Functiones et Approximatio
47.2 (2012), 149–156
doi: 10.7169/facm/2012.47.2.2

A RELATION BETWEEN THE BRAUER GROUP AND THE TATE-SHAFAREVICH GROUP

Chuangxun Cheng

Abstract: In this paper, we prove a relation between the Brauer group and the Tate-Shafarevich group for genus one curves over number fields. This is a generalization of a result of Milne in genus one curves case.

Keywords: Brauer group, Tate-Shafarevich group.

1. Introduction

Let K be a number field, and let Ω_K be the set of primes of K. The completion of K at $v \in \Omega_K$ is denoted by K_v. Let E be an elliptic curve over K. Define $Ш(E,K)$ and $\mathcal{H}_v(E,K)$ by

$$Ш(E,K) = Ker(H^1(G_K, E) \to \bigoplus_{v' \in \Omega_K} H^1(G_{K_{v'}}, E)),$$
$$\mathcal{H}_v(E,K) = Ker(H^1(G_K, E) \to \bigoplus_{v' \neq v} H^1(G_{K_{v'}}, E)).$$

Then we define $\mathcal{H}(E,K) = \cup_v \mathcal{H}_v(E,K) \supset Ш(E,K)$. The set $\mathcal{H}(E,K)$ is called *Kolyvagin set* in [1]. Let $C \in \mathcal{H}(E,K)$, then $C(K_v) = \emptyset$ for at most one $v \in \Omega_K$. Set

$$Br(C)' = Ker\left(Br(C_K) \to \bigoplus_{v \in \Omega_K} Br(C_v)\right).$$

In [5], the author proves a comparison result between $Br(C)'$ and $Ш(E)$ in the case $C \in Ш(E,K)$. (Note that the result in [5] is for general abelian varieties.) In this paper, we extend the result in [5] to the case that $C \in \mathcal{H}(E,K)$, and draw some consequences on the Brauer-Manin obstruction.

To state our theorems, we first recall some results about *period* and *index*. Let $C \in \mathcal{H}(E,K)$. Let $\mathfrak{p} \in \Omega_K$ such that $C(K_v) \neq \emptyset$ for $v \neq \mathfrak{p}$. By Proposition 6 of [1],

2010 Mathematics Subject Classification: primary: 11G05; secondary: 11G35

we know that the period and the index of C are equal. We denote it by d. By Theorem 3 of [3], we know that the period and the index of $C_{K_{\mathfrak{p}}}$ are equal. Denote it by $d_{\mathfrak{p}}$. It is obvious that $d_{\mathfrak{p}}|d$. Let $d'_{\mathfrak{p}} = d/d_{\mathfrak{p}}$. We also write Q for the group $\mathbb{Q}/\mathbb{Z}$, and Q' the quotient of $\mathbb{Q}/\mathbb{Z}$ by the subgroup $\frac{1}{d_{\mathfrak{p}}}\mathbb{Z}/\mathbb{Z}$. For $q \in Q$, we write $\bar{q}$ the image of q in Q' under the obvious map $Q \to Q'$. Note that Q' is isomorphic to Q.

Theorem 1.1. *With the notations as above, let $C \in \mathcal{H}(E,K)$, and assume that $\text{Ш}(E,K)$ has no nonzero infinitely divisible elements. Then there is an exact sequence*

$$0 \to Br(C)' \to \text{Ш}(E,K)/T_1 \to T_2 \to 0$$

in which T_1 and T_2 are finite groups of order $d'_{\mathfrak{p}}$. In particular, if one of $Br(C)'$ or $\text{Ш}(E,K)$ is finite, so is the other, and their orders are related by

$$(d'_{\mathfrak{p}})^2 \sharp Br(C)' = \sharp \text{Ш}(E,K).$$

Remark 1.2. If C is actually an element in $\text{Ш}(E,K)$, then $d_{\mathfrak{p}} = 1$ and $d'_{\mathfrak{p}} = d$. The result in Theorem 1.1 then recovers the main theorem of [5] in the case of genus one curves.

Let $B = Ker(Br(C_K) \to \oplus_{v \in \Omega_K} H^1(G_{K_v}, Pic(C_{\bar{K}_v})))$. (See (2.2) for the construction of this map.) In section 2.1, we define a pairing

$$<,>^b \colon B \times \prod_{v \neq \mathfrak{p}} C(K_v) \to Q'.$$

Then define

$$\left(\prod_{v \neq \mathfrak{p}} C(K_v)\right)^B = \left\{ (x_v)_{v \neq \mathfrak{p}} \in \prod_{v \neq \mathfrak{p}} C(K_v) \mid < b, (x_v) >^b = 0 \text{ for all } b \in B \right\}.$$

We have the following theorem which is an analogue of a result in [6].

Theorem 1.3. *Let $C \in \mathcal{H}(E,K)$, assume that $\text{Ш}(E,K)$ is finite, then*

$$\left(\prod_{v \neq \mathfrak{p}} C(K_v)\right)^B \neq \emptyset \Leftrightarrow d'_{\mathfrak{p}} = 1.$$

We fix some notation. If L is a perfect field, we write G_L for the absolute Galois group $Gal(\bar{L}/L)$. If X is a variety over L and $L \subset L'$ is an inclusion of fields, we write $X_{L'}$ for the base change $X \times_{SpecL} SpecL'$. We also write $K(X)$ for the function field of X.

2. Proof of the theorems

2.1. Some definitions

The Hochschild-Serre spectral sequence

$$H^r(G_K, H^s(C_{\bar{K}}, \mathbb{G}_m)) \Rightarrow H^{r+s}(C_K, \mathbb{G}_m)$$

yields

$$\begin{aligned} 0 &\to Pic(C_K) \to (Pic(C_{\bar{K}}))^{G_K} \to Br(K) \\ &\to Br(C_K) \to H^1(G_K, Pic(C_{\bar{K}})) \to H^3(G_K, \bar{K}^\times) = 0 \end{aligned} \tag{2.1}$$

If L is any local or global field then $H^3(G_L, \bar{L}^\times) = 0$. If $v \neq \mathfrak{p}$, then $C(K_v) \neq \emptyset$, the local points provide section maps $Br(C_{K_v}) \to Br(K_v)$, so that in the corresponding sequence for K_v, $Br(K_v) \to Br(C_{K_v})$ is injective. If $v = \mathfrak{p}$, then from the proof of Theorem 3 in [3], the image of $(Pic(C_{\bar{K}_v}))^{G_{K_v}}$ in $Br(K_\mathfrak{p}) = \mathbb{Q}/\mathbb{Z}$ is $\frac{1}{d_\mathfrak{p}}\mathbb{Z}/\mathbb{Z}$. We have the following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Br(K) & \longrightarrow & Br(C_K) & \longrightarrow & H^1(G_K, Pic(C_{\bar{K}})) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \oplus_v Br(K_v) & \longrightarrow & \oplus_v Br(C_{K_v}) & \longrightarrow & \oplus_v H^1(G_{K_v}, Pic(C_{\bar{K}_v})) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \sum_v inv_v} & & & & & & \\ & & Q & & & & & & \end{array} \tag{2.2}$$

We only have to check the injectivity of $Br(K) \to Br(C_K)$. If $D \in Ker(Br(K) \to Br(C_K))$, then D maps to 0 in $Br(C_{K_v})$ for all $v \neq \mathfrak{p}$. Therefore $D \otimes K_v \in Br(K_v)$ is trivial for all $v \neq \mathfrak{p}$ and therefore $D \otimes K_v$ is trivial for all v. So D is zero by the injectivity of $Br(K) \to \oplus_v Br(K_v)$. From the diagram, we have

$$Pic(C_K) = (Pic(C_{\bar{K}}))^{G_K}.$$

Remark 2.1. This identity shows that there is no obstruction for a rational divisor class being represented by a rational divisor. Therefore, the index of C and the period of C are the same.

We define

$$Ш(P, K) = Ker(H^1(G_K, Pic(C_{\bar{K}})) \to \oplus_v H^1(G_{K_v}, Pic(C_{\bar{K}_v}))),$$

and

$$B = Ker(Br(C_K) \to \oplus_{v \in \Omega_K} H^1(G_{K_v}, Pic(C_{\bar{K}_v}))).$$

Suppose $b \in B$, and let (b_v) be its image in $\oplus_v Br(C_{K_v})$. By the definition of of B, (b_v) is the image of an element $(a_v) \in \oplus_v Br(K_v)$. Note that a_v is unique if $v \neq \mathfrak{p}$, $a_{\mathfrak{p}}$ is not uniquely determined. For any $(x_v)_{v\neq\mathfrak{p}} \in \prod_{v\neq\mathfrak{p}} C(K_v)$, we have $ev_v(b_v, x_v) = a_v$. (Here ev_v is the evaluation map $Br(C_{K_v}) \times C(K_v) \to Br(K_v)$.) Thus $< b, (x_v) >^b = (\sum_{v\neq\mathfrak{p}} ev_v(b_v, x_v) + inv_{\mathfrak{p}}(a_{\mathfrak{p}}))^-$ is a well-defined pairing

$$<,>^b : B \times \prod_{v\neq\mathfrak{p}} C(K_v) \to Q'.$$

This pairing gives us a map $\chi : B \to Q'$. In particular, we see that

$$\left(\prod_{v\neq\mathfrak{p}} C(K_v)\right)^B \neq \emptyset \iff \chi = 0.$$

Lemma 2.2. *There is an exact sequence*

$$0 \to Br(C)' \to Ш(P, K) \xrightarrow{\phi} Q'.$$

Proof. This is essentially the Snake lemma. The difference is that in (2.2), the first map in second row is not injective. Let $p \in Ш(P, K)$. By diagram chasing, it is easy to get an element $(b_v^p)_v \in \oplus_v Br(C_{K_v})$ which maps to zero in $\oplus_{v\in\Omega_K} H^1(G_{K_v}, Pic(C_{\bar{K}_v}))$. Every lift $(b_v)_v$ of $(b_v^p)_v$ in $\oplus_v Br(K_v)$ gives an element in Q. All the elements give the same element in Q' under the map $Q \to Q'$. So we obtain a well defined map $\phi : Ш(P, K) \to Q'$. We have to check that $Ker(\phi) \subset Br(C)'$.

Assume that $p \in Ker(\phi)$. Let $b^p \in Br(C_K)$ be a preimage of p, $(b_v^p)_v$ be the image of b^p in $\oplus_v Br(C_{K_v})$, and $(b_v)_v$ a lift of $(b_v^p)_v$ in $\oplus_v Br(K_v)$. Then $(\sum_v inv_v(b_v))^- = 0 \in Q'$. Note that the image of $(Pic(C_{\bar{K}_{\mathfrak{p}}}))^{G_{K_{\mathfrak{p}}}}$ in $Br(K_{\mathfrak{p}})$ is $\frac{1}{d_{\mathfrak{p}}}\mathbb{Z}/\mathbb{Z}$, we may choose a different lift $b'_{\mathfrak{p}}$ of $b^p_{\mathfrak{p}}$, such that $\sum_v inv_v(b'_v) = 0 \in Q$, where $b'_v = b_v$ if $v \neq \mathfrak{p}$. Let $b \in Br(K)$ be the preimage of $(b'_v)_v$ in $Br(K)$, b' be the image of b in $Br(C_K)$, then $b^p - b'$ is an element in $Br(C)'$ which maps to p. The lemma follows. ■

2.2. Cassels-Tate pairing

The following definition is from [5]. From the exact sequence of G_K modules

$$1 \to \bar{K}^\times \to K(C_{\bar{K}})^\times \to Div(C_{\bar{K}}) \to Pic(C_{\bar{K}}) \to 0$$

we obtain the following diagram

$$\begin{array}{ccccc} & & H^1(G_K, Div(C_{\bar{K}})) = 0 & & \\ & & \downarrow & & \\ Br(K) & & H^1(G_K, Pic(C_{\bar{K}})) & & \\ \downarrow & & \downarrow & & \\ H^2(G_K, K(C_{\bar{K}})^\times) & \longrightarrow & H^2(G_K, K(C_{\bar{K}})^\times/\bar{K}^\times) & \longrightarrow & H^3(G_K, \bar{K}^\times) = 0 \\ & & \downarrow & & \\ & & H^2(G_K, Div(C_{\bar{K}})) & & \end{array} \tag{2.3}$$

In the following, we use δ to denote the boundary operator. Write S for the map $Div(C_{\bar{K}}) \to Pic(C_{\bar{K}})$. Represent $\alpha \in Ш(P,K)$ by a cocycle $a \in Z^1(G_K, Pic(C_{\bar{K}}))$, and let $\mathfrak{a} \in C^1(G_K, Div(C_{\bar{K}}))$ be such that $S(\mathfrak{a}) = a$. Then $\delta(\mathfrak{a}) \in Z^2(G_K, K(C_{\bar{K}})^\times/\bar{K}^\times)$. We can lift it to an element $f \in Z^2(G_K, K(C_{\bar{K}})^\times)$. On the other hand, a is locally trivial. Write $Res_v a = \delta(a_v)$ with $a_v \in C^0(G_{K_v}, Pic(C_{\bar{K}_v}))$ and let $\mathfrak{a}_v \in C^0(G_{K_v}, Div(C_{\bar{K}_v}))$ such that $S(\mathfrak{a}_v) = a_v$. We see that $S(Res_v \mathfrak{a}) = Res_v a = \delta(a_v) = S(\delta(\mathfrak{a}_v))$, therefore $Res_v \mathfrak{a} = \delta(\mathfrak{a}_v) + (f_v)$ with $f_v \in C^1(G_{K_v}, K(C_{\bar{K}_v})^\times)$. Since $\delta(Res_v f/\delta f_v) = 0$, we see that $Res_v f/\delta f_v \in Z^2(G_{K_v}, \bar{K}_v^\times)$. Let γ_v be the class of $Res_v f/\delta f_v$ in $Br(K_v)$, then $\phi(\alpha)$ is $(\sum_v inv_v(\gamma_v))^-$, i.e., the image of $\sum_v inv_v(\gamma_v)$ in Q'.

Note that if $\mathfrak{c}_v$ is any divisor of degree $d_\mathfrak{p}$ on C_{K_v} such that neither f nor δf_v has a zero or a pole in the support of $\mathfrak{c}_v$, then $(Res_v f)(\mathfrak{c}_v)/\delta f_v(\mathfrak{c}_v) = d_\mathfrak{p}(Res_v f/\delta f_v)$. Because $\delta f_v(\mathfrak{c}_v) = \delta(f_v(\mathfrak{c}_v))$ with $f_v(\mathfrak{c}_v) \in C^1(G_{K_v}, \bar{K}_v^\times)$, we have that $d_\mathfrak{p}\gamma_v$ is represented by $f(\mathfrak{c}_v)$. See section 4 of [4] for more details.

Now we recall the definition of Cassels-Tate pairing

$$<,>: Ш(E,K) \times Ш(E,K) \to Q.$$

Let $\alpha \in Ш(E,K)$ be represented by $a \in Z^1(G_K, E(\bar{K}))$, and let $Res_v a = \delta a_v$ with $a_v \in Z^0(G_{K_v}, E(\bar{K}_v))$. Write

$$\begin{aligned} a &= S(\mathfrak{a}), & \mathfrak{a} &\in C^1(G_K, Div^0(C_{\bar{K}})) \\ a_v &= S(\mathfrak{a}_v), & \mathfrak{a}_v &\in C^0(G_{K_v}, Div^0(C_{\bar{K}_v})). \end{aligned}$$

We have $Res_v \mathfrak{a} = \delta\mathfrak{a}_v + (f_v)$ in $C^1(G_{K_v}, Div^0(C_{\bar{K}_v}))$ with $f_v \in C^1(G_{K_v}, K(C_{\bar{K}_v}))^\times)$. Moreover, $\delta\mathfrak{a} = (f)$ where $f \in Z^2(G_K, K(C_{\bar{K}})^\times)$. Let β be another element of $Ш(E,K)$ and define $\mathfrak{b}$, $\mathfrak{b}_v$, g_v and g as for α. Note that $g \cup \mathfrak{a} - f \cup \mathfrak{b}$ is an element in $C^3(G_K, \bar{K}^\times)$ such that $\delta(g \cup \mathfrak{a} - f \cup \mathfrak{b}) = 0$. We may assume that $g \cup \mathfrak{a} - f \cup \mathfrak{b} = \delta\theta$ where $\theta \in C^2(G_K, \bar{K}^\times)$.

Let $\gamma_v \in Br(K_v)$ be the class of $g_v \cup Res_v \mathfrak{a} - \mathfrak{b}_v \cup Res_v f - Res_v \theta$, where $\cup$ is the cup-product pairing induced by $(f, \mathfrak{a}) \mapsto f(\mathfrak{a})$ for $f \in K(C_{\bar{K}})^\times$ and $\mathfrak{a} \in Div(C_{\bar{K}})$. Then the Cassels-Tate pairing is defined by

$$< \alpha, \beta >= \sum_v inv_v(\gamma_v).$$

Remark 2.3. Note that in the definition in [5], the θ is omitted.

Let $<,>'$: $Ш(E,K) \times Ш(E,K) \to Q'$ be the composition of the Cassels-Tate pairing and the natural map $Q \to Q'$.

2.3. The proof

The idea is to give another description of ϕ using Cassels-Tate pairing. Consider the cohomology sequence of

$$0 \to E \to Pic(C) \to \mathbb{Z} \to 0$$

we get the following diagram

$$\begin{array}{ccccccccc}
P(K) & \xrightarrow{deg} & \mathbb{Z} & \longrightarrow & H^1(G_K, E) & \longrightarrow & H^1(G_K, P) & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\oplus_v P(K_v) & \xrightarrow{(deg_v)_v} & \oplus_v \mathbb{Z} & \longrightarrow & \oplus_v H^1(G_{K_v}, E) & \longrightarrow & \oplus_v H^1(G_{K_v}, P) & \longrightarrow & 0
\end{array} \tag{2.4}$$

Note that $Im(deg) = d\mathbb{Z}$, $Im(deg_{\mathfrak{p}}) = d_{\mathfrak{p}}\mathbb{Z}$, and deg_v is surjective if $v \neq \mathfrak{p}$. By Snake lemma, we have a short exact sequence

$$0 \to \mathbb{Z}/d'_{\mathfrak{p}}\mathbb{Z} \to Ш(E, K) \xrightarrow{\rho} Ш(P, K) \to 0.$$

Let T_1 be the image of $\mathbb{Z}/d'_{\mathfrak{p}}\mathbb{Z}$ in $Ш(E, K)$, and let T_2 be the image of the map $\phi : Ш(P, K) \to Q'$ in Lemma 2.1. From the diagram

$$\begin{array}{ccccccc}
 & & & & 0 & & \\
 & & & & \downarrow & & \\
 & & & & T_1 & & \\
 & & & & \downarrow & & \\
 & & & & Ш(E, K) & & \\
 & & & & \downarrow \rho & \searrow & \\
0 & \longrightarrow & Br(C)' & \longrightarrow & Ш(P, K) & \xrightarrow{\phi} & Q' \\
 & & & & \downarrow & & \\
 & & & & 0 & &
\end{array}$$

we get a short exact sequence

$$0 \to Br(C)' \to Ш(E, K)/T_1 \to T_2 \to 0.$$

The theorems follows from the following lemma.

Lemma 2.4. *Let* $\beta \in Ш(E,K)$ *be a generator of* T_1. *Then the composite*

$$Ш(E,K) \xrightarrow{\rho} Ш(P,K) \xrightarrow{\phi} Q'$$

is $\alpha \mapsto < \alpha, \beta >'$.

Proof. Let $\alpha \in Ш(E,K)$ and define $\mathfrak{a}$, $\mathfrak{a}_v$, f_v and f as above. We know that $\phi(\rho(\alpha))$ is the image of $\sum inv_v(\gamma_v)$ in Q' where $d_{\mathfrak{p}}\gamma_v$ is represented by $f(\mathfrak{c}_v)$ for some divisor $\mathfrak{c}_v$ of degree $d_{\mathfrak{p}}$ on C_{K_v}.

On the other hand, let P be any point of $C_{\bar{K}}$. Let $\mathfrak{b} = d_{\mathfrak{p}}(\delta P)$. Then $\beta \in Ш(E,K)$ is represented by $b = S(\mathfrak{b})$. In the construction of Cassels-Tate pairing, we choose $\mathfrak{b}_v = d_{\mathfrak{p}}P - \mathfrak{c}_v$. First, since $\delta(S(\mathfrak{b}_v)) = S(\delta(d_{\mathfrak{p}}P)) = Res_v b$, we may choose $g_v = 1$. Second, since $\delta(\mathfrak{b}) = 0$, we may choose $g = 0$. Now, with the choices of g and g_v, we have $g \cup \mathfrak{a} - f \cup \mathfrak{b} = -f \cup \mathfrak{b} = -d_{\mathfrak{p}}\delta(f(P)) = 0$ because $\delta(f) = 0$ from the construction. Therefore $< \alpha, \beta >= -\sum_v inv_v(\gamma'_v)$ where γ'_v is represented by $f(\mathfrak{b}_v) = f(d_{\mathfrak{p}}P)/f(\mathfrak{c}_v)$. Let γ be the class of $f(d_{\mathfrak{p}}P)$ in $Br(K)$. Then

$$\begin{aligned} < \alpha, \beta >' &= (< \alpha, \beta >)^- \\ &= (-\sum_v inv_v(\gamma'_v))^- = (-\sum_v inv_v(\gamma/\gamma_v))^- \\ &= (\sum inv_v(\gamma_v) - \sum inv_v(\gamma))^- = (\sum inv_v(\gamma_v))^- \\ &= \phi(\rho(\alpha)). \end{aligned}$$

■

Remark 2.5.

(1) The reason for the assumption that $Ш(K,E)$ is finite in Theorem 1.3 is that the Cassels-Tate pairing is non degenerate under this assumption.

(2) For any $C \in H^1(G_K, E)$, we know that $C(K_v) \neq \emptyset$ for almost all $v \in \Omega_K$. We can generalize Theorem 1.1, and get a relation between $Br(C)'$ and $Ш(K,E)$. But this relation will be more complicated because in general the relation between the period of C and the index of C is not as simple as in the case we considered. After the author wrote these notes, he found out that in [2], Cristian D. Gonzalez-Aviles proved a general theorem which gave a relation between the Brauer groups and the Tate-Shafarevich groups. The idea in [2] is essentially the same as the idea in [5].

Acknowledgements. The author would like to thank the referee for helpful suggestions.

References

[1] P. Clark, *There are genus one curves of every index over every number field.* J. Reine Angew. Math. **594** (2006), 201–206.

[2] C.D. Gonzalez-Aviles, *Brauer groups and Tate-Shafarevich groups*, J. Math. Sci. Univ. Tokyo **10** (2003), 391–419.
[3] S. Lichtenbaum, *The period-index problem for elliptic curves*, Amer. J. of Math. **90** (1968), 1209–1223.
[4] S. Lichtenbaum, *Duality theorems for curves over p-adic fields*, Inventiones Math. **7** (1969), 120–136.
[5] J. Milne, *Comparison of the Brauer group with the Tate-Shafarevich group*, J. Fac. Science, Univ. Tokyo, Sec. IA
[6] V. Scharaschkin, *The Brauer-Manin obstruction for curves.*
[7] J. Silverman, *The arithmetic of elliptic curves*, GTM **106**, Springer-Verlag.

Address: Chuangxun Cheng: Department of Mathematics, Northwestern University, Evanston, IL, USA 60208.

E-mail: cxcheng@math.northwestern.edu

Received: 4 August 2011