ON THE TATE-SHAFAREVICH GROUPS
OVER DEGREE 3 NON-GALOIS EXTENSIONS

Hoseog Yu

Abstract. Let $A$ be an abelian variety defined over a number field $K$ and let $L$ be a degree 3 non-Galois extension of $K$. Let $\Sha(A/K)$ and $\Sha(A/L)$ denote, respectively, the Tate-Shafarevich groups of $A$ over $K$ and over $L$. Assuming that $\Sha(A/L)$ is finite, we compute $\left[\Sha(A/K)\right]/\left[\Sha(A/L)\right]$, where $[X]$ is the order of a finite abelian group $X$.

1. Introduction

Let $K$ be a number field and let $L$ be a degree 3 non-Galois extension of $K$. Let $L_0$ be the number field containing $L$ which is Galois over $K$ such that the Galois group $\text{Gal}(L_0/K)$ is isomorphic to a symmetric group $S_3$. Write $\overline{K}$, $G_K$, $M_K$, $K_v$ for the algebraic closure of $K$, $\text{Gal}(\overline{K}/K)$, a complete set of places on $K$, the completion of $K$ at the place $v \in M_K$, respectively. Fix $\sigma \in G_K - G_L$ and fix $\tau \in G_L - G_{L_0}$.

Let $A$ be an abelian variety defined over $K$. We define the restriction of scalars $\text{Res}_{L/K}(A)$ of $A$ from $L$ to $K$ as Weil did in [11, p.5]. There is an abelian variety $\text{Res}_{L/K}(A)$ defined over $K$ with an isomorphism $\phi: \text{Res}_{L/K}(A) \rightarrow A$ defined over $L$ such that

$$(\phi, \sigma(\phi), \sigma^2(\phi)): \text{Res}_{L/K}(A) \rightarrow A \times A \times A$$

is an isomorphism. For the properties of the restriction of scalars, see [11, p.5].
Let $\Phi$ be a 3-dimensional integral representation of $S_3$ defined by

$$
\Phi(\sigma) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \Phi(\tau) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}
$$

and let $\varphi$ be a 2-dimensional integral representation of $S_3$ defined by

$$
\varphi(\sigma) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad \varphi(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.
$$

Assume that 1 is the identity automorphism on $A$. Note that $\text{Res}_{L/K}(A)$ is a twist of $A^3 := A \times A \times A$ defined over $K$ such that

$$
\tau \begin{pmatrix} \phi \\ \sigma(\phi) \\ \sigma^2(\phi) \end{pmatrix} = \Phi(\tau) \begin{pmatrix} \phi \\ \sigma(\phi) \\ \sigma^2(\phi) \end{pmatrix}.
$$

There is a twist $A_\varphi$ of $A^2 := A \times A$ defined over $K$ with an isomorphism $\tilde{\varphi} : A_\varphi \to A^2$ defined over $L_0$ satisfying $\sigma(\tilde{\varphi}) = \varphi(\sigma) \circ \tilde{\varphi}$ and $\tau(\tilde{\varphi}) = \varphi(\tau) \circ \tilde{\varphi}$.

Let $\text{III}(A/K)$ and $\text{III}(A/L)$ denote the Tate-Shafarevich groups of $A$ over $K$ and over $L$, respectively. We assume throughout that these groups are finite. We write $[X]$ for the order of a finite abelian group $X$.

Note that $\text{Res}_{L/K}(A)$ is isomorphic to $A \times A_\varphi$ over $L_0$ and is isogeneous to $A \times A_\varphi$ over $K$. But the Tate-Shafarevich group is not an isogeny invariant and in general,

$$
[\text{III}(A/L)] = [\text{III}(\text{Res}_{L/K}(A)/K)] \neq [\text{III}(A/K)][\text{III}(A_\varphi/K)].
$$

The difference was computed for quadratic extensions in [12, Main Theorem] and for cyclic extensions in [13, Main Theorem]. In this paper we derive a formula relating $[\text{III}(A/L)]$, $[\text{III}(A/K)]$ and $[\text{III}(A_\varphi/K)]$ for the non-Galois extension $L/K$.

We construct a short exact sequence of abelian varieties defined over $K$

$$
0 \longrightarrow A \xrightarrow{f_1} \text{Res}_{L/K}(A) \xrightarrow{f_2} A_\varphi \longrightarrow 0
$$

and its dual exact sequence

$$
0 \longrightarrow A^\vee \xrightarrow{f_2^\vee} \text{Res}_{L/K}(A^\vee) \xrightarrow{f_1^\vee} A^\vee \longrightarrow 0,
$$

where $X^\vee$ is the dual abelian variety of an abelian variety $X$.

Denote by $H^1(f_1) : H^1(K, A) \to H^1(K, \text{Res}_{L/K}(A))$ the induced morphism from $f_1 : A \to \text{Res}_{L/K}(A)$ and denote by $H^1(f_1,\nu) : H^1(K, A) \to \ldots$
Tate-Shafarevich groups over degree 3 non-Galois extensions

$H^1(K_v, Res_{L/K}(A))$ the induced morphism from the map $f_{1,v}: A(K_v) \to Res_{L/K}(K_v)$.

For a morphism $f: A_1 \to A_2$ defined over $K$, write $f(K): A_1(K) \to A_2(K)$.

**Main Theorem.** Assume that the Tate-Shafarevich groups are finite. Then

$$[X(A/K)][X(A_{\varphi}/K)] [X(A/L)] = [Ker(H^1(f_1))][Ker(H^1(f_2))] \prod_{v \in M_K} [Ker(H^1(f_{1,v}))]$$

$$= [Coker(f_2(K))][Coker(f_1^\vee(K))] \prod_{v \in M_K} [Coker(f_{2,v}(K))]$$

**Proof.** The first equality of the theorem is obvious from Theorem 6 and Corollary 8. From the short exact sequence (1) we have the exact sequence

$$Res_{L/K}(A)(K) \overset{f_2(K)}{\longrightarrow} A_{\varphi}(K) \to H^1(K, A) \overset{H^1(f_1)}{\longrightarrow} H^1(K, Res_{L/K}(A))$$

and thus

$$Ker(H^1(f_1)) \cong Coker(f_2(K)) : Res_{L/K}(A)(K) \to A_{\varphi}(K)).$$

Similarly, $Ker(H^1(f_{1,v})) \cong Coker(f_{2,v}(K): Res_{L/K}(A)(K_v) \to A_{\varphi}(K_v))$ and $Ker(H^1(f_1^\vee)) \cong Coker(f_1^\vee(K)): Res_{L/K}(A^\vee)(K) \to A^\vee(K))$.

2. Tate-Shafarevich groups over exact sequences

Define 1 to be the identity automorphism on $A$. Define $3 \times 1$ matrix

$$M_1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \text{ and } 2 \times 3 \text{ matrix } M_2 = \begin{pmatrix} 1 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix}.$$  Then we have a short exact sequence

$$0 \longrightarrow A \overset{M_1}{\longrightarrow} A^3 \overset{M_2}{\longrightarrow} A^2 \longrightarrow 0.$$  With the representations $\Phi$ and $\varphi$ of $S_3$, we have a commutative diagram

$$\begin{array}{cccccc}
0 & \longrightarrow & A & \overset{M_1}{\longrightarrow} & A^3 & \overset{M_2}{\longrightarrow} & A^2 & \longrightarrow & 0 \\
& & \| & \Phi(\bullet) & \| & \varphi(\bullet) & \| & & \\
0 & \longrightarrow & A & \overset{M_1}{\longrightarrow} & A^3 & \overset{M_2}{\longrightarrow} & A^2 & \longrightarrow & 0,
\end{array}$$

which induces a short exact sequence of abelian varieties over $K$

$$0 \longrightarrow A \overset{f_1}{\longrightarrow} Res_{L/K}(A) \overset{f_2}{\longrightarrow} A_{\varphi} \longrightarrow 0.$$
such that the following diagram commutes:

\[
\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{f_1} & Res_{L/K}(A) & \xrightarrow{f_2} & A_\phi & \longrightarrow & 0 \\
\| & & \downarrow \hat{\Phi} & & \downarrow \bar{\varphi} & & & & \\
0 & \longrightarrow & A & \xrightarrow{M_1} & A^3 & \xrightarrow{M_2} & A^2 & \longrightarrow & 0,
\end{array}
\]

where \( \hat{\Phi} = (\phi, \sigma(\phi), \sigma^2(\phi)) \).

Now we have the dual exact sequence of the exact sequence (2)

(3) 0 \longrightarrow A_\phi^\vee \xrightarrow{f_2^\vee} Res_{L/K}(A^\vee) \xrightarrow{f_1^\vee} A^\vee \longrightarrow 0,

which induces a long exact sequence

\[
\begin{array}{ccccccccc}
0 & \longrightarrow & A\vee(K) & \longrightarrow & Res_{L/K}(A\vee)(K) & \xrightarrow{f_1^\vee(K)} & A\vee(K) \\
\longrightarrow & H^1(K, A\vee) & \xrightarrow{H^1(f_2^\vee)} & H^1(K, Res_{L/K}(A\vee)) & \longrightarrow & H^1(K, A\vee).
\end{array}
\]

Then

\[
\text{Ker}(H^1(f_2^\vee)) \cong \text{Coker}(f_1^\vee(K) : Res_{L/K}(A\vee)(K) \to A\vee(K)) = \frac{A\vee(K)}{f_1^\vee(Res_{L/K}(A\vee)(K))}.
\]

Now the exact sequence

0 \longrightarrow \text{Ker}(H^1(f_2^\vee)) \longrightarrow H^1(K, A\vee) \xrightarrow{H^1(f_2^\vee)} H^1(K, Res_{L/K}(A\vee))

induces a natural commutative diagram:

(4)

\[
\begin{array}{ccccccccc}
\bigoplus_{v \in M_K} \text{Ker}(H^1(f_2^\vee_v)) & \xhookrightarrow{} & H^1(K, A\vee) & \xrightarrow{H^1(f_2^\vee)} & f_1^\vee(H^1(K, A\vee)) & \longrightarrow & 0 \\
\bigoplus_{v \in M_K} H^1(K_v, A\vee) & \xhookrightarrow{} & \bigoplus_{v \in M_K} \bigoplus_{v \in M_K} H^1(K_v, Res_{L/K}(A\vee)) & & & & & \bigoplus_{v \in M_K} H^1(K_v, Res_{L/K}(A\vee)),
\end{array}
\]

where \( f_{1,v} : A(K_v) \to Res_{L/K}(K_v) \) is derived from \( f_1 \).

We denote by \( I \) the map \( \text{Coker}(F^\vee) \to \text{Coker}(G^\vee) \) induced from above diagram (4). Therefore,

\[
\text{Ker}(H^1) = \text{III}(Res_{L/K}(A\vee)/K) \cap H^1(f_2^\vee)(H^1(K, A\vee)) = \text{III}(Res_{L/K}(A\vee)/K) \cap \text{Ker}(H^1(f_1^\vee)).
\]
Note that $\text{Ker}(\mathcal{G}^\vee) = \text{III}(A_\varphi^\vee/K)$. Then the Kernel-Cokernel sequence of diagram (4) is

\begin{equation}
0 \to \text{Ker}(\mathcal{F}^\vee) \to \text{III}(A^\vee_\varphi/K) \to \text{III}(\text{Res}_{L/K}(A^\vee)/K) \cap \text{Ker}(\text{H}^1(f^\vee_1)) \to \text{Coker}(\mathcal{F}^\vee) \to I(\text{Coker}(\mathcal{F}^\vee)) \to 0.
\end{equation}

For a topological abelian group $M$, let $\widehat{M}$ be the completion of $M$ with respect to the topology defined by the subgroups of finite index. Write $M^*$ for the group of continuous characters of finite order of $M$, i.e. $M^* = \text{Hom}_{cts}(M, \mathbb{Q}/\mathbb{Z})$.

**Theorem 1** (Global Duality Theorem). Assume that III$(A/K)$ is finite. Then there is an exact sequence:

\begin{equation}
0 \to \text{III}(A/K) \to \text{H}^1(K, A) \to \bigoplus_{v \in M_K} \text{H}^1(K_v, A) \to \overline{A^\vee(K)^*} \to 0.
\end{equation}

**Proof.** See [1, Corollary 1], [3, Theorem 1.1] or [5, I.6.14(b)].

**Theorem 2** (Local Duality Theorem). For a place $v \in M_K$ there exists a bilinear, non-degenerate pairing

\[ \langle \ , \rangle : \text{H}^0(K_v, A^\vee) \times \text{H}^1(K_v, A) \to \mathbb{Q}/\mathbb{Z}. \]

**Proof.** See [9, p.156-04], [10, p.289] and [5, I.3.4 and I.3.7].

Here $\text{H}^0(K_v, A^\vee) = A^\vee(K_v)$ unless $v$ is archimedian, in which case it equals the quotient of $A^\vee(K_v)$ by its identity component (see [10, p.289]).

**Lemma 3.** The dual of the exact sequence

\begin{equation*}
0 \to \text{Ker}(\text{H}^1(f^\vee_{2,v})) \to \text{H}^1(K_v, A_\varphi^\vee) \xrightarrow{\text{H}^1(f^\vee_{2,v})} \text{H}^1(K_v, \text{Res}_{L/K}(A^\vee)) \quad \text{is the exact sequence}
\end{equation*}

\begin{equation*}
0 \leftarrow \text{Ker}(\text{H}^1(f_{1,v})) \leftarrow \text{H}^0(K_v, A_\varphi) \xrightarrow{\text{H}^0(f_{2,v})} \text{H}^0(K_v, \text{Res}_{L/K}(A)).
\end{equation*}

**Proof.** The exact sequence

\begin{equation*}
0 \to A \xrightarrow{f_1} \text{Res}_{L/K}(A) \xrightarrow{f_2} A_\varphi \to 0
\end{equation*}

induces the exact sequence

\begin{equation*}
\text{H}^1(K_v, \text{Res}_{L/K}(A)) \xrightarrow{\text{H}^1(f_{1,v})} \text{H}^1(K_v, A) \xrightarrow{f_1} A \xrightarrow{f_2} A_\varphi \to 0.
\end{equation*}
Then the lemma follows from the local duality theorem.

**Lemma 4.** Suppose that $M$ is a finite abelian group and that $M'$ is an abelian group. Let $f: M \to M'$ be a group homomorphism and let $\text{Hom}(f, \cdot): \text{Hom}(M', \mathbb{Q}/\mathbb{Z}) \to \text{Hom}(M, \mathbb{Q}/\mathbb{Z})$ be the dual of $f$. Then $[\text{image of } \text{Hom}(f, \cdot)] = [\text{image of } f]$.

*Proof.* It is obvious.

**Lemma 5.** Define $F: \text{Ker}(H^1(f_1)) \to \prod_{v \in M_K} \text{Ker}(H^1(f_{1,v}))$. Then $[\mathcal{I}(\text{Coker}(F^\vee))] = [\text{Ker}(H^1(f_1))/\text{Ker}(F)]$.

*Proof.* From diagram (4) there is the following commutative diagram:

\[
\begin{array}{ccc}
\bigoplus_{v \in M_K} \text{Ker}(H^1(f_{1,v})) & \longrightarrow & \bigoplus_{v \in M_K} H^1(K_v, A_\varphi^v) \\
\text{surjective} & & \downarrow \\
\text{Coker}(F^\vee) & \longrightarrow & \text{Coker}(G^\vee)
\end{array}
\]

Diagram (6) implies that $[\mathcal{I}(\text{Coker}(F^\vee))] = [\text{image of the map (7)}]$.

From Lemma 3 and [5, I.6.14(b)], the dual of a composition map in the above diagram

\[
\begin{array}{ccc}
\bigoplus_{v \in M_K} \text{Ker}(H^1(f_{1,v})) & \longrightarrow & \bigoplus_{v \in M_K} H^1(K_v, A_\varphi^v) \\
\text{surjective} & & \downarrow \\
\text{Coker}(F^\vee) & \longrightarrow & \text{Coker}(G^\vee)
\end{array}
\]

is the composition map

\[
\prod_{v \in M_K} \text{Ker}(H^1(f_{1,v})) \leftarrow \prod_{v \in M_K} H^0(K_v, A_\varphi) \leftarrow \hat{A}_\varphi(K).
\]

Diagram (6) implies that $[\mathcal{I}(\text{Coker}(F^\vee))] = [\text{image of the map (7)}]$ and Lemma 4 implies $[\text{image of the map (7)}] = [\text{image of the map (8)}]$. From the following natural commutative diagram:

\[
\begin{array}{ccc}
\prod_{v \in M_K} \text{Ker}(H^1(f_{1,v})) & \leftarrow & \prod_{v \in M_K} H^0(K_v, A_\varphi) \\
\uparrow & & \uparrow \\
\text{Ker}(H^1(f_1)) & \leftarrow & \hat{A}_\varphi(K),
\end{array}
\]

$[\text{image of the map (8)}] = [\text{image of } F] = [\text{Ker}(H^1(f_1))/\text{Ker}(F)]$. Then the lemma follows.

**Theorem 6.** Assume that $\text{III}(A/L)$ is finite. Then

\[
\frac{[\text{III}(A_\varphi^v/K)] \text{[Ker}(F)]}{[\text{III}(\text{Res}_{L/K}(A^v)/K) \cap \text{Ker}(H^1(f_1^v))]} = \frac{[\text{Ker}(H^1(f_1))][\text{Ker}(H^1(f_2^v))]}{\prod_{v \in M_K} \text{Ker}(H^1(f_{1,v}))}.
\]
Proof. From the map $F^\vee$ in diagram (4), we have
\[
\frac{\text{Coker}(F^\vee)}{\text{Ker}(F^\vee)} = \bigoplus_v \text{Ker}(H^1(f_{1,v})) \bigg/ \text{H}^1(G, A(L)).
\]
Then from the sequence (5) and Lemma 5, the theorem is immediate. \qed

3. Cassels pairing

When $\text{III}(A/K)$ is finite, there is a canonical pairing
\[
\text{III}(A/K) \times \text{III}(A^\vee/K) \to \mathbb{Q}/\mathbb{Z},
\]
which is non-degenerate. This pairing will be called Cassels pairing. For details, see [4], [10, p.292], [5, pp.96–99] and [6, 12.2].

Let $\langle -, - \rangle_K : \text{III}(A/K) \times \text{III}(A^\vee/K) \to \mathbb{Q}/\mathbb{Z}$ be the Cassels pairing for $A$ defined over $K$, and let $\langle -, - \rangle_L : \text{III}(A/L) \times \text{III}(A^\vee/L) \to \mathbb{Q}/\mathbb{Z}$ be the Cassels pairing for $A$ defined over $L$.

Write $\text{res}_A$ for the restriction map $H^1(K, A) \to H^1(L, A)$ and write $\text{cores}_{A^\vee}$ for the corestriction map $H^1(L, A^\vee) \to H^1(K, A^\vee)$ (for the definition see [7] or [8, p.259]).

Theorem 7. For $a \in \text{III}(A/K)$ and $b^\vee \in \text{III}(A^\vee/L)$
\[
\langle a, \text{cores}(b^\vee) \rangle_K = \langle \text{res}(a), b^\vee \rangle_L.
\]

Proof. See [12, p.216]. \qed

Corollary 8. We get
\[
\frac{[\text{Ker}(F)]}{[\text{III}(\text{Res}_{L/K}(A^\vee)/K) \cap \text{Ker}(H^1(f_1^\vee))]} = \frac{[\text{III}(A/K)]}{[\text{III}(A/L)]}
\]

Proof. From Shapiro’s lemma (see [2, (6.2) Proposition]) we have an isomorphism $H^1(K, \text{Res}_{L/K}(A^\vee)) \cong H^1(L, A^\vee)$. From the previous theorem and the following commutative diagram:
\[
\begin{array}{ccc}
H^1(K, \text{Res}_{L/K}(A^\vee)) & \cong & H^1(L, A^\vee) \\
\downarrow f_1^\vee & & \downarrow \text{cores}_{A^\vee} \\
H^1(K, A^\vee), & & \\
\end{array}
\]
we have the isomorphism:
\[
\text{III}(\text{Res}_{L/K}(A^\vee)/K) \cap \text{Ker}(H^1(f_1^\vee)) \cong \text{III}(A^\vee/L) \cap \text{Ker}(\text{cores}_{A^\vee}) \\
\cong \text{Hom}(\text{III}(A/L)/\text{res}_A(\text{III}(A/K)), \mathbb{Q}/\mathbb{Z}).
\]
From the isomorphism $\text{III}(A/K)/\text{Ker}(\text{res}_A) \cong \text{res}_A(\text{III}(A/K))$,

$$\frac{[\text{Ker}(\text{res}_A: \text{III}(A/K) \to \text{III}(A/L))]}{[\text{III}(\text{Res}_{L/K}(A^\vee)/K) \cap \text{Ker}(H^1(f_{L,K}))]} = \frac{[\text{III}(A/K)]}{[\text{III}(A)/L]}.$$ 

Then Shapiro’s lemma implies

$$\text{Ker}(\mathcal{F}: \text{Ker}(H^1(f_1)) \to \prod_{v \in \mathcal{M}_K} \text{Ker}(H^1(f_{1,v}))$$

$$= \text{Ker}(H^1(f_1): \text{III}(A/K) \to \text{III}(\text{Res}_{L/K}(A)/K))$$

$$\cong \text{Ker}(\text{res}_A: \text{III}(A/K) \to \text{III}(A/L))$$

and the corollary follows. 

\[\square\]

References

[1] M. I. Bashmakov, *The cohomology of abelian varieties over a number field*, Russian Math. Surveys 27, no. 6 (1972), 25–70.
[2] K. S. Brown, *Cohomology of groups*, Grad. Texts in Math. 87. Springer-Verlag 1982.
[3] J. W. S. Cassels, *Arithmetic on curves of genus 1. VII. The dual exact sequence*, J. Reine Angew. Math. 216 (1964), 150–158.
[4] J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On the conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. 217 (1965), 180–189.
[5] J. S. Milne, *Arithmetic Duality Theorems*, Perspectives in Math. vol. 1. Academic Press Inc. 1986.
[6] B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. Math. 150 (1999), 1109–1149.
[7] C. Riehm, *The Corestriction of Algebraic Structures*, Inven. Math. 11 (1970), 73–98.
[8] J. Tate, *Relations between $K_2$ and Galois cohomology*, Inventiones Math. 36 (1976), 257–274.
[9] J. Tate, *WC-group over $p$-adic fields*, In: Séminaire Bourbaki, 1957-58, exposé 156.
[10] J. Tate, *Duality theorem in Galois cohomology over number fields*, Proc. Int. Cong. Math., Stockholm (1962), 288–295.
[11] A. Weil, *Adeles and algebraic groups*, Progr in Math. 23. Birkhauser 1982.
[12] H. Yu, *On Tate-Shafarevich groups over Galois extensions*, Israel J. Math. 141 (2004), 211–220.
[13] H. Yu, *On Tate-Shafarevich groups over cyclic extensions*, Honam Math. J. 32 (2010), 45–51.
Hoseog Yu
Department of Mathematics,
Sejong University,
Seoul, 143-747, Korea
E-mail: hsyu@sejong.ac.kr