

RELATIONS AMONG SHAFAREVICH-TATE GROUPS

HWASIN PARK AND DAEYEOL KIM

Dept. of Mathematics,

Chonbuk National University, Chonju, Chonbuk 561-756, Korea.

1. Group Cohomology

Let G be a (finite) group, and let A be an abelian group on which G acts, i.e., A is a 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

$$C^1(G, A) = \text{hom}(G, A),$$

$$Z^1(G, A) = \{f \in \text{hom}(G, A) : f(\sigma\tau) = \sigma f(\tau) + f(\sigma) \quad \forall \sigma, \tau \in G\},$$

$$B^1(G, A) = \{f \in \text{hom}(G, A) : \exists a \in A \text{ s.t. } f(\sigma) = \sigma a - a \quad \forall \sigma \in G\}.$$

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 $H^1(G, A) = \text{hom}(G, A)$.

Now, if A is a G -module, and if H is any subgroup of G , then A is an H -module. Hence, we get the restriction map $Z^1(G, A) \rightarrow Z^1(H, A)$. Also, under this map, $B^1(G, A)$ maps into $B^1(H, A)$. Hence, they induce the restriction map $H^1(G, A) \rightarrow H^1(H, A)$. If

Received April 16, 1999.

This was partially supported by KOSEF, 1996, 961-0101-003-2.

$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is an exact sequence of G -modules, then we have the following long exact sequence of homologies

$$\begin{aligned} 0 \rightarrow H^0(G, A) \rightarrow H^0(G, B) \rightarrow H^0(G, C) \\ \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C). \end{aligned}$$

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

Then, we have the following exact sequence.

$$0 \rightarrow H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A).$$

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,

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

And, hence, give the map

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

Now, we define the *Shafarevich-Tate group* $\text{|||}(E/K)$ as the kernel of the above map.

3. Some Known Facts

PROPOSITION 1 ([2]). (1) $\text{|||}(E/K)$ is a torsion group.

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

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

(2) The following sequence

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

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

$$\begin{aligned} 0 \rightarrow E(K)[p] \rightarrow E(K) \xrightarrow{p} E(K) \\ \rightarrow H^1(G, E[p]) \rightarrow H^1(G, E) \xrightarrow{p} H^1(G, E). \end{aligned}$$

Hence, the diagram

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

is commutative. Therefore,

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

is exact. Here,

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

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

CONJECTURE 2. $\underline{\underline{\underline{\underline{\quad}}}}(E/K)$ is finite.

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

THEOREM 3 ([2]). If $\underline{\underline{\underline{\underline{\quad}}}}(E/K)$ is finite, then there is a non-degenerate canonical alternating bilinear pairing

$$\underline{\underline{\underline{\underline{\quad}}}}(E/K) \times \underline{\underline{\underline{\underline{\quad}}}}(E/K) \rightarrow \mathbb{Q}/\mathbb{Z}.$$

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

$$\langle, \rangle: A \times A \rightarrow \mathbb{Q}/\mathbb{Z},$$

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

As a corollary, we have

COROLLARY 5 ([2]). If $\underline{\underline{\underline{\underline{\quad}}}}(E/K)$ is finite, then it is a square.

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

In 1987, Rubin proved that if E/\mathbb{Q} has complex multiplication and $L(E/\mathbb{Q}, 1) \neq 0$, then $\underline{\underline{\underline{\underline{\quad}}}}(E/\mathbb{Q})$ is finite. Here $L(E/\mathbb{Q}, s)$ is L -series of E/\mathbb{Q} . He actually calculated $\underline{\underline{\underline{\underline{\quad}}}}(E/\mathbb{Q})$ for some elliptic curves with complex multiplication. For example, if E is given as $E : y^2 = x^3 - x$, then $\underline{\underline{\underline{\underline{\quad}}}} = 0$; if $E : y^2 = x^3 + 17x$, then $\underline{\underline{\underline{\underline{\quad}}}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; and if $E : y^2 = x^3 - 2^8 3^4 5^2$, then

$\text{III} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. These were the first known examples of elliptic curves with finite Shafarevich-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 $\text{III}(E/\mathbb{Q})$ is finite. For example, if $E : y^2 = 4x^3 - 4x + 1$, then it has not complex multiplication, and $\text{III} = 0$.

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

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

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

Here, all vertical arrows are inclusions.

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

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

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

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 finite group, and let $\sum n_H \epsilon_H = \sum m_H \epsilon_H$, where n_H and m_H are non-negative integers. Let $A = Z[|G|^{-1}]$. If M is a finite $A[G]$ -module, then there is a A -module isomorphism

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

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 $\tilde{M} = \{x \in M : \text{The order of } x \text{ is prime to } |G|\}$. 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, $|\tilde{M}^{\epsilon_H}| \sim_{|G|} |M^{\epsilon_H}|$. Therefore,

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

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

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

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, $x^{\sum_{\sigma \in H} \sigma} = |H|x$, 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.

Returning 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 extension field with Galois group G .

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

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

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

LEMMA 11. $|\underline{\underline{|||}}(E/L^H)| \sim_{|G|} |\underline{\underline{|||}}(E/L)^H|$.

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

$$\begin{array}{ccccccc} 0 \rightarrow & \Phi & \rightarrow & \underline{\underline{|||}}(E/L^H) & \rightarrow & \underline{\underline{|||}}(E/L)^H & \rightarrow & \Psi \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 \rightarrow & H^1(H, E(L)) & \rightarrow & H^1(G_{L^H/L^H}, E) & \rightarrow & H^1(G_{L/L}, E)^H & \rightarrow & H^2(H, E(L)) \end{array}$$

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.,

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

Therefore, we have

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

Combining Proposition 9 and Lemma 11, we have

THEOREM 12. $\prod_H |\underline{\underline{|||}}(E/L^H)|^{n_H} \sim_{|G|} 1$.

References

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 Arithmetica **XXXV** (1979), 33-40.