Honam Mathematical J. **32** (2010), No. 1, pp. 45–51

ON TATE-SHAFAREVICH GROUPS OVER CYCLIC EXTENSIONS

Hoseog Yu

Abstract. Let A be an abelian variety defined over a number field K and let L be a cyclic extension of K with Galois group $G = \langle\sigma\rangle$ of order n. Let $Ш(A/K)$ and $Ш(A/L)$ denote, respectively, the Tate-Shafarevich groups of A over K and of A over L. Assume $Ш(A/L)$ is finite. Let $M(\chi)$ be a companion matrix of $1+x+\cdots+x^{n-1}$ and let A^χ be the twist of A^{n-1} defined by $f^{-1}\circ f^\sigma = M(\chi)$ where $f\colon A^{n-1} \to A^\chi$ is an isomorphism defined over L. In this paper we compute $[Ш(A/K)][Ш(A^\chi/K)]/[Ш(A/L)]$ in terms of cohomology, where $[X]$ is the order of an finite abelian group X.

1. Introduction

In this paper we generalize Main Theorem in [11]. Let L/K be a cyclic extension of number fields with Galois group G of order n. 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 $v_L \in M_L$ lying above v for each $v \in M_K$. Denote $\mathrm{Gal}(L_w/K_w)$ by G_w for $w \in M_L$. Fix $\sigma \in G_K$ such that σG_L is a generator of $G = G_K/G_L$.

Let A be an abelian variety defined over K and let $Ш(A/K)$ be the Tate-Shafarevich group of A over K. Denote by $M(\chi)$ the $(n-1)\times(n-1)$

Received December 3, 2009. Accepted January 15, 2010.
2000 Mathematics Subject Classification: 11G40.
Key words and phrases: Tate-Shafarevich group,corestriction map, transgression map, Kronecker product .
This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (KRF-2008-331-C00003).

matrix

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -1 & -1 & -1 & \cdots & -1 & -1 \end{pmatrix} \in \mathrm{End}_K(A^{n-1}),$$

where 1 is the identity homomorphism in $\mathrm{End}_K(A)$. Note that $M(\chi)$ is the companion matrix of $1 + x + \cdots + x^{n-1}$. Let A^χ be an abelian variety such that there is an isomorphism $f\colon A^{n-1} \to A^\chi$ defined over L satisfying $f^{-1} \circ f^\sigma = M(\chi)$. For the existence and the uniqueness up to K-isomorphism of such a variety A^χ, see [5, §2].

We write $[X]$ for the order of a finite abelian group X and write V^T for the transpose of the matrix V.

Main Theorem. *Assume that* $Ш(A/L)$ *is finite. Then*

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

where A' *is the dual variety of* A.

Proof. We can prove Main Theorem from Theorem 1, Theorem 2, Lemma 3, Lemma 5, and Lemma 7. □

Note that the Tate-Shafarevich group is not an isogeny invariant and in general,

$$[Ш(A/L)] \neq [Ш(A/K)][Ш(A^\chi/K)].$$

On the difference there are partial results in [3, Corollary 4.6], [5, Corollary to Theorem 3], and [7, Theorem 4.8]. For quadratic extensions, the above theorem is proved in [11, Main Theorem].

We can find another type of result in [6]. From [5, proof of Theorem 1] we know that $Ш(A/L) \cong Ш(Res_{L/K}(A)/K)$, where $Res_{L/K}(A)$ is the restriction of scalars of A from L to K. Note that in [5] the restriction of scalars is denoted by A_*. Simple computations implies that $Res_{L/K}(A)$ is isogenous to $A \times A^\chi$ over K. Then by using the equality [6, (7.3.1) in p.120] we can compute the difference.

2. Proof of main theorem

At first we introduce two results from [11].

Theorem 1. *Assume* $\text{Ш}(A/L)$ *is finite. Let* $\mathcal{F}'_0\colon \widehat{\mathrm{H}}^0(G, A'(L)) \to \prod_{v\in M_K} \widehat{\mathrm{H}}^0(G_{v_L}, A'(L_{v_L}))$ *and let* $\mathrm{trans}\colon \mathrm{H}^1(L, A)^G \to \mathrm{H}^2(G, A(L))$ *be the transgression map (for the definition see* [4, p.129] *or* [11]*). Then*

$$\frac{[\text{Ш}(A/L)^G]}{[\text{Ш}(A/K)]} = \frac{[\mathrm{trans}(\text{Ш}(A/L)^G)][\mathrm{Ker}(\mathcal{F}'_0)]}{[\widehat{\mathrm{H}}^0(G, A'(L))][\mathrm{H}^1(G, A(L))]} \prod_{v\in M_K} [\mathrm{H}^1(G_{v_L}, A(L_{v_L}))].$$

Proof. See [11, Theorem 6]. □

Theorem 2. *Assume* $\text{Ш}(A^\chi/K)$ *is finite. Denote by* ${}_N\text{Ш}(A^\chi/L)$ *the kernel of the norm map* $N\colon \text{Ш}(A^\chi/L) \to \text{Ш}(A^\chi/L)^G$. *Define* $\mathrm{res}_{(A^\chi)'}\colon \mathrm{H}^1(K, (A^\chi)') \to \mathrm{H}^1(L, (A^\chi)')^G$ *to be the restriction map. Write* cores *for the corestriction map* $\mathrm{H}^1(L, A^\chi) \to \mathrm{H}^1(K, A^\chi)$ *(for the definition see* [8] *or* [10, p.259]*). Then*

$$\frac{[\text{Ш}(A^\chi/K)]}{[N(\text{Ш}(A^\chi/L))]} = [\mathrm{cores}({}_N\text{Ш}(A^\chi/L))][\mathrm{Ker}(\mathrm{res}_{(A^\chi)'}) \cap \text{Ш}((A^\chi)'/K)].$$

Proof. See [11, Lemma 10]. □

We will show that $[N(\text{Ш}(A^\chi/L))] = [(1-\sigma)\text{Ш}(A/L)]$ in Lemma 3, and $[\mathrm{Ker}(\mathcal{F}'_0)] = [\mathrm{Ker}(\mathrm{res}_{(A^\chi)'}) \cap \text{Ш}((A^\chi)'/K)]$ in Lemma 5. Finally we will prove $[\mathrm{trans}(\text{Ш}(A/L)^G)] = [\mathrm{cores}({}_N\text{Ш}(A^\chi/L))]$ in Lemma 7. Because $[\text{Ш}(A/L)] = [\text{Ш}(A/L)^G][(1-\sigma)\text{Ш}(A/L)]$, Main Theorem is immediate.

Lemma 3. $[N(\text{Ш}(A^\chi/L))] = [(1-\sigma)\text{Ш}(A/L)]$

Proof. Let $\text{Ш}(f)\colon \text{Ш}(A/L)^{n-1} \to \text{Ш}(A^\chi/L)$ be the isomorphism induced by $f\colon A^{n-1} \to A^\chi$. For $z = (a_1, \cdots, a_{n-1})^T \in \text{Ш}(A/L)^{n-1}$, we know that $N(\text{Ш}(f)(z)) = \text{Ш}(f)(b, b^{\sigma^{n-1}}, b^{\sigma^{n-2}}, \cdots, b^{\sigma^2})^T$ with $b = \sum_{i=1}^{n-1}(a_i^{\sigma^{i-1}} - a_i^{\sigma^{n-1}}) \in (1-\sigma)\text{Ш}(A/L)$. For $b = (1-\sigma)c \in (1-\sigma)\text{Ш}(A/L)$, we can show that

$$N(\text{Ш}(f)(0, \cdots, 0, c^{\sigma^2})^T) = \text{Ш}(f)(b, b^{\sigma^{n-1}}, b^{\sigma^{n-2}}, \cdots, b^{\sigma^2})^T.$$

Now

$$N(\text{Ш}(A^\chi/L)) = \{\text{Ш}(f)(b, b^{\sigma^{n-1}}, b^{\sigma^{n-2}}, \cdots, b^{\sigma^2})^T \mid b \in (1-\sigma)\text{Ш}(A/L)\}$$

So the lemma follows. □

Lemma 4. *For* $P \in {}_N A^\chi(L)$ *there is* $Q = (0, 0, \cdots, 0, a)^T \in A(L)^{n-1}$ *with* $a \in A(K)$ *such that* $P - f(Q) \in (1-\sigma)A^\chi(L)$.

Proof. Note $(1-\sigma)A^\chi(L) \subseteq {}_N A^\chi(L)$. Let $P = f(a_1, \cdots, a_{n-1})^T$. Define $b_i = -\sum_{j=1}^{i-1} a_j^{\sigma^{n+j-i}}$ for $i \geq 2$. Then we have

$$P - (1-\sigma)f(0, b_2, \cdots, b_{n-1})^T = f(0, \cdots, 0, a)^T \in {}_N A^\chi(L).$$

Now it is easy to show that $a \in A(K)$. □

Define a surjective homomorphism $A(K) \to {}_N A^\chi(L)/(1-\sigma)A^\chi(L)$ induced by $a \in A(K) \to f(0, \cdots, 0, a)^T \in {}_N A^\chi(L)$. It is easy to show that the kernel is $NA(L)$. Then $A(K)/NA(L) \cong {}_N A^\chi(L)/(1-\sigma)A^\chi(L)$, that is,

$$\widehat{\mathrm{H}}^0(G, A(L)) \cong \mathrm{H}^1(G, A^\chi(L)). \tag{1}$$

Lemma 5. $[\mathrm{Ker}(\mathcal{F}_0')] = [\mathrm{Ker}(\mathrm{res}_{(A^\chi)'}) \cap Ш((A^\chi)'/K)]$.

Proof. Note that

$$\mathrm{Ker}(\mathrm{res}_{(A^\chi)'}) \cap Ш((A^\chi)'/K) \cong \mathrm{Ker}(\mathrm{res}_{(A')^\chi}) \cap Ш((A')^\chi/K).$$

From [11, diagram (1)] it follows that $\mathrm{Ker}(\mathrm{res}_{(A')^\chi}) \cap Ш((A')^\chi/K) = \mathrm{Ker}\{\mathrm{H}^1(G, (A')^\chi(L)) \to \prod_{v \in M_K} \mathrm{H}^1(G_{v_L}, (A')^\chi(L_{v_L}))\}$. Now from the natural isomorphism (1), the lemma follows. □

Lemma 6. *For $z \in {}_N Ш(A^\chi/L)$, there is $z' = (0, \cdots, 0, z_1)^T \in Ш(A/L)^{n-1}$ such that $z - Ш(f)(z') \in \mathrm{Ker}(\mathrm{cores})$. Furthermore, $z_1 \in Ш(A/L)^G$ and $Ш(f)(z') \in {}_N Ш(A^\chi/L)$.*

Proof. Note that $(1-\sigma)Ш(A^\chi/L) \subseteq \mathrm{Ker}(\mathrm{cores})$ because $\mathrm{cores}(z) = \mathrm{cores}(z^\sigma)$ for $z \in \mathrm{H}^1(L, A^\chi)$ (see [1, Exercises 1, p.83] or [2, (10), p.256]). Let $z = Ш(f)(y_1, \cdots, y_{n-1})^T$ where $y_i \in Ш(A/L)$.

Define $w_i = -\sum_{j=1}^{i-1} y_j^{\sigma^{n+j-i}}$ for $i \geq 2$. Note that $Ш(f)^\sigma = Ш(f^\sigma) = Ш(f)M(\chi)$. Then we can prove that

$$\begin{aligned} &z - (1-\sigma)Ш(f)(0, w_2, \cdots, w_{n-1})^T \\ &\qquad = Ш(f)(0, \cdots, 0, z_1)^T \in {}_N Ш(A^\chi/L). \end{aligned}$$

It is easy to show that $z_1 \in Ш(A/L)^G$. □

Define a homomorphism

$$\Phi\colon Ш(A/L)^G \hookrightarrow {}_N Ш(A^\chi/L) \xrightarrow{\mathrm{cores}} Ш(A^\chi/K)$$

by $\Phi(a) = \mathrm{cores}(Ш(f)(0, \cdots, 0, a))$. From the previous lemma we know that $\Phi(Ш(A/L)^G) = \mathrm{cores}({}_N Ш(A^\chi/L))$.

Lemma 7. *For $z \in Ш(A/L)^G$, $\mathrm{trans}(z) = 0$ if and only if $\Phi(z) = 0$. Furthermore, $[\mathrm{trans}(Ш(A/L)^G)] = [\mathrm{cores}({}_N Ш(A^\chi/L))]$.*

Proof. Because G is a cycle group, for any 2-cocyle $\alpha \in Z^2(G, A(L))$ there is $\beta \in Z^2(G, A(L))$ cohomologous to α such that with $P \in A(K)$ for $\tau_i \in \sigma^{k_i} G_L$

$$\beta(\tau_1, \tau_2) = \begin{cases} 0, & \text{when } \ k_1 + k_2 < n \\ P, & \text{when } \ k_1 + k_2 \geq n. \end{cases} \tag{2}$$

From the definition of transgression map(see [4, p.129] and [11]) for given $z \in Ш(A/L)^G$ there are a cochain $\Gamma \in Z^1(G_K, A)$ and a 2-cocycle $\beta \in Z^2(G, A(L))$ satisfying (2) such that $\Gamma|_{G_L} \in z$, $\beta \in \text{trans}(z)$ and

$$\beta(\tau_1, \tau_2) = -\Gamma(\tau_1\tau_2) + \Gamma(\tau_1) + \tau_1\Gamma(\tau_2) \quad \text{for} \quad \tau_i \in G_K. \tag{3}$$

Now $\text{trans}(z) = 0$, that is, β is a coboundary, if and only if $P \in N(A(L))$.

From the definition in [8], we know that for $\tau \in \sigma^k G_L$,

$$\begin{aligned} \text{cores}(f \circ (0, \cdots, 0, \Gamma|_{G_L})^T)(\tau) &= \sum_{i=0}^{n-1} \sigma^i (f(0, \cdots, 0, \Gamma(\sigma^{-i}\tau\sigma^{p_k(i)}))^T) \\ &= \sum_{i=0}^{n-1} f M^i (0, \cdots, 0, \sigma^i \Gamma(\sigma^{-i}\tau\sigma^{p_k(i)}))^T, \end{aligned}$$

where

$$p_k(i) = \begin{cases} n + i - k, & \text{when } i < k \\ i - k, & \text{when } i \geq k. \end{cases}$$

Using the equation (3) we compute

$$\sigma^i \Gamma(\sigma^{-i}\tau\sigma^{p_k(i)}) = \begin{cases} \tau\Gamma(\sigma^{n+i-k}) + \Gamma(\tau) - \Gamma(\sigma^i) - P, & \text{when } i < k \\ \tau\Gamma(\sigma^{i-k}) + \Gamma(\tau) - \Gamma(\sigma^i), & \text{when } i \geq k. \end{cases}$$

From direct computation we know that the i-th element of the column vector $\sum_{i=0}^{n-1} M^i (0, \cdots, 0, \sigma^i \Gamma(\sigma^{-i}\tau\sigma^{p_k(i)}))^T$ is

$$\begin{cases} (\sigma^{n-i-1} - \tau\sigma^{n-k-i-1})\Gamma(\sigma), & \text{when } i < n - k \\ \tau\Gamma(\sigma^{n-1}) + \sigma^{k-1}\Gamma(\sigma) - P, & \text{when } i = n - k \\ (\sigma^{n-i-1} - \tau\sigma^{2n-k-i-1})\Gamma(\sigma), & \text{when } i > n - k. \end{cases}$$

Then it follows that

$$\Phi(\Gamma)(\tau) = \text{cores}(f \circ (0, \cdots, 0, \Gamma|_{G_L})^T)(\tau) = (1 - \tau) f(Q(\Gamma)) - f(Q(\tau)),$$

where $Q(\Gamma) = (\sigma^{n-2}\Gamma(\sigma), \cdots, \sigma\Gamma(\sigma), \Gamma(\sigma))^T$ and

$$Q(\tau) = \begin{cases} (0, \cdots, 0, \overset{(n-k)}{P}, 0, \cdots, 0)^T, & \text{when } \tau \in \sigma^k G_L \text{ with } k \geq 1 \\ 0, & \text{when } \tau \in G_L. \end{cases}$$

Then $\Phi(z) = 0$ if and only if $f(Q(\tau)) = (1-\tau)Q_2$ with $Q_2 \in A^{\chi}(L)$. Now it is easy to show $\Phi(z) = 0$ if and only if $P \in NA(L)$. So the lemma follows. □

3. Corollary

Denote by R the companion matrix of $x^n - 1$. Assume that $h_i(x) \in \mathbf{Z}[x] (i = 1, 2)$ are integral polynomials of degree m_i such that $x^n - 1 = h_1(x)h_2(x)$. Let M_i be the companion matrices of $h_i(x) (i = 1, 2)$. Then there are abelian varieties B_i and isomorphisms $\psi_i\colon A^{m_i} \to B_i$ defined over L such that $\psi_i^{-1} \circ \psi_i^{\sigma} = M_i$.

Corollary 8. *Assume that* $Ш(A/L)$ *is finite. Then*

$$\frac{[Ш(B_1/K)][Ш(B_2/K)]}{[Ш(A/L)]} = \frac{[\widehat{\mathrm{H}}^0(G, {B_1}'(L))][\mathrm{H}^1(G, B_1(L))]}{\prod_{v \in M_K} [\mathrm{H}^1(G_{v_L}, B_1(L_{v_L}))]}.$$

Proof. From Main Theorem we know that

$$\frac{[Ш(B_1/K)][Ш({B_1}^{\chi}/K)]}{[Ш(B_1/L)]} = \frac{[\widehat{\mathrm{H}}^0(G, {B_1}'(L))][\mathrm{H}^1(G, B_1(L))]}{\prod_{v \in M_K} [\mathrm{H}^1(G_{v_L}, B_1(L_{v_L}))]}.$$

Note that $[Ш(B_1/L)] = [Ш(A/L)]^{m_1}$. From the definition of restriction of scalars(see [5]) it is obvious that the restriction of scalar $Res_{L/K}(A)$ is the twist of A^n defined by R. Then the following lemma implies that B_1^{χ} is isomorphic to $Res_{L/K}(A)^{m_1-1} \times B_2$ over K. Because $Ш(A/L) \cong Ш(Res_{L/K}(A)/K)$(see [5, proof of Theorem 1]), we get $[Ш({B_1}^{\chi}/K)] = [Ш(B_2/K)][Ш(A/L)]^{m_1-1}$. So the corollary is obvious. □

Lemma 9. *The Kronecker product* $M_1 \otimes M(\chi)$ *is similar to the direct sum* $\underbrace{R \oplus \cdots \oplus R}_{m_1-1} \oplus M_2$, *where* $M(\chi)$ *is the companion matrix of* $1 + x + \cdots + x^{n-1}$.

Proof. Denote by $\mathrm{Id}(k)$ the $k \times k$ identity matrix. It is enough to show that $x\,\mathrm{Id}(m_1(n-1)) - R \oplus \cdots \oplus R \oplus M_2$ is equivalent to $x\,\mathrm{Id}(m_1(n-1)) - M_1 \otimes M(\chi)$ over $\mathbf{Z}[x]$ (see [9, Theorem A.2]). Note that [9, proof of Theorem A.3(i)] implies that $x\,\mathrm{Id}(m_1(n-1)) - R \oplus \cdots \oplus R \oplus M_2$ is equivalent to a diagonal matrix $\mathrm{Diag}(1, \ldots, 1, \underbrace{x^n - 1, \ldots, x^n - 1}_{m_1-1}, f_2(x))$. Now using the similar methods in [9, proof of Theorem A.3(i)] it is easy to show that $x\,\mathrm{Id}(m_1(n-1)) - M_1 \otimes M(\chi)$ is equivalent to $\mathrm{Id}(m_1(n-2)) \oplus \left(\sum_{k=1}^{n} x^{n-k} M_1^{k-1}\right)$. Note that

$$\left(\sum_{k=1}^{n} x^{n-k} M_1^{k-1}\right)(x\,\mathrm{Id}(m_1) - M_1) = (x^n - 1)\,\mathrm{Id}(m_1).$$

Because $x\,\mathrm{Id}(m_1) - M_1$ is equivalent to $\mathrm{Diag}(1, \ldots, 1, f_1(x))$ (see [9, proof of Theorem A.3(i)]), $\sum_{k=1}^{n} x^{n-k} M_1^{k-1}$ is equivalent to the diagonal matrix $\mathrm{Diag}(x^n - 1, \ldots, x^n - 1, f_2(x))$. Then the lemma follows. □

References

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

[2] K. Cartan and S. Eilenberg, *Homological algebra*, Princeton University Press 1956.

[3] C. D. Gonzalez-Avilés, *On Tate-Shafarevich groups of abelian varieties*, Proc. Amer. Math. Soc. **128** (2000), 953–961.

[4] G. Hochschild and J-P. Serre, *Cohomology of Group Extension*, Trans. Amer. Math. Soc. **74** (1953), 110–134.

[5] J. S. Milne, *On the arithmetic of abelian varieties*, Inventiones Math. **17** (1972), 177–190.

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

[7] Hwasin Park, *Idempotent relations and the conjecture of Birch and Swinnerton-Dyer*, In: Algebra and Topology 1990 (Taejon, 1990), 97–125.

[8] Carl Riehm, *The Corestriction of Algebraic Structures*, Inven. Math. **11** (1970), 73–98.

[9] L. Solomon, *Similarity of the companion matrix and its transpose*, Linear Algebra Appl. **302/303** (1999), 555–561.

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

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

Hoseog Yu
Department of Applied Mathematics,
Sejong University,
Seoul, 143-747, Korea
E-mail: hsyu@sejong.ac.kr