Functiones et Approximatio
54.1 (2016), 39–55
doi: 10.7169/facm/2016.54.1.4

MILNOR K-GROUPS ATTACHED TO ELLIPTIC CURVES OVER A p-ADIC FIELD

Toshiro Hiranouchi

Abstract: We study the Galois symbol map of the Milnor K-group attached to elliptic curves over a p-adic field. As by-products, we determine the structure of the Chow group for the product of elliptic curves over a p-adic field under some assumptions.

Keywords: Elliptic curves, Chow groups, Local fields.

1. Introduction

K. Kato and M. Somekawa introduced in [13] the Milnor type K-group $K(k; G_1, \dots, G_q)$ attached to semi-abelian varieties $G_1, \dots, G_q$ over a field k which is now called the *Somekawa K-group*. The group is defined by the quotient

$$K(k; G_1, \dots, G_q) := \left(\bigoplus_{k'/k:\,\mathrm{finite}} G_1(k') \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} G_q(k') \right) /R \tag{1}$$

where k' runs through all finite extensions over k and R is the subgroup which produces “the projection formula” and “the Weil reciprocity law” as in the Milnor K-theory. As a special case, for the multiplicative groups $G_1 = \cdots = G_q = \mathbb{G}_m$, the group $K(k; \overbrace{\mathbb{G}_m, \dots, \mathbb{G}_m}^{q})$ is isomorphic to the ordinary Milnor K-group $K_q^M(k)$ of the field k ([13], Thm. 1.4). For general semi-abelian varieities $G_1, \dots, G_q$, let $G_i[m]$ be the Galois module defined by the kernel of $G_i(\overline{k}) \xrightarrow{m} G_i(\overline{k})$ the multiplication by a positive integer m prime to the characteristic of k. Somekawa defined also the Galois symbol map

$$h : K(k; G_1, \dots, G_q)/m \to H^q(k, G_1[m] \otimes \cdots \otimes G_q[m])$$

by the similar way as in the classical Galois symbol map $K_q^M(k)/m \to H^q(k, \mu_m^{\otimes q})$ on the Milnor K-group, where $\mu_m = \mathbb{G}_m[m]$ is the Galois module of all m-th

2010 Mathematics Subject Classification: primary: 11G07

roots of unity. He also presented a "conjecture" in which the map h is injective for arbitrary field k. For the case $G_1 = \cdots = G_q = \mathbb{G}_m$, the conjecture holds by the Milnor-Bloch-Kato conjecture, now is a theorem of Voevodsky, Rost, and Weibel ([17]). Although it holds in some special cases ([18], [19], and [9]), Spieß and Yamazaki disproved this for some tori ([14], Prop. 7).

The aim of this note is to show this "conjecture" for elliptic curves over a local field under some assumptions.

Theorem 1.1 (Thm. 4.1, Prop. 4.2). *Let k be a finite field extension of the p-adic field $\mathbb{Q}_p$ and n a positive integer.*

(i) *Let q be an integer $\geqslant 3$ and $E_1, \ldots, E_q$ be elliptic curves over k with $E_i[p] \subset E_i(k)$ for $i = 1, \ldots, q$. Assume that E_1 has good ordinary reduction or split multiplicative reduction, and E_i has good reduction or split multiplicative reduction for $i = 2, \ldots, q$. Then, we have*

$$K(k; E_1 \ldots, E_q)/p^n = 0.$$

(ii) *Let E_1, E_2 be elliptic curves over k with $E_i[p^n] \subset E_i(k)$ for $i = 1, 2$. Assume that E_1 has good ordinary reduction or split multiplicative reduction, and E_2 has good reduction or split multiplicative reduction. Then, the Galois symbol map*

$$h : K(k; E_1, E_2)/p^n \to H^2(k, E_1[p^n] \otimes E_2[p^n])$$

is injective.

The theorem above is known when E_i's have *semi-ordinary reduction*, that is, good ordinary or multiplicative reduction ([18], [9], see also [8]). Hence our main interest is in elliptic curves which have good supersingular reduction.

In our previous paper [3], we investigate the image of the Galois symbol map h. As byproducts, we obtain the structure of the Chow group $\mathrm{CH}_0(E_1 \times E_2)$ of 0-cycles as follows. By Corollary 2.4.1 in [9], we have

$$\mathrm{CH}_0(E_1 \times E_2) \simeq \mathbb{Z} \oplus E_1(k) \oplus E_2(k) \oplus K(k; E_1, E_2).$$

The Albanese kernel $T(E_1 \times E_2) := \mathrm{Ker}(\mathrm{alb} : \mathrm{CH}_0(E_1 \times E_2)^0 \to (E_1 \times E_2)(k))$ coincides with the Somekawa K-group $K(k; E_1, E_2)$, where $\mathrm{CH}_0(E_1 \times E_2)^0$ is the kernel of the degree map $\mathrm{CH}_0(E_1 \times E_2) \to \mathbb{Z}$. Mattuck's theorem [6] implies the following:

Corollary 1.2. *Let E_1 and E_2 be elliptic curves over k with good or split multiplicative reduction. Assume that E_1 does not have good supersingular reduction and $E_i[p^n] \subset E_i(k)$ for $i = 1, 2$. Then, we have*

$$\mathrm{CH}_0(E_1 \times E_2)/p^n \simeq \begin{cases} (\mathbb{Z}/p^n)^{2[k:\mathbb{Q}_p]+6}, & \text{if } E_1 \text{ and } E_2 \text{ have a same reduction type,} \\ (\mathbb{Z}/p^n)^{2[k:\mathbb{Q}_p]+7}, & \text{otherwise.} \end{cases}$$

Notation

Throughout this note, for an abelian group A and a positive integer m, let $A[m]$ be the kernel and A/m the cokernel of the map $m : A \to A$ defined by the multiplication by m. For a field F, we denote by F^{sep} the separable closure of F and $G_F := \mathrm{Gal}(F^{\mathrm{sep}}/F)$ the absolute Galois group of F. We also denote by $H^i(F, M) := H^i(G_F, M)$ the Galois cohomology group of G_F for a G_F-module M. The tensor product $A \otimes B$ for abelian groups A, B means $A \otimes_{\mathbb{Z}} B$.

For a finite field extension $K/\mathbb{Q}_p$, we denote by v_K the normalized valuation, $\mathfrak{m}_K$ the maximal ideal of the valuation ring $\mathcal{O}_K$, $\mathcal{O}_K^\times = U_K^0$ the group of units in $\mathcal{O}_K$ and $\mathbb{F}_K = \mathcal{O}_K/\mathfrak{m}_K$ the finite residue field.

Acknowledgments. This work was supported by KAKENHI 25800019. The author would like to thank the referee for pointing out mistakes of the proof of Theorem 3.6 in an earlier version of this article.

2. Mackey functors

Throughout this section, let k be a field of characteristic 0.

Mackey products

Definition 2.1. A *Mackey functor* A over k is a contravariant functor from the category of étale schemes over k to that of abelian groups equipped with a covariant structure for finite morphisms such that $A(X_1 \sqcup X_2) = A(X_1) \oplus A(X_2)$ and if

$$\begin{tikzcd} X' \arrow[r, "g'"] \arrow[d, "f'"'] & X \arrow[d, "f"] \\ Y' \arrow[r, "g"] & Y \end{tikzcd}$$

is a Cartesian diagram, then the induced diagram

$$\begin{tikzcd} A(X') \arrow[r, "{g'}_*"] & A(X) \\ A(Y') \arrow[r, "g_*"] \arrow[u, "{f'}^*"] & A(Y) \arrow[u, "f^*"'] \end{tikzcd}$$

commutes.

For a Mackey functor A, we denote by $A(K)$ its value $A(\mathrm{Spec}(K))$ for a field extension K over k.

Definition 2.2. For Mackey functors $A_1, \dots, A_q$, their *Mackey product* $A_1 \otimes \cdots \otimes A_q$ is defined as follows: For any finite field extension K/k,

$$(A_1 \otimes \cdots \otimes A_q)(K) := \left(\bigoplus_{L/K\colon \text{finite}} A_1(L) \otimes \cdots \otimes A_q(L) \right) / R,$$

where R is the subgroup generated by elements of the following form:

(PF) For any finite field extensions $K \subset K_1 \subset K_2$, and if $x_{i_0} \in A_{i_0}(K_2)$ and $x_i \in A_i(K_1)$ for all $i \neq i_0$, then

$$j^*(x_1) \otimes \cdots \otimes x_{i_0} \otimes \cdots \otimes j^*(x_q) - x_1 \otimes \cdots \otimes j_*(x_{i_0}) \otimes \cdots \otimes x_q,$$

where $j = j_{K_2/K_1} : \operatorname{Spec}(K_2) \to \operatorname{Spec}(K_1)$ is the canonical map.

This product gives a monoidal structure in the abelian category of Mackey functors with unit $\mathbb{Z} : k' \mapsto \mathbb{Z}$. We write $\{x_1, \dots, x_q\}_{K/k}$ for the image of $x_1 \otimes \cdots \otimes x_q \in A_1(K) \otimes \cdots \otimes A_q(K)$ in the product $(A_1 \otimes \cdots \otimes A_q)(k)$. For any field extension K/k, the canonical map $j = j_{K/k} : k \hookrightarrow K$ induces the pull-back

$$\operatorname{Res}_{K/k} := j^* : (A_1 \otimes \cdots \otimes A_q)(k) \longrightarrow (A_1 \otimes \cdots \otimes A_q)(K)$$

which is called the *restriction map*. If the extension K/k is finite, then the push-forward

$$N_{K/k} := j_* : (A_1 \otimes \cdots \otimes A_q)(K) \longrightarrow (A_1 \otimes \cdots \otimes A_q)(k)$$

is given by $N_{K/k}(\{x_1, \dots, x_q\}_{L/K}) = \{x_1, \dots, x_q\}_{L/k}$ on symbols and is called the *norm map*.

Let $G_1, \dots, G_q$ be semi-abelian varieties over k. These form a Mackey functor by $K \mapsto G_i(K)$. The *Somekawa K-group* $K(k; G_1, \dots, G_q)$ attached to $G_1, \dots, G_q$ is defined by a quotient of $(G_1 \otimes \cdots \otimes G_q)(k)$ by the subgroup which produces "the Weil reciprocity law" (see for the precise definition, [13]).

Galois symbol map

For any positive integer m, we consider the isogeny $m : G_i \to G_i$ induced from the multiplication by m. The exact sequence

$$0 \to G_i[m] \to G_i(\overline{k}) \xrightarrow{m} G_i(\overline{k}) \to 0$$

of Galois modules gives an injection of Mackey functors

$$G_i/m \hookrightarrow H^1(-, G_i[m]),$$

where $G_i/m := \operatorname{Coker}(m)$ (in the category of Mackey functors) and $H^1(-, G_i[m])$ is also the Mackey functor given by $K \mapsto H^1(K, G_i[m])$. The cup products and the corestriction on the Galois cohomology groups give

$$G_1/m \otimes \cdots \otimes G_q/m \to H^q(-, G_1[m] \otimes \cdots \otimes G_q[m]). \tag{2}$$

This map factors through $K(-;G_1,\dots,G_q)/m$ ([13], Prop. 1.5). The induced homomorphism

$$K(k;G_1,\dots,G_q)/m \to H^q(k, G_1[m]\otimes\cdots\otimes G_q[m])$$

is called the *Galois symbol map*.

3. Higher unit groups

Throughout this section, we fix a finite field extension k of $\mathbb{Q}_p$ and *assume* that it contains $\mu_p := \mathbb{G}_m[p]$ the group of all p-th roots of unity.

Mackey functor defined by higher unit groups

Let K be a finite field extension of k and put $e_0(K) := v_K(p)/(p-1)$. The unit group $U_K^0 = \mathcal{O}_K^\times$ and the higher unit groups $U_K^i := 1+\mathfrak{m}_K^i$ $(i \geqslant 1)$ induce a filtration $\{\overline{U}_K^i\}_{i\geqslant 0}$ of $K^\times/p$ which is given by

$$\overline{U}_K^i := \mathrm{Im}(U_K^i \hookrightarrow K^\times \twoheadrightarrow K^\times/p).$$

By abuse of notation, we still use $a \in \overline{U}_K^i$ for the residue class represented by a unit $a \in U_K^i$.

Lemma 3.1 (cf. [5], Lem. 2.1.3).

(a) *If* $0 \leqslant i < pe_0(K)$, *then*

$$\overline{U}_K^i/\overline{U}_K^{i+1} \simeq \begin{cases} \mathbb{F}_K, & \text{if } p \nmid i,\\ 1, & \text{if } p \mid i.\end{cases}$$

(b) *If* $i = pe_0(K)$, *then* $\overline{U}_K^{pe_0(K)}/\overline{U}_K^{pe_0(K)+1} \simeq \mathbb{Z}/p$.

(c) *If* $i > pe_0(K)$, *then* $\overline{U}_K^i = 1$.

Lemma 3.2 ([5], Lem. 2.1.5). *Let K be a finite field extension of k. For a positive integer i, and $a \in \overline{U}_K^i \smallsetminus \overline{U}_K^{i+1}$, we define an extension $L = K(\sqrt[p]{a})$ of K. For any $\sigma \in \mathrm{Gal}(L/K)$, put $i(\sigma) := v_L(\sigma(\varpi)-\varpi)$, where ϖ is a uniformizer of L.*

(a) *If $1 \leqslant i < pe_0(K)$ and $p \nmid m$ then L/K is a totally ramified extension of degree p and $i(\sigma) = pe_0(K) - i + 1$ for $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma \neq 1$.*

(b) *If $i = pe_0(K)$, then L/K is an unramified extension of degree p.*

For any integer $i \geqslant 0$, we define a sub Mackey functor $\overline{U}^i$ of $\mathbb{G}_m/p := \mathrm{Coker}(p : \mathbb{G}_m \to \mathbb{G}_m)$ over k by

$$\overline{U}^i(K) := \overline{U}_K^{ie(K/k)}$$

for a field extension K/k with ramification index $e(K/k)$. For a finite field extension L/K over k and $j = j_{L/K} : \mathrm{Spec}(L) \to \mathrm{Spec}(K)$, the covariant map $N_{L/K} :=$

$j_* : \overline{U}^i(L) \to \overline{U}^i(K)$ is given by the norm homomorphism $N_{L/K} : L^\times \to K^\times$. We also denote by $\mathrm{Res}_{L/K}$ the contravariant map j^*. The Galois symbol map (2) induces the following isomorphisms:

Lemma 3.3 ([9], Lem. 4.2.1). *For integers $i, j \geqslant 0$ with $i + j \geqslant 2$, we have*

$$(\overline{U}^0)^{\otimes i} \otimes (\mathbb{G}_m/p)^{\otimes j} \xrightarrow{\simeq} \begin{cases} H^2(-, \mu_p^{\otimes 2}), & \text{if } i + j = 2, \\ 0, & \text{otherwise.} \end{cases}$$

For integers $m, n \geqslant 0$, we define a map $h^{m,n} : \overline{U}^m \otimes \overline{U}^n \to H^2(-, \mu_p^{\otimes 2})$ of Mackey functors over k by the composition

$$h^{m,n} : \overline{U}^m \otimes \overline{U}^n \to \mathbb{G}_m/p \otimes \mathbb{G}_m/p \xrightarrow{\simeq} H^2(-, \mu_p^{\otimes 2}).$$

Here, the latter map is the Galois symbol map on $\mathbb{G}_m/p \otimes \mathbb{G}_m/p$ defined in (2) and is an isomorphism (Lem. 3.3). We also denote by

$$h^{-1,n} : \mathbb{G}_m/p \otimes \overline{U}^n \to \mathbb{G}_m/p \otimes \mathbb{G}_m/p \xrightarrow{\simeq} H^2(-, \mu_p^{\otimes 2})$$

by convention. For any finite field extension K/k, the map $h^{m,n}$ induces $h_K^{m,n} : \left(\overline{U}^m \otimes \overline{U}^n\right)(K) \to H^2(K, \mu_p^{\otimes 2})$.

As noted in (2), the Galois symbol map

$$h : (\mathbb{G}_m/p \otimes \mathbb{G}_m/p)(k) \to H^2(k, \mu_p^{\otimes 2})$$

is given by $h(\{a, b\}_{K/k}) = \mathrm{Cor}_{K/k}(h^1(a) \cup h^1(b))$ for a symbol $\{a, b\}_{K/k} \in (\mathbb{G}_m/p \otimes \mathbb{G}_m/p)(k)$, where $h^1 : \mathbb{G}_m/p(K) \to H^1(K, \mu_p)$ is the Kummer map. The corestriction $\mathrm{Cor}_{K/k}$ is bijective (e.g., [8], Lem. 5.8). The cup product $\cup : H^1(K, \mu_p) \otimes H^1(K, \mu_p) \to H^2(K, \mu_p^{\otimes 2})$ on the Galois cohomology groups is characterized by the Hilbert symbol $(\ ,\ )_K : K^\times/p \otimes K^\times/p \to \mu_p$ as in the following commutative diagram (cf. [11], Chap. XIV):

$$\begin{tikzcd} H^1(K, \mu_p) \otimes H^1(K, \mu_p) \arrow[r, "\cup"] & H^2(K, \mu_p^{\otimes 2}) \arrow[d, "\simeq"] \\ K^\times/p \otimes K^\times/p \arrow[u, "\simeq"] \arrow[r, "(\ ,\ )_K"] & \mu_p \end{tikzcd} \quad . \tag{3}$$

The image in $H^2(K, \mu_p^{\otimes 2})$ by the Hilbert symbol are calculated as follows (cf. [3], Lem. 3.1):

Lemma 3.4. *Let m, n be integers $\geqslant 0$.*

(i)

$$\#(K^\times/p, \overline{U}_K^n)_K = \begin{cases} p, & \text{if } n \leqslant pe_0(K), \\ 0, & \text{otherwise.} \end{cases}$$

(ii) *If $p \nmid m$ or $p \nmid n$, then*

$$\#(\overline{U}_K^m, \overline{U}_K^n)_K = \begin{cases} p, & \text{if } m+n \leqslant pe_0(K), \\ 0, & \text{otherwise}. \end{cases}$$

(iii) *If $p \mid m$ and $p \mid n$, then*

$$\#(\overline{U}_K^m, \overline{U}_K^n)_K = \begin{cases} p, & \text{if } m+n < pe_0(K), \\ 0, & \text{otherwise}. \end{cases}$$

Let π be a uniformizer of K. Since $\overline{U}_K^{pe_0(K)} \simeq \mathbb{Z}/p$ (Lem. 3.1), one can find a unit $\rho \in \mathcal{O}_K^\times$ such that $1+\rho\pi^{pe_0(K)}$ is a generator of $\overline{U}_K^{pe_0(K)}$. It is known that the Hilbert symbol $(\pi, 1+\rho\pi^{pe_0(K)})_K$ is a generator of $H^2(K, \mu_p^{\otimes 2})$ (e.g., [7], Cor. A.12).

Lemma 3.5.

(i) *Let i, j be positive integers with $i+j = pe_0(K)$. Assume $i \nmid p$. Then, for any unit $u \in \mathcal{O}_K^\times$, there exists $v \in \mathcal{O}_K^\times$ such that $(1+u\pi^i, 1+v\pi^j)_K \neq 0$.*

(ii) *Let i be an integer which is prime to p with $0 < i < pe_0(K)$. Then, there exists $u \in \mathcal{O}_K^\times$ such that $(1+u\pi^i, \pi)_K \neq 0$.*

(iii) *Let i, j be positive integers. Assume $p \nmid i$, $p \nmid (i+j)$, $i+j < pe_0(K)$, and $i+2j > pe_0(K)$. Then, for any $\eta \in \mu_{q-1} \subset \mathcal{O}_K^\times$ there exists $v \in \mathcal{O}_K^\times$ such that $(1+\eta\pi^i, 1+v\pi^j)_K \neq 0$, where $q = \#\mathbb{F}_K$.*

Proof. (i) As in [1], Lemma 4.1, we have the following equalities:

$$\begin{aligned}
&(1+u\pi^i, 1+\rho u^{-1}\pi^j)_K \\
&\quad = (1+u\pi^i(1+\rho u^{-1}\pi^j), 1+\rho u^{-1}\pi^j)_K \quad \text{(by Lem. 3.4)} \\
&\quad = -(1+u\pi^i(1+\rho u^{-1}\pi^j), -u\pi^i)_K \\
&\quad = -(1+\tfrac{\rho}{1+u\pi^i}\pi^{pe_0(K)}, -u\pi^i)_K \quad \text{(from the Steinberg relation)} \\
&\quad = -(1+\rho\pi^{pe_0(K)}, -u\pi^i)_K \quad (\text{by } 1+\rho\pi^{pe_0(K)} = 1+\tfrac{\rho}{1+u\pi^i}\pi^{pe_0(K)} \text{ in } \overline{U}_K^{pe_0(K)}) \\
&\quad = -i(1+\rho\pi^{pe_0(K)}, \pi)_K \quad \text{(by Lem. 3.4)} \\
&\quad = i(\pi, 1+\rho\pi^{pe_0(K)})_K.
\end{aligned}$$

This implies $(1+u\pi^i, 1+\rho u^{-1}\pi^j)_K \neq 0$ because of $p \nmid i$.

(ii) Since $((1-\pi^i)^i, \pi)_K = (1-\pi^i, \pi^i)_K = 0$, we have

$$\begin{aligned}
(1+\rho\pi^{pe_0(K)}, \pi)_K &= (1+\rho\pi^{pe_0(K)}, \pi)_K + ((1-\pi^i)^i, \pi)_K \\
&= ((1+\rho\pi^{pe_0(K)})(1-\pi^i)^i, \pi)_K.
\end{aligned}$$

The unit $(1+\rho\pi^{pe_0(K)})(1-\pi^i)^i \in U_K^i \setminus U_K^{i+1}$ gives the required unit u.

(iii) From (ii), there exists $u \in \mathcal{O}_K^\times$ such that $(1 + u\pi^{i+j}, \pi)_K \neq 0$. Put $v = (1+\eta\pi^i)u\eta^{-1} \in \mathcal{O}_K^\times$. The calculations of symbols as in (i) we have

$$
\begin{aligned}
&(1+\eta\pi^i, 1+v\pi^j)_K \\
&\qquad = (1+\eta\pi^i(1+v\pi^j), 1+v\pi^j)_K \quad \text{(by } i+2j > pe_0(K) \text{ and Lem. 3.4)} \\
&\qquad = -(1+\eta\pi^i(1+v\pi^j), -\eta\pi^i)_K \\
&\qquad = -i(1+u\pi^{i+j}, \pi)_K \neq 0.
\end{aligned}
$$

∎

Mackey products of higher unit groups

The rest of this section is devoted to show the following theorem.

Theorem 3.6. *Put $e_0 := e_0(k)$. Let n be an integer $\geqslant 0$ with $p \mid n$.*

(i) *The map $h^{-1,n}$ induces an isomorphism*

$$\mathbb{G}_m/p \otimes \overline{U}^n \xrightarrow{\simeq} \begin{cases} H^2(-, \mu_p^{\otimes 2}), & \text{if } n \leqslant pe_0, \\ 0, & \text{otherwise.} \end{cases}$$

(ii) *For $m = 0$ or pe_0, the map $h^{m,n}$ induces an isomorphism*

$$\overline{U}^m \otimes \overline{U}^n \xrightarrow{\simeq} \begin{cases} H^2(-, \mu_p^{\otimes 2}), & \text{if } m+n < pe_0, \\ 0, & \text{otherwise.} \end{cases}$$

Let n be a *positive* integer with $p \mid n$ and K/k a finite field extension with ramification index $e := e(K/k)$. From now on, we investigate the Galois symbol map

$$h := h_K^{0,n} : \left(\overline{U}^0 \otimes \overline{U}^n\right)(K) \to H^2(K, \mu_p^{\otimes 2}).$$

We basically follow the proof of Lemma 4.2.1 in [9] and proceed the steps below to show the injectivity of h:

Step 1. For any symbol of the form $\{a,b\}_{K/K} \in \left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$, if $h(\{a,b\}_{K/K}) = 0$ then $\{a,b\}_{K/K} = 0$. (Prop. 3.7)

Step 2. The map h is injective on the subgroup of $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ generated by symbols of the form $\{a,b\}_{K/K}$. (Prop. 3.10)

Step 3. $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ is generated by symbols of the form $\{a,b\}_{K/K}$. (Prop. 3.11)

Proposition 3.7.

(i) *For any symbol $\{a,b\}_{K/K}$ in $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$, if $h(\{a,b\}_{K/K}) = 0$, then we have $\{a,b\}_{K/K} = 0$.*

(ii) *For symbols of the form $\{a,b\}_{K/K}, \{a',b\}_{K/K}$ in $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ with $h(\{a,b\}_{K/K}) = h(\{a',b\}_{K/K})$, we have $\{a,b\}_{K/K} = \{a',b\}_{K/K}$.*

Proof. (i) Take a symbol $\{a,b\}_{K/K}$ in $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ and assume $h(\{a,b\}_{K/K}) = 0$. The symbol map is written by the Hilbert symbol $h(\{a,b\}_{K/K}) = (a,b)_K$ as in (3) and thus a is in the image of the norm $N_{L/K} : \overline{U}^0_L \to \overline{U}^0_K$ for $L = K(\sqrt[p]{b})$ ([2], Chap. IV, Prop. 5.1). Take $\alpha \in \overline{U}^0_L$ such that $N_{L/K}(\alpha) = a$. We obtain

$$\{a,b\}_{K/K} = \{N_{L/K}(\alpha), b\}_{K/K} = \{\alpha, \mathrm{Res}_{L/K}(b)\}_{L/K} = 0$$

by the condition (PF) in the definition of the Mackey product (Def. 2.2).

(ii) Suppose $h(\{a,b\}_{K/K}) = h(\{a',b\}_{K/K})$ and thus $h(\{a(a')^{-1},b\}_{K/K}) = 0$. From (i) we obtain $\{a(a')^{-1},b\}_{K/K} = 0$. Therefore we get $\{a,b\}_{K/K} = \{a',b\}_{K/K}$. ∎

Now we *assume* $n < pe_0$ and introduce subgroups $S(K)$ and $T(K)$ of $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ as follows:

$S(K) :=$ subgroup generated by symbols of the form $\{a,b\}_{K/K}$ in $\left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$,

$T(K) :=$ subgroup generated by symbols $\{a,b\}_{K/K} \in S(K)$ for $a \in \overline{U}^{pe_0(K)-ne-1}_K$.

Lemma 3.8. *Using the above notation, we have $S(K) = T(K)$.*

Proof. Define a filtration of $S(K)$ by

$$S^i(K) := \text{subgroup generated by symbols } \{a,b\}_{K/K} \in S(K) \text{ for } a \in \overline{U}^i_K.$$

By the very definition, we have $S(K) = S^0(K)$ and $T(K) = S^{pe_0(K)-ne-1}(K)$. It is enough to show $S^i(K) = S^{i+1}(K)$ for i with $0 \leqslant i < pe_0(K) - ne - 1$.

Fix a uniformizer π of K. Take a symbol $\xi = \{1+u\pi^s, 1+v\pi^t\}_{K/K} \in S^i(K)$ with $u,v \in \mathcal{O}_K^\times$, $s \geqslant i, t \geqslant ne$. To show $\xi \in S^{i+1}(K)$ we may assume $s = i$. We may also assume s and t are prime to p (Lemma 3.1) and $s+t \leqslant pe_0(K)$ (Lem. 3.4 and Lem. 3.7). From Proposition 3.7, Lemma 3.5(i) and Lemma 3.4 we have the following equalities:

$$\begin{aligned}
\xi &= \{1+u\pi^i, 1+v\pi^t\}_{K/K} \\
&= c\{1+u\pi^i, 1+v'\pi^{pe_0(K)-i}\}_{K/K} \quad (\text{for some } c \text{ and } v' \in \mathcal{O}_K^\times) \\
&= c\{1+\eta\pi^i, 1+v'\pi^{pe_0(K)-i}\}_{K/K} \quad (\text{for } u = \eta u_1 \in \mathcal{O}_K^\times \\
&\qquad\qquad \text{with } \eta \in \mu_{q-1}(K) \text{ and } u_1 \in U_K^1),
\end{aligned}$$

where $q := \#\mathbb{F}_K$. Since $i = s$ is prime to p and we have inequalities

$$i + 2(pe_0(K) - i - 1) > pe_0(K) + ne - 1 \geqslant pe_0(K) + p - 1$$

(recall $p \mid n$ and $n > 0$), one can apply Lemma 3.5(iii) so that there exists a non-zero symbol $\{1+\eta\pi^i, 1+v''\pi^{pe_0(K)-i-1}\}_{K/K}$ for some unit $v'' \in \mathcal{O}_K^\times$. From

Proposition 3.7(ii) we have

$$\{1+\eta\pi^i, 1+v'\pi^{pe_0(K)-i}\}_{K/K} = c'\{1+\eta\pi^i, 1+v''\pi^{pe_0(K)-i-1}\}_{K/K} \quad (\text{for some } c' \in \mathbb{Z}).$$

Now we suppose $p \nmid i+1$. From Proposition 3.5(i) again we have

$$\{1+\eta\pi^i, 1+v''\pi^{pe_0(K)-i-1}\}_{K/K} = c''\{1+u'\pi^{i+1}, 1+v''\pi^{pe_0(K)-i-1}\}_{K/K} \quad (\text{for some } u' \in \mathcal{O}_K^\times \text{ and some } c'').$$

Thus $\xi \in S^{i+1}(K)$. In the case of $p \mid i+1$, we have $\overline{U}_K^{pe_0(K)-(i+1)} = \overline{U}_K^{pe_0(K)-(i+2)}$ (Lem. 3.1). Therefore, the same computations as above give

$$\begin{aligned}\{1+\eta\pi^i, 1+v''\pi^{pe_0(K)-i-1}\}_{K/K} &= \{1+\eta\pi^i, 1+v'''\pi^{pe_0(K)-i-2}\}_{K/K} \quad (\text{for some } v''' \in \mathcal{O}_K^\times)\\ &= c''\{1+u'\pi^{i+2}, 1+v'''\pi^{pe_0(K)-i-2}\}_{K/K} \quad (\text{for some } u' \in \mathcal{O}_K^\times \text{ and some } c'').\end{aligned}$$

Hence we obtain $S^i(K) = S^{i+1}(K)$. ■

Define a bilinear map of $\mathbb{F}_p$-vector spaces

$$\Phi : \mathbb{F}_K \times \mathbb{F}_K \to S(K); (a,b) \mapsto \{1+\widetilde{a}\pi^{pe_0(K)-ne-1}, 1+\widetilde{b}\pi^{ne+1}\}_{K/K},$$

where $\widetilde{a}, \widetilde{b} \in \mathcal{O}_K$ are lifts of a, b respectively. The map Φ is well-defined (Lem. 3.4, Prop. 3.7(i)). Take a non-zero single symbol $\{a,b\}_{K/K} \in T(K)$ with $a \in \overline{U}_K^{pe_0(K)-ne-1}, b \in \overline{U}_K^{ne+1} = \overline{U}^n(K)$. If $a \in \overline{U}_K^{pe_0(K)-ne}$ or $b \in \overline{U}_K^{ne+2}$, then $(a,b)_K = 0$ (Lem. 3.4) and this contradicts with $\{a,b\}_{K/K} \neq 0$ by Lemma 3.7(i). Thus $a \in \overline{U}_K^{pe_0(K)-ne-1} \smallsetminus \overline{U}_K^{pe_0(K)-ne}, b \in \overline{U}_K^{ne+1} \smallsetminus \overline{U}_K^{ne+2}$ and there exist $\overline{a}, \overline{b} \in \mathbb{F}_K$ such that $\{a,b\}_{K/K} = \Phi(\overline{a}, \overline{b})$. From Lemma 3.8, any single symbol in $S(K)$ can be written as $\Phi(a,b)$ for some $a, b \in \mathbb{F}_K$ so that any non-zero element in $S(K)$, that is, a finite sum of symbols, can be written as $\sum_i \Phi(a_i, b_i)$ for some $a_i, b_i \in \mathbb{F}_K$. We also define

$$\Psi := h \circ \Phi : \mathbb{F}_K \times \mathbb{F}_K \to H^2(K, \mu_p^{\otimes 2}).$$

Lemma 3.9. *If $\Psi(a,b) = \Psi(c,d)$ for $a,b,c,d \in \mathbb{F}_K$, then $\Phi(a,b) = \Phi(c,d)$.*

Proof. Put $\alpha = \Psi(a,b) = \Psi(c,d)$ and we may assume $\alpha \neq 0$ by Proposition 3.7(i).

If $\{b,d\} \subset \mathbb{F}_K$ are linearly dependent in $\mathbb{F}_K$ (as an $\mathbb{F}_p$-vector space), then $sb = d$ for some $s \in \mathbb{F}_p$ ($s \neq 0$). From $\Psi(a,b) = \Psi(c,d) = s\Psi(c,b) = \Psi(sc,b)$, we have $\Phi(a,b) = \Phi(sc,b) = \Phi(c,d)$ by Proposition 3.7(ii).

When $\{b,d\} \subset \mathbb{F}_K$ are linearly independent, we define non-zero homomorphisms $\psi_b, \psi_d : \mathbb{F}_K \to H^2(K, \mu_p^{\otimes 2})$ by $\psi_b(x) = \Psi(x,b), \psi_d(x) = \Psi(x,d)$. These are linearly independent. In fact, if we assume $\psi_b = s\psi_d$ for some constant s then, for any $x \in \mathbb{F}_K$, $\psi_b(x) = s\psi_d(x)$ and thus $\Psi(x, b-sd) = 0$. Take a generator

$1+\rho\pi^{pe_0(K)} \in \overline{U}_K^{pe_0(K)}$ with $\rho \in \mathcal{O}_K^\times$ and denote the reduction of ρ to $\mathbb{F}_K$ by $r \in \mathbb{F}_K$. Since $u := b - sd \neq 0$, the calculations of symbols as in the proof of Lemma 3.5(i) give

$$0 = \Psi(ru^{-1}, u) = (1+\rho\widetilde{u}^{-1}\pi^{pe_0(K)-ne-1}, 1+\widetilde{u}\pi^{ne+1})_K = (1+\rho\pi^{pe_0(K)}, \pi)_K.$$

This contradicts with $(1+\rho\pi^{pe_0(K)}, \pi)_K \neq 0$. Thus ψ_b and ψ_d are linearly independent. One can find $x \in \mathbb{F}_K$ such that $\psi_b(x) = \psi_d(x) = \alpha$. Putting $y := d$, we have

$$\alpha = \Psi(a,b) = \Psi(x,b) = \Psi(x,y) = \Psi(c,y) = \Psi(c,d).$$

From these equalities and Proposition 3.7(i), we obtain

$$\Phi(a,b) - \Phi(c,d) = \Phi(a-x,b) + \Phi(x,b-y) + \Phi(x-c,y) + \Phi(c,y-d) = 0. \quad \blacksquare$$

Proposition 3.10. *Let K be a finite field extension of k, and n an integer with $p \mid n$ and $0 < n < pe_0(K)$. Then, the Galois symbol map h is injective on $S(K)$.*

Proof. Take a non-zero symbol $\Phi(a_0, b_0) \in S(K)$. By Proposition 3.7(i), it is enough to show that $S(K)$ is generated by the symbol $\Phi(a_0,b_0)$. Since $\Psi(a_0,b_0)$ is a generator of $H^2(K, \mu_p^{\otimes 2})$, for any non-zero element $\xi = \sum_{i=1}^n \Phi(a_i,b_i) \in S(K)$, there exists c_i such that $\Psi(a_i,b_i) = c_i\Psi(a_0,b_0)$ for each i. By Lemma 3.9, $\Phi(a_i,b_i) = \Phi(c_ia_0,b_0) = c_i\Phi(a_0,b_0)$ for all i and hence $\xi = (\sum_{i=1}^n c_i)\Phi(a_0,b_0)$. $\blacksquare$

Proposition 3.11. *Let K be a finite field extension of k, and n an integer with $p \mid n$ and $0 < n < pe_0(K)$. Then, we have $S(K) = \left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$.*

Proof. Take a symbol $\{a,b\}_{L/K} \in \left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ and we have to prove that the symbol $\{a,b\}_{L/K}$ is in $S(K)$.

(a) Reduce to the case of a Galois extension L/K: First we assume that this claim holds for all Galois extensions, namely, for any finite extension K/k and any symbol $\{a',b'\}_{K'/K} \in \left(\overline{U}^0 \otimes \overline{U}^n\right)(K)$ where K'/K is a finite Galois extension, we have $\{a',b'\}_{K'/K} \in S(K)$.

Let M be the Galois closure of L/K. The Galois symbol maps are compatible with norm maps as in the following commutative diagram:

$$\begin{array}{ccc}
\left(\overline{U}^0 \otimes \overline{U}^n\right)(M) & \xrightarrow{h_M^{0,n}} & H^2(M, \mu_p^{\otimes 2}) \\
{\scriptstyle N_{M/L}}\downarrow & & \downarrow{\scriptstyle \mathrm{Cor}_{M/L}} \\
\left(\overline{U}^0 \otimes \overline{U}^n\right)(L) & \xrightarrow{h_L^{0,n}} & H^2(L, \mu_p^{\otimes 2}).
\end{array}$$

Since the corestriction map $\mathrm{Cor}_{M/L} : H^2(M, \mu_p^{\otimes 2}) \to H^2(L, \mu_p^{\otimes 2})$ on the Galois cohomology groups is bijective ([8] Lem. 5.8) and the Galois symbol map $h_M^{0,n}$ are surjective (Lem. 3.4), one can find a symbol $\{\alpha, \beta\}_{M/M} \in S(M)$ such that

$$\begin{aligned} h_L^{0,n}(\{a, b\}_{L/L}) &= \mathrm{Cor}_{M/L} \circ h_M^{0,n}(\{\alpha, \beta\}_{M/M}) \\ &= h_L^{0,n} \circ N_{M/L}(\{\alpha, \beta\}_{M/M} = h_L^{0,n}(\{\alpha, \beta\}_{M/L}). \end{aligned}$$

Since M/L is Galois, $\{\alpha, \beta\}_{M/L} \in S(L)$ and thus $\{a, b\}_{L/L} = \{\alpha, \beta\}_{M/L}$ by Prop. 3.10. From the equalities

$$\{a, b\}_{L/K} = N_{L/K}(\{a, b\}_{L/L}) = N_{L/K}(\{\alpha, \beta\}_{M/L}) = \{\alpha, \beta\}_{M/K}$$

and the extension M/K is Galois, we obtain $\{a, b\}_{L/K} \in S(K)$. Therefore, without loss of generality, we may suppose L/K is a finite Galois extension and show $\{a, b\}_{L/K} \in S(K)$.

(b) *The case* $p \nmid e(L/K)$. In this extension, the norm map $N_{L/K} : \overline{U}_L^0 \to \overline{U}_K^0$ is surjective. There exist $\gamma \in \overline{U}_L^0$ and $d \in \overline{U}_K^{ne}$ such that $\{N_{L/K}(\gamma), d\}_{K/K}$ is a generator of $S(K)$. By the projection formula (PF), we have

$$\{N_{L/K}(\gamma), d\}_{K/K} = \{\gamma, \mathrm{Res}_{L/K}(d)\}_{L/K} = N_{L/K}(\{\gamma, \mathrm{Res}_{L/K}(d)\}_{L/L}).$$

Since the symbol $\{\gamma, \mathrm{Res}_{L/K}(d)\}_{L/L}$ is also a generator of $S(L)$, we obtain

$$\{a, b\}_{L/K} = N_{L/K}(\{a, b\}_{L/L}) = N_{L/K}(i\{\gamma, \mathrm{Res}_{L/K}(d)\}_{L/L}) = i\{N_{L/K}(\gamma), d\}_{K/K}$$

for some i. Hence $\{a, b\}_{L/K}$ is in $S(K)$.

(c) *The case* $p \mid e(L/K)$. By taking the maximal tamely ramified extension $K \subset K' \subset L$ in L/K, we have $\{a, b\}_{L/K} = N_{K'/K}(\{a, b\}_{L/K'})$. From the above arguments (b) again, we may assume that L/K is totally ramified Galois extension with $[L : K] = p^s$.

Take a finite sub extension K' of K_p/K, where K_p is the fixed field of the p-Sylow subgroup of G_k and put $L' = LK'$. As in (b), there exists $\alpha \in \overline{U}_{L'}^0$ such that $N_{L'/L}(\alpha) = a$. Therefore,

$$\begin{aligned} \{a, b\}_{L/K} &= \{N_{L'/L}(\alpha), b\}_{L/K} \\ &= \{\alpha, \mathrm{Res}_{L'/L}(b)\}_{L'/K} \\ &= N_{K'/K}\{\alpha, \mathrm{Res}_{L'/L}(b)\}_{L'/K'}. \end{aligned}$$

Choosing K' large enough, we may also assume $e(K/k) > 1$.

We prove $\{a, b\}_{L/K} \in S(K)$ for a finite extension K/k with $e(K/k) > 1$ and L/K is a totally ramified Galois extension with $[L : K] = p^s$ by induction on s.

If $s = 0$, there is nothing to show. So we assume $s > 0$. There exists an intermediate field M of L/K such that L/M is a cyclic extension of degree p. (The subfield M exists since the Galois group $\mathrm{Gal}(L/K)$ is solvable.) There exists an element $d \in \overline{U}^n(M) = \overline{U}_M^{ne(M/k)}$ such that $\Sigma = M(\sqrt[p]{d})$ is a totally ramified nontrivial extension of M and $\Sigma \neq L$. In fact, if the element d is in $\overline{U}_M^i \smallsetminus \overline{U}_M^{i+1}$

$(ne(M/k) < i < pe_0(M), p \nmid i)$ then the upper ramification subgroups of $G := \mathrm{Gal}(\Sigma/M)$ ([11], Chap. IV) is known to be

$$G = G^0 = G^1 = \cdots = G^{pe_0(M)-i} \supset G^{pe_0(M)-i+1} = \{1\}$$

(Lem. 3.2, see also [11], Chap. V, Sect. 3). Hence we can choose d such that the ramification break of Σ/M is different[1] from that of L/M. Using the element d, there exists $c \in \overline{U}^0_M$ such that $\{c, d\}_{M/M} \neq 0$. By local class field theory, we have $U^0_M = N_{L/M} U^0_L \cdot N_{\Sigma/M} U^0_\Sigma$. Therefore, one can find $\gamma \in U^0_L$ and $\gamma' \in U^0_\Sigma$ with $c = N_{K/M}(\gamma) N_{\Sigma/M}(\gamma')$. Since $\{N_{\Sigma/M}(\gamma'), d\}_{M/M} = \{\gamma', \mathrm{Res}_{\Sigma/M}(d)\}_{\Sigma/M} = 0$, we obtain

$$\begin{aligned}\{c, d\}_{M/M} &= \{N_{\Sigma/M}(\gamma'), d\}_{M/M} + \{N_{L/M}(\gamma), d\}_{M/M} \\ &= N_{L/M}(\{\gamma, \mathrm{Res}_{L/M}(d)\}_{L/L}).\end{aligned}$$

In particular, $\{\gamma, \mathrm{Res}_{L/M}(d)\}_{K/K} \neq 0$. Therefore, there exists i such that

$$\begin{aligned}\{a, b\}_{L/K} &= N_{L/K}(\{a, b\}_{L/L}) \\ &= N_{M/K} \circ N_{L/M}(\{\gamma^i, \mathrm{Res}_{L/M}(d)\}_{L/L}) \\ &= N_{M/K}(\{\gamma^i, \mathrm{Res}_{L/M}(d)\}_{L/M}) \\ &= N_{M/K}(\{N_{L/M}(\gamma^i), d\}_{M/M}) \\ &= \{N_{L/M}(\gamma^i), d\}_{M/K}.\end{aligned}$$

By the induction hypothesis, the last symbol $\{N_{L/M}(\gamma^i), d\}_{M/K}$ is in $S(K)$. ∎

Proof of Thm. 3.6. The proof of (i) is basically same as in (ii) and much easier so that we show the assertion (ii) only. For any finite extension K/k with ramification index e, we prove that the Galois symbol map gives isomorphisms

$$h := h^{m,n}_K : \left(\overline{U}^m \otimes \overline{U}^n\right)(K) \xrightarrow{\simeq} \begin{cases} H^2(K, \mu_p^{\otimes 2}), & \text{if } m + n < pe_0, \\ 0, & \text{otherwise.}\end{cases} \tag{4}$$

(a) The case $m = pe_0$: We show $\left(\overline{U}^{pe_0} \otimes \overline{U}^n\right)(K) = 0$. For any symbol $\{a, b\}_{L/K}$ in $\left(\overline{U}^{pe_0} \otimes \overline{U}^n\right)(K)$, we have $N_{L/K}(\{a, b\}_{L/L}) = \{a, b\}_{L/K}$. Thus it is enough to show $\{a, b\}_{K/K} = 0$ with $a \neq 1$. Since the extension $L = K(\sqrt[p]{a})$ is unramified and of degree p (Lem. 3.2), the norm map $N_{L/K} : \overline{U}^n(L) \to \overline{U}^n(K)$ is surjective ([11], Chap. V, Sect. 2, Prop. 3). By the projection formula (PF),

$$\{a, b\}_{K/K} = \{a, N_{L/K}(\beta)\}_{K/K} = \{\mathrm{Res}_{L/K}(a), \beta\}_{L/K} = 0$$

for some $\beta \in \overline{U}^n(L)$.

(b) The case $m = 0$ and $n \geqslant pe_0$: From the norm arguments, it is enough to show $\{a, b\}_{K/K} = 0$ for any symbol $\{a, b\}_{K/K} \in (\overline{U}^0 \otimes \overline{U}^n)(K)$. Since $e_0(K) = e_0 e$

and $\overline{U}^n(K) = \overline{U}_K^{ne}$, Lemma 3.4 implies $h(\{a,b\}_{K/K}) = 0$. The required assertion $\{a,b\}_{K/K} = 0$ follows from Proposition 3.7(i).

(c) The case $m = 0$ and $n < pe_0$: From Lemma 3.3, we may assume $n > 0$. Lemma 3.4(iii) implies that $h = h_K^{0,n}$ is surjective. Since h is injective on $S(K)$ (Prop. 3.10) and we have $S(K) = (\overline{U}^0 \otimes \overline{U}^n)(K)$ (Prop. 3.11), the symbol map h is injective. ∎

4. Galois symbol map for elliptic curves

Let k be a finite field extension of $\mathbb{Q}_p$ and put $e_0 = v_k(p)/(p-1)$ as in the last section.

Theorem 4.1. *Let n be an integer $\geqslant 1$. Let E_1, E_2 be elliptic curves over k with $E_i[p^n] \subset E_i(k)$ for $i = 1, 2$. Assume that E_1 has good ordinary reduction or split multiplicative reduction, and E_2 has good reduction or split multiplicative reduction. Then the Galois symbol map*

$$h_{p^n} : K(k; E_1, E_2)/p^n \to H^2(k, E_1[p^n] \otimes E_2[p^n])$$

is injective.

Proof. Consider the following diagram with exact rows:

$$\begin{array}{ccccc} K(k;E_1,E_2)/p^{n-1} & \longrightarrow & K(k;E_1,E_2)/p^n & \longrightarrow & K(k;E_1,E_2)/p \\ \downarrow{\scriptstyle h_{p^{n-1}}} & & \downarrow{\scriptstyle h_{p^n}} & & \downarrow{\scriptstyle h_p} \\ H^2(k, E_1[p^{n-1}] \otimes E_2[p^{n-1}]) & \longrightarrow & H^2(k, E_1[p^n] \otimes E_2[p^n]) & \longrightarrow & H^2(k, E_1[p] \otimes E_2[p]). \end{array}$$

The assumption $E_i[p^n] \subset E_i(k)$ implies the injectivity of the left lower map $H^2(k, E_1[p^{n-1}] \otimes E_2[p^{n-1}]) \to H^2(k, E_1[p^n] \otimes E_2[p^n])$. By induction on n, the assertion follows from the case of $n = 1$. More strongly we show that the Galois symbol map on the Mackey product

$$h : (E_1 \otimes E_2)(k)/p \to H^2(k, E_1[p] \otimes E_2[p])$$

is injective.

We recall the following results on the image of the Kummer map $h^1 : E(k) \to H^1(k, E[p])$ for an elliptic curve E over k ([5], see also [15], Rem. 3.2). Assume $E[p] \subset E(k)$ and choose an isomorphism of the Galois modules $E[p] \simeq (\mu_p)^{\oplus 2}$ which maps $E[p]^0$ onto the first factor μ_p, where $E[p]^0$ is the subgroup of $E[p]$ consisting of $\overline{k}$-valued points of the maximal connected finite flat p-torsion subgroup scheme of the Néron model of E. From the isomorphism, we can identify $H^1(k, E[p])$ and $(k^\times/p)^{\oplus 2}$. On the latter group $k^\times/p$, the higher unit groups $U_k^m = 1 + \mathfrak{m}_k^m$ induce a filtration $\overline{U}_k^m := \mathrm{Im}(U_k^m \to k^\times/p)$ as noted in the last section.

In terms of this filtration, the image of $h^1 : E(k)/p \hookrightarrow H^1(k, E[p]) = (k^\times/p)^{\oplus 2}$ is written precisely as follows (cf. [15]):

$$\mathrm{Im}(h^1) = \begin{cases} \overline{U}_k^{p(e_0-t_0)} \oplus \overline{U}_k^{pt_0}, & \text{if } E \text{ has good reduction,} \\ k^\times/p \oplus 1, & \text{if } E \text{ has split multiplicative reduction,} \end{cases} \tag{5}$$

where $t_0 := t_0(E) \in \mathbb{Z}$ with $0 < t_0 \leqslant e_0$ (It is calculated from the theory of the canonical subgroup of Katz-Lubin, cf. [3], Thm. 3.5).

Fix isomorphisms of Galois modules $E_1[p] \simeq \mu_p^{\oplus 2}$ and $E_2[p] \simeq \mu_p^{\oplus 2}$ as above. From the isomorphisms we can identify $H^1(-, E_1[p]) \simeq (\mathbb{G}_m/p)^{\oplus 2}$ and $H^1(-, E_2[p]) \simeq (\mathbb{G}_m/p)^{\oplus 2}$.

(a) E_1 *has split multiplicative reduction*: Consider the case that E_1 has split multiplicative reduction. We also assume that E_2 has good reduction. The other case on E_2 is treated in the same way and much easier. From (5), the Kummer maps on E_1 and E_2 induces isomorphisms

$$E_1/p \xrightarrow{\simeq} \mathbb{G}_m/p, \qquad E_2/p \xrightarrow{\simeq} \overline{U}^{p(e_0-t_0)} \oplus \overline{U}^{pt_0},$$

where $t_0 := t_0(E_2)$. Therefore $E_1/p \otimes E_2/p \simeq (\mathbb{G}_m/p \otimes \overline{U}^{p(e_0-t_0)}) \oplus (\mathbb{G}_m/p \otimes \overline{U}^{pt_0})$. The Galois symbol map h commutes with the maps $h^{-1,p(e_0-t_0)}$ and h^{-1,pt_0} defined in the last section and the injectivity of h follows from Theorem 3.6(i).

(b) E_1 *has good ordinary reduction*: Next we assume that E_1 has good ordinary reduction and E_2 has good reduction. In this case also, by (5), we have

$$E_1/p \xrightarrow{\simeq} \overline{U}^0 \oplus \overline{U}^{pe_0}, \qquad E_2/p \xrightarrow{\simeq} \overline{U}^{p(e_0-t_0)} \oplus \overline{U}^{pt_0},$$

where $t_0 := t_0(E_2)$. We have to show that the induced Galois symbol maps on

$$\overline{U}^0 \otimes \overline{U}^{p(e_0-t_0)}, \quad \overline{U}^0 \otimes \overline{U}^{pt_0}, \quad \overline{U}^{pe_0} \otimes \overline{U}^{p(e_0-t_0)}, \quad \text{and} \quad \overline{U}^{pe_0} \otimes \overline{U}^{p(e_0-t_0)}$$

are injective. This follows from Theorem 3.6(ii). ■

Proposition 4.2. *Let n be an integer $\geqslant 1$ and q an integer $\geqslant 3$. Let $E_1, \dots, E_q$ be elliptic curves over k. Assume that $E_i[p] \subset E_i(k)$ for $1 \leqslant i \leqslant 3$, E_1 has good ordinary reduction or split multiplicative reduction, and E_i has good reduction or split multiplicative reduction for $i = 2, 3$. Then, we have*

$$K(k; E_1, \dots, E_q)/p^n = 0.$$

Proof. By considering the exact sequence

$$(E_1 \otimes E_2 \otimes E_3)(k)/p^{n-1} \to (E_1 \otimes E_2 \otimes E_3)(k)/p^n \to (E_1 \otimes E_2 \otimes E_3)(k)/p,$$

it is enough to show $(E_1 \otimes E_2 \otimes E_3)(k)/p = 0$. We show only the case E_1 has good ordinary reduction and E_i has good reduction for each $i = 2, 3$. As in the above proof of Theorem 4.1, we have

$$E_1/p \xrightarrow{\simeq} \overline{U}^0 \oplus \overline{U}^{pe_0}, \qquad E_i/p \xrightarrow{\simeq} \overline{U}^{p(e_0-t_0(E_i))} \oplus \overline{U}^{pt_0(E_i)} \qquad (i = 2, 3),$$

By Theorem 3.6,

$$\overline{U}^0 \otimes \overline{U}^{p(e_0 - t_0(E_2))} \simeq \overline{U}^0 \otimes \overline{U}^{pt_0(E_2)} \simeq \mathbb{G}_m/p \otimes \mathbb{G}_m/p.$$

Hence the assertion follows from Lemma 3.3. ■

Remark 4.3. From the same arguments in the proof of Theorem 4.1, we obtain the injectivity of the Galois symbol map

$$h : K(k; \mathbb{G}_m, E)/p^n \to H^2(k, \mathbb{G}_m[p^n] \otimes E[p^n])$$

under the assumption $E[p^n] \subset E(k)$ for $n \geqslant 1$. As in [3] we can determine the image of the above h and have

$$K(k; \mathbb{G}_m, E)/p^n \simeq \begin{cases} \mathbb{Z}/p^n, & \text{if } E \text{ has multiplicative reduction,} \\ (\mathbb{Z}/p^n)^{\oplus 2}, & \text{if } E \text{ has good reduction.} \end{cases}$$

It is known that the Somekawa K-group $K(k; \mathbb{G}_m, E)$ is isomorphic to the homology group $V(E)$ of the complex

$$K_2(k(E)) \xrightarrow{\oplus \partial_P} \bigoplus_{P \in E:\text{ closed points}} k(P)^\times \xrightarrow{\sum N_{k(P)/k}} k^\times.$$

By the class field theory of curves over local field ([10], [20]), we have $V(E)/p^n \simeq \pi_1(E)^{\mathrm{ab,geo}}_{\mathrm{tor}}/p^n$. Therefore, the above computations give the structure of $\pi_1(E)^{\mathrm{ab}}$.

References

[1] S. Bloch and K. Kato, *p-adic étale cohomology*, Inst. Hautes Études Sci. Publ. Math. (1986), 107–152.

[2] I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions*, second ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, Providence, RI, 2002, With a foreword by I. R. Shafarevich.

[3] T. Hiranouchi and S. Hirayama, *On the cycle map for products of elliptic curves over a p-adic field*, Acta Arith. **157** (2013), no. 2, 101–118.

[4] B. Kahn, *Nullité de certains groupes attachés aux variétés semi-abéliennes sur un corps fini; application*, C. R. Acad. Sci. Paris Sér. I Math. **314** (1992), no. 13, 1039–1042.

[5] M. Kawachi, *Isogenies of degree p of elliptic curves over local fields and Kummer theory*, Tokyo J. Math. **25** (2002), 247–259.

[6] A. Mattuck, *Abelian varieties over p-adic ground fields*, Ann. of Math. (2) **62** (1955), 92–119.

[7] J. Milnor, *Introduction to algebraic K-theory*, Princeton University Press, Princeton, N.J., 1971, Annals of Mathematics Studies, No. 72.

[8] J. Murre and D. Ramakrishnan, *Local Galois symbols on $E \times E$*, Motives and algebraic cycles, Fields Inst. Commun., vol. 56, Amer. Math. Soc., Providence, RI, 2009, pp. 257–291.

[9] W. Raskind and M. Spiess, *Milnor K-groups and zero-cycles on products of curves over p-adic fields*, Compositio Math. **121** (2000), 1–33.
[10] S. Saito, *Class field theory for curves over local fields*, J. Number Theory **21** (1985), no. 1, 44–80.
[11] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.
[12] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
[13] M. Somekawa, *On Milnor K-groups attached to semi-abelian varieties*, K-Theory **4** (1990), no. 2, 105–119.
[14] M. Spiess and T. Yamazaki, *A counterexample to generalizations of the Milnor-Bloch-Kato conjecture*, J. K-Theory **4** (2009), no. 1, 77–90.
[15] T. Takemoto, *Zero-cycles on products of elliptic curves over p-adic fields*, Acta Arith. **149** (2011), no. 3, 201–214.
[16] J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274.
[17] C. Weibel, *The norm residue isomorphism theorem*, J. Topol. **2** (2009), 346–372.
[18] T. Yamazaki, *On Chow and Brauer groups of a product of Mumford curves*, Math. Ann. **333** (2005), 549–567.
[19] T. Yamazaki, *Milnor K-group attached to a torus and Birch-Tate conjecture*, Internat. J. Math. **20** (2009), no. 7, 841–857.
[20] T. Yoshida, *Finiteness theorems in the class field theory of varieties over local fields*, J. Number Theory **101** (2003), no. 1, 138–150.

Address: Toshiro Hiranouchi: Department of Mathematics, Graduate School of Science, Hiroshima University 1-3-1 Kagamiyama, Higashi-Hiroshima, 739-8526 Japan.

E-mail: hira@hiroshima-u.ac.jp

Received: 10 March 2015; **revised:** 19 August 2015