Honam Mathematical J. **37** (2015), No. 1, pp. 1–6
http://dx.doi.org/10.5831/HMJ.2015.37.1.1

ON THE TATE-SHAFAREVICH GROUPS OVER BIQUADRATIC EXTENSIONS

Hoseog Yu

Abstract. Let A be an abelian variety defined over a number field K. Let L be a biquadratic extension of K with Galois group G and let $Ш(A/K)$ and $Ш(A/L)$ denote, respectively, the Tate-Shafarevich groups of A over K and over L. Assuming $Ш(A/L)$ is finite, we compute $[Ш(A/K)]/[Ш(A/L)]$ where $[X]$ is the order of a finite abelian group X.

1. Introduction

Let L/K be a biquadratic extension of number fields with Galois group $G = \langle \sigma, \tau \rangle$. Write $\overline{K}$, G_K, M_K, K_v for the algebraic closure of K, $\mathrm{Gal}(\overline{K}/K)$, a complete set of places on K, the completion of K at the place $v \in M_K$, respectively. Fix a place $\tilde{v} \in M_L$ lying above v for each $v \in M_K$. Denote $\mathrm{Gal}(L_w/K_w)$ by G_w for $w \in M_L$.

Let A be an abelian variety defined over K. Define $Res_{L/K}(A)$ to be the restriction of scalars of A from L to K with a morphism $\phi\colon Res_{L/K}(A) \to A$ defined over L. For the definition and properties of the restriction of scalars, see [6, p.5]. Let φ be a 3-dimensional integral representation of G associated with the quotient G-module $\mathbf{Z}[G]/\mathbf{Z}(1 + \sigma + \tau + \sigma\tau)$ such that

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

Then there is a twist A_φ of A^3 defined over K with an isomorphism $\widetilde{\varphi}\colon A_\varphi \to A^3$ defined over L such that $\sigma(\widetilde{\varphi}) = \varphi(\sigma) \circ \widetilde{\varphi}$.

Received November 6, 2014. Accepted December 10, 2014.
2010 Mathematics Subject Classification: 11G40.
Key words and phrases: Tate-Shafarevich group, abelian varieties, restriction of scalars.

The conjecture of Birch and Swinnerton-Dyer predicts the leading coefficient of the Taylor expansion for the L-function attached to A/K at $s = 1$. The conjectured leading coefficient is the product of several algebraic invariants including the order of the Tate-Shafarevich group.

Let $Ш(A/K)$ and $Ш(A/L)$ 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 $Res_{L/K}(A)$ is isogeneous to $A \times A_\varphi$ over K. But the Tate-Shafarevich group is not an isogeny invariant and in general,

$$[Ш(A/L)] \neq [Ш(A/K)][Ш(A_\varphi/K)].$$

The difference was computed exactly for quadratic extensions in [7, Main Theorem] and for cyclic extensions in [8, Main Theorem]. In this paper we derive a simple formula relating $[Ш(A/L)]$, $[Ш(A/K)]$ and $[Ш(A_\varphi/K)]$ for the biquadratic extension L/K.

Main Theorem. *Assume that the Tate-Shafarevich groups are finite. Let $A^\vee$ be the dual variety of A. Then*

$$\frac{[Ш(A/K)][Ш(A_\varphi/K)]}{[Ш(A/L)]} = \frac{[\widehat{\mathrm{H}}^0(G, A^\vee(L))][\mathrm{H}^1(G, A(L))]}{\prod_{v \in M_K}[\mathrm{H}^1(G_{\tilde{v}}, A(L_{\tilde{v}}))]},$$

where $\tilde{v}$ is the fixed place of L lying above v for each $v \in M_K$.

Proof. Because $\mathrm{Ker}(\mathcal{F}) = \mathrm{Ker}(\mathrm{res}_A\colon Ш(A/K) \to Ш(A/L))$, it is obvious from Theorem 1 and Corollay 3 . ☐

2. Tate-Shafarevich groups over biquadratic extensions

Write res_A for the restriction map $\mathrm{H}^1(K, A) \to \mathrm{H}^1(L, A)$. From [7, Theorem 6] we have the following equality

(1)

$$\frac{[Ш(A_\varphi^\vee/L) \cap \mathrm{res}_{A_\varphi^\vee}(\mathrm{H}^1(K, A_\varphi^\vee))]}{[Ш(A_\varphi^\vee/K)]} = \frac{[\mathrm{Ker}(\mathcal{F}_0)] \prod_{v \in M_K} [\mathrm{H}^1(G_{\tilde{v}}, A_\varphi^\vee(L_{\tilde{v}}))]}{[\widehat{\mathrm{H}}^0(G, A_\varphi(L))][\mathrm{H}^1(G, A_\varphi^\vee(L))]}$$

with the dual abelian variety $A_\varphi^\vee$ of the abelian variety A_φ and the map $\mathcal{F}_0\colon \widehat{\mathrm{H}}^0(G, A_\varphi(L)) \to \prod_{v \in M_K} \widehat{\mathrm{H}}^0(G_{\tilde{v}}, A_\varphi(L_{\tilde{v}}))$.

Define 1 to be the identity automorphism on A. Define 4×1 matrix $M_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ and 3×4 matrix $M_2 = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$. Then we have a short exact sequence

$$0 \longrightarrow A \xrightarrow{M_1} A^4 \xrightarrow{M_2} A^3 \longrightarrow 0.$$

With the regular representation reg of G, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{M_1} & A^4 & \xrightarrow{M_2} & A^3 & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \mathrm{reg}(\bullet)} & & \downarrow{\scriptstyle \varphi(\bullet)} & & \\ 0 & \longrightarrow & A & \xrightarrow{M_1} & A^4 & \xrightarrow{M_2} & A^3 & \longrightarrow & 0, \end{array}$$

which induces a short exact sequence of abelian varieties over K

$$0 \longrightarrow A \xrightarrow{f_1} Res_{L/K}(A) \xrightarrow{f_2} A_\varphi \longrightarrow 0 \tag{2}$$

such that the following diagram commutes:

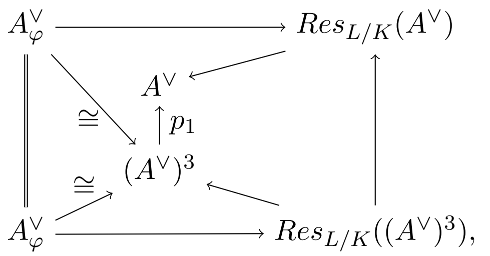
$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f_1} & Res_{L/K}(A) & \xrightarrow{f_2} & A_\varphi & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \widetilde{\varphi}} & & \\ 0 & \longrightarrow & A & \xrightarrow{M_1} & A^4 & \xrightarrow{M_2} & A^3 & \longrightarrow & 0, \end{array}$$

where $\Phi = (\phi, \sigma(\phi), \tau(\phi), \sigma\tau(\phi))$.

Now we have the dual exact sequence of (2)

$$0 \longrightarrow A_\varphi^\vee \xrightarrow{f_2^\vee} Res_{L/K}(A^\vee) \xrightarrow{f_1^\vee} A^\vee \longrightarrow 0. \tag{3}$$

From the property of the restriction of scalars $Res_{L/K}(A^\vee)$, we have the following commutative diagram:



where p_1 is the projection to the first component. Combining the above diagram with (2) and (3), we have the commutative diagram:

$$
\begin{array}{ccccccc}
0 \to A^\vee_\varphi & \xrightarrow{f_2^\vee} & Res_{L/K}(A^\vee) & \xrightarrow{f_1^\vee} & A^\vee & \to 0 \\
\| & & \uparrow & & \uparrow & \\
0 \to A^\vee_\varphi & \longrightarrow & Res_{L/K}((A^\vee)^3) & \longrightarrow & A^\vee_{\varphi\varphi} & \to 0 \\
& & \uparrow & & \uparrow & \\
& & Res_{L/K}((A^\vee)^2) & = & Res_{L/K}((A^\vee)^2). &
\end{array}
\tag{4}
$$

Note that in the commutative diagram (4) the vertical exact sequences split. Thus $A^\vee_{\varphi\varphi} \cong A^\vee \times Res_{L/K}((A^\vee)^2)$. Now we have the isomorphism $\mathrm{H}^1(G, A^\vee_\varphi(L)) \cong \widehat{\mathrm{H}}^0(G, A^\vee(L))$ by computing the long exact sequence:

$$
\begin{array}{ccccc}
0 \to \widehat{\mathrm{H}}^0(G, A^\vee(L)) & \longrightarrow & \mathrm{H}^1(K, A^\vee_\varphi) & \longrightarrow & \mathrm{H}^1(K, Res_{L/K}(A^\vee)) \\
\uparrow \cong & & \| & & \uparrow \\
0 \to \mathrm{H}^1(G, A^\vee_\varphi(L)) & \longrightarrow & \mathrm{H}^1(K, A^\vee_\varphi) & \longrightarrow & \mathrm{H}^1(K, Res_{L/K}((A^\vee)^3)).
\end{array}
$$

For the local case we get $\mathrm{H}^1(G_{\tilde{v}}, A^\vee_\varphi(L_{\tilde{v}})) \cong \widehat{\mathrm{H}}^0(G_{\tilde{v}}, A^\vee(L_{\tilde{v}}))$ and thus $[\mathrm{H}^1(G_{\tilde{v}}, A^\vee_\varphi(L_{\tilde{v}}))] = [\mathrm{H}^1(G_{\tilde{v}}, A(L_{\tilde{v}}))]$ because $[\widehat{\mathrm{H}}^0(G_{\tilde{v}}, A^\vee(L_{\tilde{v}}))] = [\mathrm{H}^1(G_{\tilde{v}}, A(L_{\tilde{v}}))]$ from the local duality theorem(see [7, Theorem 2]).

Similarily we have the isomorphism $\widehat{\mathrm{H}}^0(G, A_\varphi(L)) \cong \mathrm{H}^1(G, A(L))$ from the dual diagram:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & Res_{L/K}(A) & \longrightarrow & A_\varphi & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \| & & \\
0 & \longrightarrow & A_{\varphi\varphi} & \longrightarrow & Res_{L/K}(A^3) & \longrightarrow & A_\varphi & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & & & \\
& & Res_{L/K}(A^2) & = & Res_{L/K}(A^2). & & & &
\end{array}
$$

Note that from the above isomphism $\widehat{\mathrm{H}}^0(G, A_\varphi(L)) \cong \mathrm{H}^1(G, A(L))$, we get $\mathrm{Ker}(\mathcal{F}_0) \cong \mathrm{Ker}(\mathrm{H}^1(G, A(L)) \to \prod_{v \in M_K} \mathrm{H}^1(G_{\tilde{v}}, A(L_{\tilde{v}})))$.

Theorem 1. *Defining* $\mathcal{F}\colon \mathrm{H}^1(G, A(L)) \to \prod_{v \in M_K} \mathrm{H}^1(G_{\tilde{v}}, A(L_{\tilde{v}}))$ *we have*

$$\frac{[Ш(Res_{L/K}(A^\vee)/K) \cap \mathrm{Ker}(f_1^\vee)]}{[Ш(A_\varphi/K)]} = \frac{[\mathrm{Ker}(\mathcal{F})] \prod_{v \in M_K} [\mathrm{H}^1(G_{\tilde{v}}, A(L_{\tilde{v}}))]}{[\widehat{\mathrm{H}}^0(G, A^\vee(L))][\mathrm{H}^1(G, A(L))]}.$$

Proof. From the diagram (4) we get

$$\begin{aligned} Ш(A_\varphi^\vee/L) \cap \mathrm{res}_{A_\varphi^\vee}(\mathrm{H}^1(K, A_\varphi^\vee)) &\cong Ш(Res_{L/K}(A^\vee)/K) \cap f_2^\vee(\mathrm{H}^1(K, A_\varphi^\vee)) \\ &= Ш(Res_{L/K}(A^\vee)/K) \cap \mathrm{Ker}(f_1^\vee). \end{aligned}$$

Then we have the theorem by putting above computation to the equation (1). □

3. Cassels pairing

When $Ш(A/K)$ is finite, there is a canonical pairing

$$Ш(A/K) \times Ш(A^\vee/K) \longrightarrow \mathbf{Q}/\mathbf{Z},$$

which is non-degenerate. This pairing will be called Cassels pairing. For details, see [2], [3, pp.96–99] and [5, p.292].

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

Write $\mathrm{cores}_{A^\vee}$ for the corestriction map $\mathrm{H}^1(L, A^\vee) \to \mathrm{H}^1(K, A^\vee)$ (for the definition see [4, p.259]).

Theorem 2. *For $a \in Ш(A/K)$ and $b^\vee \in Ш(A^\vee/L)$*

$$\left\langle a, \mathrm{cores}(b^\vee) \right\rangle_K = \left\langle \mathrm{res}(a), b^\vee \right\rangle_L .$$

Proof. See [7, p.216]. □

Corollary 3. *We get*

$$\frac{[Ш(Res_{L/K}(A^\vee)/K) \cap \mathrm{Ker}(f_1^\vee)]}{[\mathrm{Ker}_A(\mathrm{res}\colon Ш(A/K) \to Ш(A/L))]} = \frac{[Ш(A/L)]}{[Ш(A/K)]}.$$

Proof. We have an isomorphism $\mathrm{H}^1(K, Res_{L/K}(A^\vee)) \cong \mathrm{H}^1(L, A^\vee)$ from Shapiro's lemma (see [1, (6.2) Proposition]). From the previous theorem and the following commutative diagram:

$$\begin{array}{ccc} \mathrm{H}^1(K, Res_{L/K}(A^\vee)) & \xrightarrow{\cong} & \mathrm{H}^1(L, A^\vee) \\ & \searrow^{f_1^\vee} & \downarrow \text{cores} \\ & & \mathrm{H}^1(K, A^\vee), \end{array}$$

we have the isomorphism:

$$\begin{aligned} Ш(Res_{L/K}(A^\vee)/K) \cap \mathrm{Ker}(f_1^\vee) &\cong Ш(A^\vee/L) \cap \mathrm{Ker}(\mathrm{cores}) \\ &\cong \mathrm{Hom}(Ш(A/L)/\,\mathrm{res}_A(Ш(A/K)), \mathbf{Q}/\mathbf{Z}). \end{aligned}$$

Then from the isomorphism $Ш(A/K)/\,\mathrm{Ker}(\mathrm{res}_A) \cong \mathrm{res}_A(Ш(A/K))$, the corollary follows. □

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(grant no NRFK 2011-0026832).

References

[1] K. S. Brown, *Cohomology of groups*, Grad. Texts in Math. 87. Springer-Verlag 1982.

[2] J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On the conjectures of Birch and Swinnerton-Dyer*, J. Reine Angrew. Math. **217** (1965), 180–189.

[3] J. S. Milne, *Arithmetic Duality Theorems*, Perspectives in Math. vol. **1**. Academic Press Inc. 1986.

[4] J. Tate, *Relations between K_2 and Galois cohomology*, Inventiones Math. **36** (1976), 257–274.

[5] J. Tate, *Duality theorem in Galois cohomology over number fields*, Proc. Int. Cong. Math., Stockholm (1962), 288–295.

[6] A. Weil, *Adeles and algebraic groups*, Progrss in Math. **23**. Birkhauser 1982.

[7] H. Yu, *On Tate-Shafarevich groups over Galois extensions*, Israel J. Math. **141** (2004), 211–220.

[8] 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`