ON THE RATIO OF TATE-SHAFAREVICH GROUPS OVER CYCLIC EXTENSIONS OF ORDER p^2

HOSEOG YU

Abstract. Let A be an abelian variety defined over a number field K and p be a prime. Define $\varphi_i = (x^{p^i} - 1)/(x^{p^{i-1}} - 1)$. Let A_{φ_i} be the abelian variety defined over K associated to the polynomial φ_i and let $\text{III}(A_{\varphi_i})$ denote the Tate-Shafarevich groups of A_{φ_i} over K . In this paper assuming $\text{III}(A/F)$ is finite, we compute $[\text{III}(A_{\varphi_1})][\text{III}(A_{\varphi_2})]/[\text{III}(A_{\varphi_1\varphi_2})]$ in terms of K -rational points of A_{φ_i} , $A_{\varphi_1\varphi_2}$ and their dual varieties, where $[X]$ is the order of a finite abelian group X .

1. Introduction

Let p be a prime number and let F/K be a cyclic extension of number fields with Galois group G of order p^2 . 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 a place $v_F \in M_F$ lying above v for each $v \in M_K$. Fix $\sigma \in G_K$ such that σG_F is a generator of $G = G_K/G_F$. Let L be the subfield of F fixed by σ^p . Note that $[F : L] = [L : K] = p$.

Let A be an abelian variety defined over K . For positive integers $i = 1, 2$, define $\varphi_i = (x^{p^i} - 1)/(x^{p^{i-1}} - 1) = \sum_{k=0}^{p-1} x^{kp^{i-1}}$. Note $\varphi_1\varphi_2 = (x^{p^2} - 1)/(x - 1)$. For a monic polynomial $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ such that $g(x) \nmid (x^{p^2} - 1)$, denote by $M(g)$ the companion

Received March 26, 2014. Accepted May 2, 2014.

2010 Mathematics Subject Classification. 11G40.

Key words and phrases. Tate-Shafarevich group, abelian varieties, cyclic extension.

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

matrix of $g(x)$

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix} \in \text{End}_K(A^n),$$

where $\text{End}_K(A^n)$ is the endomorphism ring of A^n defined over K and 1 is the identity homomorphism of A . Let A_g be an abelian variety defined over K satisfying that there is an isomorphism $\widehat{g}: A^n \rightarrow A_g$ defined over L such that $\sigma(\widehat{g})^{-1} \circ \widehat{g} = M(g)$. For the existence and the uniqueness up to K -isomorphism of such a variety A_g , see [2, §2].

Now we can construct an exact sequence defined over K

$$0 \longrightarrow A_{\varphi_1} \xrightarrow{h_1} A_{\varphi_1\varphi_2} \xrightarrow{h_2} A_{\varphi_2} \longrightarrow 0,$$

and its dual exact sequence

$$0 \longleftarrow A'_{\varphi_1} \xleftarrow{h'_1} A'_{\varphi_1\varphi_2} \xleftarrow{h'_2} A'_{\varphi_2} \longleftarrow 0,$$

where $A'_\bullet$ is the dual abelian variety of $A_\bullet$.

We write $[X]$ for the order of a finite abelian group X and write V^T for the transpose of the matrix V . Denote by $\text{III}(A_g)$ the Tate-Shafarevich group of A_g over K .

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

We compute the ratio of the orders of Tate-Shafarevich groups of abelian varieties when there is a short exact sequence of abelian varieties.

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

$$\frac{[\text{III}(A_{\varphi_1})][\text{III}(A_{\varphi_2})]}{[\text{III}(A_{\varphi_1\varphi_2})]} = \frac{[A'_{\varphi_1}(K)/h'_1 A'_{\varphi_1\varphi_2}(K)][A_{\varphi_2}(K)/h_2 A_{\varphi_1\varphi_2}(K)]}{\prod_{v \in M_K} [A_{\varphi_2}(K_v)/h_2 A_{\varphi_1\varphi_2}(K_v)]}.$$

Proof. It is immediate from Theorem 1, we get

$$\begin{aligned} \frac{[\text{III}(A_{\varphi_1})][\text{III}(A_{\varphi_2})]}{[\text{III}(A_{\varphi_1\varphi_2})]} &= \frac{[\widehat{H}^0(L/K, A'(L))][H^1(L/K, A(L))]}{\prod_{v \in M_K} [H^1(L_{v_L}/K_v, A(L_{v_L}))]} \\ &\quad \times \frac{[\widehat{H}^0(F/L, A'(F))][H^1(F/L, A(F))]}{\prod_{v \in M_L} [H^1(F_{v_F}/L_v, A(F_{v_F}))]} \\ &\quad \times \frac{\prod_{v \in M_K} [H^1(F_{v_F}/K_v, A(F_{v_F}))]}{[\widehat{H}^0(F/K, A'(F))][H^1(F/K, A(F))]} . \end{aligned}$$

By rearranging the terms, we have

$$\begin{aligned} \frac{[\text{III}(A_{\varphi_1})][\text{III}(A_{\varphi_2})]}{[\text{III}(A_{\varphi_1\varphi_2})]} &= \frac{[\widehat{H}^0(L/K, A'(L))][\widehat{H}^0(F/L, A'(F))]}{[\widehat{H}^0(F/K, A'(F))]} \\ &\quad \times \frac{[H^1(L/K, A(L))][H^1(F/L, A(F))]}{[H^1(F/K, A(F))]} \\ &\quad \times \frac{\prod_{v \in M_K} [H^1(F_{v_F}/K_v, A(F_{v_F}))]}{\prod_{v \in M_K} [H^1(L_{v_L}/K_v, A(L_{v_L}))] \prod_{v \in M_L} [H^1(F_{v_F}/L_v, A(F_{v_F}))]} . \end{aligned}$$

Now Lemma 3, Lemma 5, and Lemma 7 imply the theorem. $\square$

Note that $A_{\varphi_1\varphi_2}$ and $A_{\varphi_1} \times A_{\varphi_2}$ are isogenous but the Tate-Shafarevich group is not an isogeny invariant and in general,

$$[\text{III}(A_{\varphi_1\varphi_2}/K)] \neq [\text{III}(A_{\varphi_1}/K)][\text{III}(A_{\varphi_2}/K)].$$

On the difference of the Tate-Shafarevich group of two isogenous abelian varieties, there are partial results in [1, Corollary 4.6], [2, Corollary to Theorem 3], [4, Theorem 4.8], and [5, Main Theorem].

We can find another type of result in [3].

2. Proof of main theorem

Denote by $v(-1)$ the transpose of $1 \times (p-1)$ matrix $(-1 \ -1 \ \cdots \ -1)$ and by I_{p-1} the $(p-1) \times (p-1)$ identity matrix. Define M_1 to be the transpose of the $(p-1) \times (p^2-1)$ matrix

$$(I_{p-1} \quad v(-1) \quad I_{p-1} \quad v(-1) \quad \cdots \quad I_{p-1} \quad v(-1) \quad I_{p-1}).$$

Denote by M_2 the $(p^2-p) \times (p^2-1)$ matrix

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 & 1 & 1 \end{pmatrix},$$

where each row has p 1's.

It is easy to check that the following sequence is exact:

$$0 \longrightarrow A^{p-1} \xrightarrow{M_1} A^{p^2-1} \xrightarrow{M_2} A^{p(p-1)} \longrightarrow 0.$$

From the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & A^{p-1} & \xrightarrow{M_1} & A^{p^2-1} & \xrightarrow{M_2} & A^{p(p-1)} \longrightarrow 0 \\ & & M(\varphi_1) \downarrow & & M(\varphi_1\varphi_2) \downarrow & & M(\varphi_2) \downarrow \\ 0 & \longrightarrow & A^{p-1} & \xrightarrow{M_1} & A^{p^2-1} & \xrightarrow{M_2} & A^{p(p-1)} \longrightarrow 0, \end{array}$$

we get an exact sequence defined over K

$$0 \longrightarrow A_{\varphi_1} \xrightarrow{h_1} A_{\varphi_1\varphi_2} \xrightarrow{h_2} A_{\varphi_2} \longrightarrow 0,$$

where $h_1 = \widehat{\varphi_1\varphi_2} \circ M_1 \circ \widehat{\varphi_1}^{-1}$ and $h_2 = \widehat{\varphi_2} \circ M_2 \circ \widehat{\varphi_1\varphi_2}^{-1}$.

At first we introduce a theorem from [5].

Theorem 1. Assume that $\text{III}(A/F)$ is finite. Then the followings hold.

$$\begin{aligned} (1) \quad & \frac{[\text{III}(A_{x^{p-1}})][\text{III}(A_{\varphi_2})]}{[\text{III}(A/F)]} = \frac{[\text{III}(A/L)][\text{III}(A_{\varphi_2})]}{[\text{III}(A/F)]} \\ & = \frac{[\widehat{H}^0(F/L, A'(F))][H^1(F/L, A(F))]}{\prod_{v \in M_L} [H^1(F_{v_F}/L_v, A(F_{v_F}))]}. \\ (2) \quad & \frac{[\text{III}(A/K)][\text{III}(A_{\varphi_1})]}{[\text{III}(A/L)]} = \frac{[\widehat{H}^0(L/K, A'(L))][H^1(L/K, A(L))]}{\prod_{v \in M_K} [H^1(G(L_{v_L}/K_v), A(L_{v_L}))]}. \\ (3) \quad & \frac{[\text{III}(A/K)][\text{III}(A_{\varphi_1\varphi_2})]}{[\text{III}(A/F)]} = \frac{[\widehat{H}^0(F/K, A'(F))][H^1(F/K, A(F))]}{\prod_{v \in M_K} [H^1(F_{v_F}/K_v, A(F_{v_F}))]}. \end{aligned}$$

Proof. See [5, Theorem 6]. □

Lemma 2. For $g = \varphi_2$ or for $g = \varphi_1\varphi_2$,

$$\widehat{g}: \left\{ x \in A^{\deg(g)}(F) \mid \sigma x = M(g)x \right\} \rightarrow A_g(K)$$

is an isomorphism.

Proof. Assume $\widehat{g}(x) \in A_g(K)$. Then $\widehat{g}(x) = \sigma(\widehat{g}(x)) = \sigma(\widehat{g})(\sigma x)$ and $\sigma x = (\sigma(\widehat{g}))^{-1} \circ \widehat{g}x = M(g)x$. $\square$

For the Galois extension F/K , write ${}_{N_{F/K}}A(F)$ for the kernel of the norm map $N_{F/K} : A(F) \rightarrow A(K)$.

Lemma 3. *We have*

$$\frac{[H^1(L/K, A(L))][H^1(F/L, A(F))]}{[H^1(F/K, A(F))]} = [A_{\varphi_2}(K)/h_2 A_{\varphi_1 \varphi_2}(K)].$$

Proof. From the inflation-restriction sequence

$$0 \rightarrow H^1(L/K, A(L)) \rightarrow H^1(F/K, A(F)) \rightarrow H^1(F/L, A(F)),$$

we know

$$\frac{[H^1(L/K, A(L))][H^1(F/L, A(F))]}{[H^1(F/K, A(F))]} = \left[{}_{N_{F/L}}A(F)/\varphi_1(\sigma) {}_{N_{F/K}}A(F) \right].$$

It is easy to show that

$$\widehat{\varphi_2}^{-1} A_{\varphi_2}(K) = \left\{ (x, \sigma(x), \dots, \sigma^{p(p-1)-1}(x))^T \mid N_{F/L}(x) = 0 \right\}$$

and

$$\widehat{\varphi_1 \varphi_2}^{-1} A_{\varphi_1 \varphi_2}(K) = \left\{ (x, \sigma(x), \dots, \sigma^{p^2-2}(x))^T \mid N_{F/K}(x) = 0 \right\}.$$

Thus

$$\begin{aligned} A_{\varphi_2}(K)/h_2 A_{\varphi_1 \varphi_2}(K) &\cong \widehat{\varphi_2}^{-1} A_{\varphi_2}(K)/\widehat{\varphi_2}^{-1} h_2 A_{\varphi_1 \varphi_2}(K) \\ &\cong \widehat{\varphi_2}^{-1} A_{\varphi_2}(K)/M_2 \widehat{\varphi_1 \varphi_2}^{-1} A_{\varphi_1 \varphi_2}(K) \\ &\cong {}_{N_{F/L}}A(F)/\varphi_1(\sigma) {}_{N_{F/K}}A(F). \end{aligned}$$

The last isomorphism is obvious by looking at the first components of $\widehat{\varphi_2}^{-1} A_{\varphi_2}(K)$ and $M_2 \widehat{\varphi_1 \varphi_2}^{-1} A_{\varphi_1 \varphi_2}(K)$. Thus we prove the lemma. $\square$

Lemma 4. *For $g = \varphi_1$ or for $g = \varphi_1 \varphi_2$,*

$$\widehat{g}' : A'_g(K) \rightarrow \left\{ x \in A'^{\deg(g)}(F) \mid \sigma x = (M(g)^T)^{-1} x \right\}$$

is an isomorphism.

Proof. Assume $\widehat{g}'^{-1}(x) \in A_g(K)$. Then $\widehat{g}'^{-1}(x) = \sigma(\widehat{g}'^{-1}(x)) = \sigma(\widehat{g}')^{-1}(\sigma x)$ and $\sigma x = (\sigma(\widehat{g}') \circ \widehat{g}'^{-1})x = (M(g)^T)^{-1} x$. $\square$

Lemma 5. *We have*

$$\frac{[\widehat{H}^0(L/K, A'(L))][\widehat{H}^0(F/L, A'(F))]}{[\widehat{H}^0(F/K, A'(F))]} = [A'_{\varphi_1}(K)/h'_1 A'_{\varphi_1 \varphi_2}(K)].$$

Proof. From the exact sequence

$$\widehat{H}^0(F/L, A'(F)) \rightarrow \widehat{H}^0(F/K, A'(F)) \rightarrow \widehat{H}^0(L/K, A'(L)) \rightarrow 0,$$

we can get

$$\frac{[\widehat{H}^0(L/K, A'(L))][\widehat{H}^0(F/L, A'(F))]}{[\widehat{H}^0(F/K, A'(F))]} = \left[N_{L/K} A'(L) / \varphi_2(\sigma)_{N_{F/K}} A'(F) \right].$$

From the property of dual varieties, we have the following commutative diagram

$$\begin{array}{ccccccc} 0 & \longleftarrow & A'^{p-1} & \xleftarrow{M_1^T} & A'^{p^2-1} & \xleftarrow{M_2^T} & A'^{p(p-1)} & \longleftarrow & 0 \\ & & \uparrow M(\varphi_1)^T & & \uparrow M(\varphi_1\varphi_2)^T & & \uparrow M(\varphi_2)^T & & \\ 0 & \longleftarrow & A'^{p-1} & \xleftarrow{M_1^T} & A'^{p^2-1} & \xleftarrow{M_2^T} & A'^{p(p-1)} & \longleftarrow & 0. \end{array}$$

The above commutative diagram implies an exact sequence defined over K

$$0 \longleftarrow A'_{\varphi_1} \xleftarrow{h'_1} A'_{\varphi_1\varphi_2} \xleftarrow{h'_2} A'_{\varphi_2} \longleftarrow 0,$$

where $h'_1 = \widehat{\varphi_1'}^{-1} \circ M_1^T \circ \widehat{\varphi_1\varphi_2}'$ and $h'_2 = \widehat{\varphi_1\varphi_2'}^{-1} \circ M_2^T \circ \widehat{\varphi_2}'$.

It is easy to show that

$$\widehat{\varphi_1'} A'_{\varphi_1}(K) = \left\{ (x, \sigma(x), \dots, \sigma^{p(p-1)-1}(x))^T \mid N_{L/K}(x) = 0 \right\}$$

and

$$\widehat{\varphi_1\varphi_2'} A'_{\varphi_1\varphi_2}(K) = \left\{ (x, \sigma(x), \dots, \sigma^{p^2-2}(x))^T \mid N_{F/K}(x) = 0 \right\}.$$

Thus

$$\begin{aligned} A'_{\varphi_1}(K) / h'_1 A'_{\varphi_1\varphi_2}(K) &\cong \widehat{\varphi_1'} A'_{\varphi_1}(K) / \widehat{\varphi_1'} h'_1 A'_{\varphi_1\varphi_2}(K) \\ &\cong \widehat{\varphi_1'} A'_{\varphi_1}(K) / M_1^T \widehat{\varphi_1\varphi_2'} A'_{\varphi_1\varphi_2}(K) \\ &\cong N_{L/K} A'(L) / \varphi_2(\sigma)_{N_{F/K}} A'(F). \end{aligned}$$

The last isomorphism is obvious from the first components of $\widehat{\varphi_1'} A'_{\varphi_1}(K)$ and $M_1^T \widehat{\varphi_1\varphi_2'} A'_{\varphi_1\varphi_2}(K)$. We prove the lemma. $\square$

For $v \in M_K$ define $M_{L,v} = \{w \in M_L \mid w \text{ is lying above } v\}$.

Lemma 6. Assume a place $v \in M_K$ splits completely at L . Then $L_w = K_v$ for $w \in M_{L,v}$ and

$$\begin{aligned} [A_{\varphi_2}(K_v)/h_2 A_{\varphi_1 \varphi_2}(K_v)] &= [\mathrm{H}^1(F_{v_F}/K_v, A(F_{v_F}))]^{p-1} \\ &= \frac{[\mathrm{H}^1(L_{v_L}/K_v, A(L_{v_L}))] \prod_{w \in M_{L,v}} [\mathrm{H}^1(F_{w_F}/L_w, A(F_{w_F}))]}{[\mathrm{H}^1(F_{v_F}/K_v, A(F_{v_F}))]}. \end{aligned}$$

Proof. Since $L_w = K_v$ for $w \in M_{L,v}$, then $[\mathrm{H}^1(L_{v_L}/K_v, A(L_{v_L}))] = 1$ and $\mathrm{H}^1(F_{w_F}/L_w, A(F_{w_F})) = \mathrm{H}^1(F_{v_F}/K_v, A(F_{v_F}))$ for $w \in M_{L,v}$. It is easy to show that $\widehat{\varphi_2}^{-1}(A_{\varphi_2}(K_v))$ is

$$\left\{ (a_i) \in \left({}_{N_{F_{v_F}/K_v}} A(F_{v_F}) \right)^{p^2-p} \mid a_{i+p} = \sigma(a_i) \text{ for } 1 \leq i \leq p^2 - 2p \right\}.$$

Note that $\widehat{\varphi_1 \varphi_2}^{-1}(A_{\varphi_1 \varphi_2}(K_v)) \subseteq (A(F_{v_F}))^{p^2-1}$ is

$$\left\{ (b_i) \mid b_{i+p} = \sigma(b_i) \text{ for } 1 \leq i \leq p^2 - p - 1, \quad {}_{N_{F_{v_F}/K_v}} \sum_{k=1}^p b_k = 0 \right\}.$$

With two sets $S_1 = \{(a_1, \dots, a_p) \mid a_i \in {}_{N_{F_{v_F}/K_v}} A(F_{v_F})\}$ and $S_2 = \{(b_1, b_2, \dots, b_p) \in (A(F_{v_F}))^p \mid {}_{N_{F_{v_F}/K_v}} \sum_{i=1}^p b_i = 0\}$ we get

$$\begin{aligned} A_{\varphi_2}(K_v)/h_2 A_{\varphi_1 \varphi_2}(K_v) &\cong \widehat{\varphi_2}^{-1}(A_{\varphi_2}(K_v))/\widehat{\varphi_2}^{-1} \circ h_2(A_{\varphi_1 \varphi_2}(K_v)) \\ &\cong \widehat{\varphi_2}^{-1}(A_{\varphi_2}(K_v))/M_2 \circ \widehat{\varphi_1 \varphi_2}^{-1}(A_{\varphi_1 \varphi_2}(K_v)) \\ &\cong S_1 / \left\{ \left(\sum_{k=1}^p b_k + (\sigma - 1) \sum_{k=1}^{i-1} b_k \right) \mid (b_i) \in S_2 \right\} \\ &\cong \bigoplus_{i=1}^{p-1} \mathrm{H}^1(F_{v_F}/K_v, A(F_{v_F})), \end{aligned}$$

which proves the theorem. $\square$

When a place $v \in M_K$ inert or ramifies at L , $M_{L,v}$ has only one element $w = v_L$. Then from Lemma 3

$$\begin{aligned} [A_{\varphi_2}(K_v)/h_2 A_{\varphi_1 \varphi_2}(K_v)] &= \frac{[\mathrm{H}^1(L_{v_L}/K_v, A(L_{v_L}))][\mathrm{H}^1(F_{v_F}/L_{v_L}, A(F_{v_F}))]}{[\mathrm{H}^1(F_{v_F}/K_v, A(F_{v_F}))]}. \end{aligned}$$

Lemma 7.

$$\prod_{v \in M_K} [A_{\varphi_2}(K_v)/h_2 A_{\varphi_1 \varphi_2}(K_v)] \\ = \frac{\prod_{v \in M_K} [H^1(L_{v_L}/K_v, A(L_{v_L}))] \prod_{v \in M_L} [H^1(F_{v_F}/L_v, A(F_{v_F}))]}{\prod_{v \in M_K} [H^1(F_{v_F}/K_v, A(F_{v_F}))]}.$$

Proof. The lemma is obvious from Lemma 6 and

$$\frac{\prod_{v \in M_K} [H^1(L_{v_L}/K_v, A(L_{v_L}))] \prod_{v \in M_L} [H^1(F_{v_F}/L_v, A(F_{v_F}))]}{\prod_{v \in M_K} [H^1(F_{v_F}/K_v, A(F_{v_F}))]} \\ = \prod_{v \in M_K} \frac{[H^1(L_{v_L}/K_v, A(L_{v_L}))] \prod_{w \in M_{L,v}} [H^1(F_{w_F}/L_w, A(F_{w_F}))]}{[H^1(F_{v_F}/K_v, A(F_{v_F}))]}.$$

□

References

- [1] C. D. Gonzalez-Avilés, *On Tate-Shafarevich groups of abelian varieties*, Proc. Amer. Math. Soc. **128** (2000), 953-961.
- [2] J. S. Milne, *On the arithmetic of abelian varieties*, Inventiones Math. **17** (1972), 177-190.
- [3] J. S. Milne, *Arithmetic Duality Theorems*, Perspectives in Math. vol. **1**. Academic Press Inc. 1986.
- [4] Hwasin Park, *Idempotent relations and the conjecture of Birch and Swinnerton-Dyer*, In: Algebra and Topology 1990 (Taejon, 1990), 97-125.
- [5] 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