Title	RELATIONS AMONG SHAFAREVICH-TATE GROUPS
Author(s)	PARK, HWASIN
Citation	数理解析研究所講究録 (1997), 998: 117-125
Issue Date	1997-06
URL	http://hdl.handle.net/2433/61273
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
998 巻 1997 年 117-125

RELATIONS AMONG SHAFAREVICH–TATE GROUPS

HWASIN PARK

1. GROUP COHOMOLOGY

Let G be a (finite) group, and let A be an abelian group on which G acts,i.e., A is an G-module. For any subgroup H of G, we denote

$$A^H = \{x \in A : \sigma x = x \text{ for all } \sigma \in H\}.$$

We define $H^0(G,A) = A^G$.

Let

$$C^1(G,A) = Hom(G,A),$$

$$Z^1(G,A) = \{f \in Hom(G,A) : f(\sigma\tau) = \sigma f(\tau) + f(\sigma) \text{ for all } \sigma, \tau \in G\},$$

$$B^1(G,A) = \{f \in Hom(G,A) : \exists a \in A \ \text{ such that } f(\sigma) = \sigma a - a \text{ for all } \sigma \in G\}.$$

Then, we easily see that $B^1(G,A) \subset Z^1(G,A)$. We define

$$H^1(G,A) = Z^1(G,A)/B^1(G,A).$$

For example, if G acts trivially on A, then $H^0(G,A) = A$ and $H^1(G,A) = hom(G,A)$.

Now, if A is a $G-$module, and if H is any subgroup of G, then A is an H-moudle. Hence, We get the restriction map $Z^1(G,A) \to Z^1(H,A)$. Also, under this map, $B^1(G,A)$

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

maps into $B^1(H,A)$. Hence, they induces the restriction map $H^1(G,A) \to H^1(H,A)$. If $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules, then we have the following long exact sequence of homologies

$$0 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \to H^1(G,A) \to H^1(G,B) \to H^1(G,C).$$

If H is a normal subgroup of G, A^H is a G/H-module. Then, we get the inflation map $Z^1(G/H, A^H) \to Z^1(G,M)$. Also, $B^1(G/H, A^H)$ maps into $B(G,A)$. Hence, they induces the inflation map $H^1(G/H, A^H) \to H^1(G,A)$.

Then, we have the following exact sequence.

$$0 \to H^1(G/H, A^H) \xrightarrow{inf} H^1(G,M) \xrightarrow{res} H^1(H,M)$$

2. Definition of the Shafarevich-Tate Group of an Elliptic Curve

Let K be a number field, and E/K be an elliptic curve over K.

Let L be a finite extension field of K. We denote

$$E(L) = \{(x,y) \in E : x, y \in L\} \cup \{O\}.$$

Then, $E(L)$ is a finitely generated abelian group.

Let $G = G(\bar{K}/K)$, the Galois group of $\bar{K}$ over K. Then, G acts on E, via, for any $\sigma \in G$,

$$\sigma P = \begin{cases} (\sigma x, \sigma y), & \text{if } P = (x,y) \\ O, & \text{if } P = O. \end{cases}$$

Then, $E(\bar{K})^{G(\bar{K}/L)} = E(L)$.

Let M_K be the set of all absolute values v in K such that $v|_{\mathbb{Q}} = |\cdot|_p$ or $|\cdot|_\infty$. For any $v \in M_K$, fix an extension w of v to $\bar{K}$. This fixes an embedding $\bar{K} \hookrightarrow \bar{K}_v$. Let $G_v = \{\sigma \in G = G(\bar{K}/K) : \sigma w = w\}$ be the decomposition group. Then, G_v acts on $E(\bar{K}_v)$. The natural inclusions $G_v \hookrightarrow G$ and $E(\bar{K}) \hookrightarrow E(\bar{K}_v)$ give the restriction maps on cohomologies,

$$H^1(G, E/K) \to H^1(G_v, E/K_v).$$

And, hence, give the map

$$H^1(G, E/K) \to \prod_{v \in M_K} H^1(G_v, E/K_v).$$

Now, we define the *Shafarevich-Tate group* $Ш(E/K)$ as the kernel of the above map.

3. Some Known Facts

Proposition 1 ([2]). *(1)* $Ш(E/K)$ *is a torsion group.*

(2) $Ш(E/K)[p] = \{x \in Ш(E/K) : px = 0\}$, *i.e.,* $Ш(E/K)(p)$, *the* p*-primary part of* $Ш(E/K)$, *is of finite corank.*

Proof. (1) Since $G = \varprojlim_{L/K:Galois} G_{L/K}$ is pro-finite, $H^1(G, E/K)$ is a torsion group. Therefore, $Ш(E/K)$ is a torsion group.

(2) The following sequence

$$0 \to E[p] \to E \xrightarrow{p} E \to 0$$

is exact. Hence, by acting G, we get the following long exact sequence

$$0 \to E(K)[p] \to E(K) \xrightarrow{p} E(K) \to H^1(G, E[p]) \to H^1(G, E) \xrightarrow{p} H^1(G, E).$$

Hence, the diagram

$$\begin{array}{ccccccccc} 0 \to & E(K)/pE(K) & \to & H^1(G, E[p]) & \to & H^1(G, E)[p] & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & \prod_{v \in M_K} E(K_v)/pE(K_v) & \to & \prod_{v \in M_K} H^1(G_v, E[p]) & \to & \prod_{v \in M_K} H^1(G_v, E)[p] & \to 0 \end{array}$$

is commutative. Therefore,

$$0 \to E(K)/pE(K) \to S^{(p)}(E/K) \to \text{Ш}(E/K)[p] \to 0$$

is exact. Here,

$$S^{(p)}(E/K) = Ker(H^1(G, E[p]) \to \prod_{v \in M_K} H^1(G_v, E)[p]),$$

which is called *p−Selmer group*. This group is finite and effectively computable. Therefore, $\text{Ш}(E/K)[p]$ is finite.

Conjecture 2. *$\text{Ш}(E/K)$ is finite.*

It is known that $\text{Ш}(2)$ and $\text{Ш}(3)$ are finite for thousands of elliptic curves over $\mathbb{Q}$.

Theorem 3 ([2]). *If $\text{Ш}(E/K)$ is finite, then there is a non-degenrate canonical alternating bilinear pairing*

$$\text{Ш}(E/K) \times \text{Ш}(E/K) \to \mathbb{Q}/\mathbb{Z}.$$

Lemma 4. *Let A be a finite abelian group. If there is a non-degenerate alternating bilinear pairing*

$$<,>: A \times A \rightarrow \mathbb{Q}/\mathbb{Z},$$

then, $A \cong S \times \hat{S}$ for some subgroup S of A, where $\hat{S}$ is the character group of S.

Proof. Let S be the subgroup of A such that $< s, s' >= 0$ for all $s, s' \in S$ and S is maximal with respect to this property. Since$< 1, 1 >= 0$, there is at least one subgroup with the property. Consider the character $\chi_a(s) =< a, s >$ of A, for each $a \in A$. They are all distinct, since the pairing $<,>$ is non-degenerate. Consider A/S. For each $a \in A/S$, we have a character of S defined by $\chi_a(s) =< a, s >$. By the definition of S, they are distinct. Therefore, $\hat{S} \cong A/S$. Therefore, $A \cong S \times \hat{S}$.

As a corollary, we have

Corollary 5 ([2]). *If $Ш(E/K)$ is finte, then it is a square.*

Until 1987, there was not a single example of an eliptic curve whose Safarevich-Tate group was known to be finite.

In 1987, Rubin proved that if E/Q has complex multiplication and $L(E/\mathbb{Q}, 1) \neq 0$, then $Ш(E/\mathbb{Q})$ is finite. Here $L(E/\mathbb{Q}, s)$ is $L-$series of $E/\mathbb{Q}$. He actually calculated $Ш(E/\mathbb{Q})$ for some elliptic curves with complex multiplication. For example, if E is given as $E : y^2 = x^3 - x$, then $Ш = 0$; if $E : y^2 = x^3 + 17x$, then $Ш = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; and if

$E : y^2 = x^3 - 2^8 3^4 5^2$, then $\text{Ш} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. These were the first known examples of elliptic curves with finite Safarevich-Tate groups.

In 1989, Kolyvagin proved that if $E/\mathbb{Q}$ is a modular curve and if $L(E/\mathbb{Q}, s)$ has no zero or simple zero at $s = 1$, then $\text{Ш}(E/\mathbb{Q})$ is finite. For example, if $E : y^2 = 4x^3 - 4x + 1$, then it has not complex multiplication, and $\text{Ш} = 0$.

Proposition 6. *Let L be a finite Galois extention field of a number field K with Galois group G. Let E be an elliptic curve over K. If $\text{Ш}(E/L)$ is finite, then so is $\text{Ш}(E/K)$.*

Proof. From the inflation-restriction exact sequence, we have the following commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \Phi & \longrightarrow & \text{Ш}(E/K) & \longrightarrow & \text{Ш}(E/L) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H^1(G, E(L)) & \longrightarrow & H^1(G_{\bar{K}/K}, E(\bar{K})) & \longrightarrow & H^1(G_{\bar{L}/L}, E(\bar{L})) \end{array}$$

Here, all vertical arrows are inclusions.

Since $H^1(G, E(L))$ is finite, so is Φ. Therefore, if $\text{Ш}(E/L)$ is finite, so is $\text{Ш}(E/K)$.

4. Main Result

Let G be a finite group. For any subgroup H of G, we put

$$\epsilon_H = \frac{1}{|H|} \sum_{\sigma \in H} \sigma \in \mathbb{Q}[G],$$

and call it the *idempotent associated with H*. Note that ϵ_H is indeed an idempotent in $\mathbb{Q}[G]$, i.e., $\epsilon_H^2 = \epsilon_H$.

A relation of the form

$$\sum_H n_H \epsilon_H = 0, \;\; n_H \in \mathbb{Q},$$

is called an *idempotent relation in* G. Whenever G is non-cyclic, G has a non-trivial idempotent relation [1].

Theorem 7 ([3]). *Let G be a fintie group, and let $\sum n_H \epsilon_H = \sum m_H \epsilon_H$, where n_H and m_H are non-negative intergers. Let $A = Z[|G|^{-1}]$. If M is a finite $A[G]-$module, then there a $A-$module isomorphism*

$$\bigoplus_H (M^{\epsilon_H})^{n_H} \to \bigoplus_H (M^{\epsilon_H})^{m_H}.$$

Here, $M^{\epsilon_H} = \{x^{\epsilon_H} : x \in M\}$.

In particular, $\prod_H |M^{\epsilon_H}|^{n_H} = \prod_H |M^{\epsilon_H}|^{m_H}$.

As a corollary, we have

Lemma 8. *If M is a finite $G-$module, and if $\sum_H n_H \epsilon_H = 0$ is an idempotent relation in G, then*

$$\prod_H |M^{\epsilon_H}|^{n_H} \sim_{|G|} 1.$$

Here, $a \sim_n b$ means a and b are the same up to prime factors of n.

Proof. Let $\tilde{M} = \{x \in M :$ The order of x is prime to $|G|.\}$. Then, $\tilde{M}$ is a finite $A-$module. Hence, by the above theorem, we have

$$\prod_H |\tilde{M}^{\epsilon_H}|^{n_H} = 1.$$

But, $\left|\tilde{M}^{\epsilon_H}\right| \sim_{|G|} \left|M^{\epsilon_H}\right|$. Therefore,

$$\prod_H \left|M^{\epsilon_H}\right|^{n_H} \sim_{|G|} 1.$$

Proposition 9. *Let M be a finite $G-$module. If $\sum_H n_H \epsilon_H = 0$ is an idempotent relation in G, then*

$$\prod_H \left|M^H\right|^{n_H} \sim_{|G|} 1.$$

Proof. By lemma 8, it is enough to show that $M^H = M^{\epsilon_H}$ as $A-$modules. If $x \in M^H$, then $x^\sigma = x$ for every $\sigma \in H$. Hence, $x^{\sum_{\sigma \in H} \sigma} = \left|H\right|x$, i.e., $x^{\epsilon_H} = x$. Therefore, $x \in M^{\epsilon_H}$.

Conversely, if $x \in M^{\epsilon_H}$, then $x = y^{\epsilon_H}$ for some $y \in M$. Let $\tau \in H$ be any element. Then,

$$x^\tau = y^{\epsilon_H \tau} = y^{\frac{1}{|H|}\sum_{\sigma \in H} \sigma\tau} = y^{\frac{1}{|H|}\sum_{\sigma \in H} \sigma} = y^{\epsilon_H} = x.$$

Hence, $x \in M^H$, which completes the proof.

Rerurning to our elliptic curve case, again we assume that E is an elliptic curve over a number field K, and L is a finite Galois extention field with Galois group G.

Suppose $\sum_H n_H \epsilon_H = 0$ is an idempotent relation in G.

Lemma 10. $\prod_H \left|E_{tors}(L^H)\right| \sim_{|G|} 1.$

Proof. $E_{tors}(L)$ is a finite $G-$module. Therefore, by Proposition 9, we get the result.

Lemma 11. $|\text{Ш}(E/L^H)| \sim_{|G|} |\text{Ш}(E/L)^H|$.

Proof. We have the following commutative diagram with inflation- restriction exact rows

$$\begin{array}{ccccccccc} 0 \to & \Phi & \to & \text{Ш}(E/L^H) & \to & \text{Ш}(E/L)^H & \to & \Psi \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 \to & H^1(H, E(L)) & \to & H^1(G_{\bar{L}^H/L^H}, E) & \to & H^1(G_{\bar{L}/L}, E)^H & \to & H^2(H, E(L)) \end{array}$$

Here, all vertical arrows are inclusions.

Since $E(L)$ is finitely generated, $H^1(H, E(L))$ and $H^2(H, E(L))$ are finite groups annihilated by $|H|$, hence by $|G|$. Hence, Φ and Ψ are also finite groups annihilated by $|G|$, i.e.,

$$|\Phi| \sim_{|G|} 1, \ |\Psi| \sim_{|G|} 1.$$

Therefore, we have

$$|\text{Ш}(E/L^H)| \sim_{|G|} |\text{Ш}(E/L)^H|.$$

Combining Propositon 9 and Lemma 11, we have

Theorem 12. $\prod_H |\text{Ш}(E/L^H)|^{n_H} \sim_{|G|} 1$.

Reference

1. E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math.Annalen **284** (1989), 307-327.
2. J. Tate, *On the conjecture of Birch and Swinnerton-Dyer and a geometric analogy*, Seminar Bourbaki **306** (1966).
3. C Walter, *Brauer's class number relation*, Acta Arithmetic XXXV (1979), 33-40.

Department of Mathematics Chonbuk National University Chonju Chonbug 560-756, Korea
E-mail: hsp1129@chonbuk.ac.kr