ}
$$

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

Let $\amalg\left(A_{/ K}\right)$ and $\amalg\left(A_{/ F}\right)$ 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

$$
0 \rightarrow \amalg\left(A_{/ F}\right) \rightarrow H^{1}(F, A) \xrightarrow{\lambda_{F}} \bigoplus_{v} H^{1}\left(F_{v}, A\right) \rightarrow \operatorname{coker}\left(\lambda_{F}\right) \rightarrow 0
$$

and

$$
0 \rightarrow \amalg\left(A_{/ K}\right) \rightarrow H^{1}(K, A) \xrightarrow{\lambda_{K}} \bigoplus_{w} H^{1}\left(K_{w}, A\right) \rightarrow \operatorname{coker}\left(\lambda_{K}\right) \rightarrow 0,
$$

where $\lambda_{F}$ and $\lambda_{K}$ are the natural localization maps. In what follows, we will assume true the well known conjecture that $Ш\left(A_{/ K}\right)$ and $\amalg\left(A_{/ F}\right)$ are finite groups. This conjecture has been verified in some special cases by Rubin [1] and Kolyvagin [6].

In the statement of the next proposition, we view $A^{\prime}(K)$ and $A^{\prime}(F)$ as topological groups with the profinite topology.
Proposition 3.3. There are canonical $G$-isomorphisms

$$
\operatorname{coker}\left(\lambda_{K}\right) \simeq A^{\prime}(K)^{*} \quad \text { and } \quad \operatorname{coker}\left(\lambda_{F}\right) \simeq A^{\prime}(F)^{*} .
$$

Proof. This follows from the finiteness of $\amalg\left(A_{/ K}\right)$ and $\amalg\left(A_{/ F}\right)$. The isomorphism $\operatorname{coker}\left(\lambda_{K}\right) \simeq A^{\prime}(K)^{*}$ is induced by the map $\bigoplus_{w} H^{1}\left(K_{w}, A\right) \rightarrow A^{\prime}(K)^{*}$, which is dual to the diagonal embedding $A^{\prime}(K) \rightarrow \prod_{w}^{w} H^{0}\left(K_{w}, A^{\prime}\right)$, and similarly for $\operatorname{coker}\left(\lambda_{F}\right)$. See Theorem I.6.13 and Remark I.6.14 of 8 .

Recall the map res : $\bigoplus_{v} H^{1}\left(F_{v}, A\right) \rightarrow\left(\bigoplus_{w} H^{1}\left(K_{w}, A\right)\right)^{G}$ introduced in $\S 2$. We have the following commutative diagram:


It follows that the map res induces a map

$$
\rho: \operatorname{coker}\left(\lambda_{F}\right) \rightarrow \operatorname{coker}\left(\lambda_{K}\right)^{G} .
$$

Proposition 3.4. There are canonical isomorphisms

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

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

in which the horizontal maps are induced by the diagonal embeddings $A^{\prime}(F) \rightarrow$ $\prod_{v} H^{0}\left(F_{v}, A^{\prime}\right)$ and $A^{\prime}(K) \rightarrow \prod_{w} H^{0}\left(K_{w}, A^{\prime}\right)$, the $v$-component of the left-hand vertical map is induced by the map $\prod_{w \mid v} H^{0}\left(K_{w}, A^{\prime}\right) \rightarrow H^{0}\left(F_{v}, A^{\prime}\right)$ of Lemma 2.2, and the right-hand vertical map is the map $N_{K / F}^{\star}: A^{\prime}(K)_{G} \rightarrow A^{\prime}(F)=A^{\prime}(K)^{G}$ induced by $N_{K / F}$. The dual of the above diagram is the commutative diagram

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

## 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) $\hat{H}^{p}(G, A(K))=\hat{H}^{p}\left(G, A^{\prime}(K)\right)=0$ for all $p$.
(B) Either $F$ is totally imaginary or both $A\left(F_{v}\right)$ and $A^{\prime}\left(F_{v}\right)$ are connected for every real prime $v$ of $F$.
Lemma 4.1. (i) For every archimedean prime $w$ of $K, H^{1}\left(G_{w}, A\left(K_{w}\right)\right)=0$.
(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.

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

$$
H^{p}\left(G, H^{1}(K, A)\right)=0
$$

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 $H^{p}\left(G, H^{q}(K, A)\right) \Longrightarrow$ $H^{p+q}(F, A)$ yields an infinite exact sequence

$$
\cdots \rightarrow H^{p+1}(F, A) \rightarrow H^{p}\left(G, H^{1}(K, A)\right) \rightarrow H^{p+2}(G, A(K)) \rightarrow H^{p+2}(F, A) \rightarrow \ldots
$$

The proposition now follows from Lemma 4.1(ii) and assumption (A) above.
Now consider the commutative diagram with exact rows

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

$$
0 \rightarrow \operatorname{ker}\left(\mathrm{res}^{\prime}\right) \rightarrow \operatorname{ker}(\mathrm{res}) \rightarrow \operatorname{ker}(\rho) \rightarrow \operatorname{coker}\left(\mathrm{res}^{\prime}\right) \rightarrow \operatorname{coker}(\mathrm{res}) \rightarrow \operatorname{coker}(\rho)
$$

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

$$
\operatorname{ker}\left(\mathrm{res}^{\prime}\right) \simeq \operatorname{ker}(\mathrm{res}) \quad \text { and } \quad \operatorname{coker}\left(\mathrm{res}^{\prime}\right) \simeq \operatorname{coker}(\mathrm{res})
$$

Proposition 4.3. There are canonical isomorphisms

$$
\begin{aligned}
\operatorname{ker}\left(\mathrm{res}^{\prime}\right) & \simeq \bigoplus_{v \in S} H^{1}\left(G_{w}, A\left(K_{w}\right)\right) \\
\operatorname{coker}\left(\mathrm{res}^{\prime}\right) & \simeq \bigoplus_{v \in S} H^{2}\left(G_{w}, A\left(K_{w}\right)\right)
\end{aligned}
$$

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

$$
\# \amalg\left(A_{/ K}\right)^{G}=\# \amalg\left(A_{/ F}\right) \cdot \prod_{v \in S} \# H^{1}\left(G_{w}, A\left(K_{w}\right)\right),
$$

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,

$$
\# H^{1}\left(G, Щ\left(A_{/ K}\right)\right)=\prod_{v \in S} \# H^{2}\left(G_{w}, A\left(K_{w}\right)\right)
$$

Proof. Consider the commutative diagram with exact rows

in which the bottom row is the long $G$-cohomology sequence associated with the exact sequence $0 \rightarrow \amalg\left(A_{/ K}\right) \rightarrow H^{1}(K, A) \rightarrow \operatorname{im}\left(\lambda_{K}\right) \rightarrow 0$, 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

$$
\begin{aligned}
0 \rightarrow \operatorname{ker}\left(\text { Res }^{\prime}\right) & \rightarrow \operatorname{ker}(\operatorname{Res}) \rightarrow \operatorname{ker}\left(\mathrm{res}^{\prime}\right) \rightarrow \operatorname{coker}\left(\operatorname{Res}^{\prime}\right) \rightarrow \operatorname{coker}(\mathrm{Res}) \\
& \rightarrow \operatorname{coker}\left(\mathrm{res}^{\prime}\right) \rightarrow H^{1}\left(G, \amalg\left(A_{/ K}\right)\right) \rightarrow H^{1}\left(G, H^{1}(K, A)\right) .
\end{aligned}
$$

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

$$
\# \operatorname{coker}\left(\operatorname{Res}^{\prime}\right) / \# \operatorname{ker}\left(\operatorname{Res}^{\prime}\right)=\# \amalg\left(A_{/ K}\right)^{G} / \# \amalg\left(A_{/ F}\right) .
$$

In the following corollary, we write ${ }_{N} \amalg\left(A_{/ K}\right)$ for the kernel of the norm map $N_{K / F}: \amalg\left(A_{/ K}\right) \rightarrow \amalg\left(A_{/ K}\right)^{G}$.

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

$$
\# \hat{H}^{0}\left(G, Щ\left(A_{/ K}\right)\right) \cdot \# Щ\left(A_{/ K}\right)=\#_{N} \amalg\left(A_{/ K}\right) \cdot \# Щ\left(A_{/ F}\right) \cdot \prod_{v \in S} \# H^{1}\left(G_{w}, A\left(K_{w}\right)\right)
$$

If furthermore $K / F$ is a cyclic extension, then

$$
\# Щ\left(A_{/ K}\right)=\#_{N} \amalg\left(A_{/ K}\right) \cdot \# Щ\left(A_{/ F}\right) .
$$

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

$$
0 \rightarrow{ }_{N} \amalg\left(A_{/ K}\right) \rightarrow \amalg\left(A_{/ K}\right) \xrightarrow{N_{K / F}} \amalg\left(A_{/ K}\right)^{G} \rightarrow \hat{H}^{0}\left(G, \amalg\left(A_{/ K}\right)\right) \rightarrow 0 .
$$

The second assertion follows from the first and the theorem, making use of the facts that, when $G$ is cyclic, $\# \hat{H}^{0}\left(G, \amalg\left(A_{/ K}\right)\right)=\# H^{1}\left(G, \amalg\left(A_{/ K}\right)\right)$ by [1], p. 109, and $\# H^{1}\left(G_{w}, A\left(K_{w}\right)\right)=\# H^{2}\left(G_{w}, A\left(K_{w}\right)\right)$ 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 $\chi$ denote the non-trivial character of $G=\operatorname{Gal}(K / F)$. We will write $A^{\chi}$ for the twist of $A$ by $\chi$ (see $\S 2$ 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

$$
\begin{equation*}
{ }_{N} \amalg\left(A_{/ K}^{\chi}\right) \simeq Щ\left(A_{/ K}\right)^{G} . \tag{2}
\end{equation*}
$$

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

$$
\# Щ\left(A_{/ K}\right)=\# \amalg\left(A_{/ F}\right) \cdot \# Щ\left(A_{/ F}^{\chi}\right) \cdot \prod_{v \in S} \# H^{1}\left(G_{w}, A\left(K_{w}\right)\right)
$$

Proof. By Corollary 4.5 applied to $A^{\chi}$ and (2), we have

$$
\begin{aligned}
\# \amalg\left(A_{/ K}\right)=\# \amalg\left(A_{/ K}^{\chi}\right) & =\#{ }_{N} \amalg\left(A_{/ K}^{\chi}\right) \cdot \# \amalg\left(A_{/ F}^{\chi}\right) \\
& =\# \amalg\left(A_{/ K}\right)^{G} \cdot \# \amalg\left(A_{/ F}^{\chi}\right) .
\end{aligned}
$$

Our result is now immediate from Theorem 4.4.

## Acknowledgements

It is a pleasure to acknowledge the help rendered me by Jean-Louis ColliotThélène, 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 $Щ(E, \mathbb{Q})$ 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


[^0]:    Received by the editors May 18, 1998.
    1991 Mathematics Subject Classification. Primary 11G40, 11G05.
    The author was supported by Fondecyt grant 1981175.

