TOKYO J. MATH.
VOL. 32, NO. 1, 2009

# Construction of a Homomorphism Concerning Euler Systems for an Elliptic Curve

Rei OTSUKI

*Keio University*

(Communicated by H. Nakada)

## 0. Introduction

In the arithmetic of elliptic curves, the modular symbols, the modular elements by Mazur and Tate [8] and the Euler system of the zeta elements constructed by Kato [4] play important roles. These elements are defined for a modular elliptic curve and for cyclotomic fields, and they are all related to the values of the $L$-functions of the elliptic curve.

As the main result of this paper, we will construct a homomorphism which relates general Euler systems to general elements in the group rings, having the same property as the modular elements. This is a generalization of the result of the homomorphism which appeared in Kurihara [6] and was used to study the Selmer groups in the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. For an odd prime number $p$, he studied the relation between the zeta elements and the modular elements in the finite extension fields in the cyclotomic $\mathbf{Z}_p$-extension of the field $\mathbf{Q}$, and showed that the two elements correspond through a map which has a nice integral property.

In this paper, we will study the relation between the modular elements and the zeta elements in general. For an elliptic curve defined over $\mathbf{Q}$, we will construct a homomorphism from the cohomology group to the group ring of the Galois group for arbitrary cyclotomic fields and a good prime $p$. We define an admissible system as a system in group rings which satisfies the same formulas of the modular elements. We will prove that an Euler system corresponds to an admissible system through the homomorphism, and as a special case, the zeta element corresponds to the modular element. We will also prove that the homomorphism has a nice integral property in many cases. We can regard Kurihara's map as a special case of our map. Since our homomorphism is defined for a finite degree extension, we expect that this homomorphism would be useful to study the Selmer group of a number field of finite degree.

Let $E$ be an elliptic curve defined over $\mathbf{Q}$. In [6], he studied the structures of Selmer groups in the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$ for a good supersingular prime $p$, and defined

Received April 19, 2008; revised September 12, 2008

the homomorphism

$$\mathcal{P}_{\mathbf{Q}_n} : \mathrm{H}^1(\mathbf{Q}_{p,n}, T_pE) \to \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$$

for each positive integer $n$, where $\mathbf{Q}_{p,n}$ is the $n$-th layer of the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}_p$ and $\mathbf{Q}_n$ is the $n$-th layer of the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. Here, we adopted the notation $\mathcal{P}_{\mathbf{Q}_n}$ which is not used in [6]. In Kurihara-Pollack [7], the map is denoted by $\mathcal{P}_n$.

One of the most important properties of the homomorphism is that the image of Kato's zeta element under the homomorphism is the modular element of Mazur and Tate for each positive integer $n$. In other words, in the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$, the Euler system of Kato's zeta elements corresponds to the system of the modular elements through the homomorphisms. See Kurihara-Pollack [7] section 1.3 (1.3). The zeta elements and the modular elements are introduced in §3.

This map plays an important role in Iwasawa theory for elliptic curves, and is related to an important homomorphism $\mathrm{Col}^{\pm}$, which is defined by Kobayashi in [5]. He formulated the Iwasawa main conjecture for supersingular primes using the homomorphism $\mathrm{Col}^{\pm}$, and proved a partial result of the main conjecture using Kato's zeta elements. In section 1 of Kurihara-Pollack [7], $\mathrm{Col}^{\pm}$ is constructed from $\mathcal{P}_{\mathbf{Q}_n}$.

We first introduce two systems which are related to the main result of this paper.

For a positive integer $N$, let $z_N \in \mathrm{H}^1(\mathbf{Z}[\mu_N, \frac{1}{S}], V_pE)$ be the zeta element, and let $\mathcal{G}_N := \mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q})$. The system of the zeta elements $(z_N)_{N\geq 1}$ is an Euler system. In other words, they satisfy the formulas below

$$\mathrm{Nr}_{qN/N}(z_{qN}) = \begin{cases} z_N & (q|N) \\ F_q(\sigma_q^{-1})z_N & (q \nmid N)\,. \end{cases} \qquad (*)$$

Here, $q$ is a prime number, $\sigma_q \in \mathcal{G}_N$ is the $q$-th Frobenius map and $F_q(T) := 1 - \frac{a_q}{q}T + \frac{\varepsilon_q}{q}T^2 \in \mathbf{Q}[T]$, where $\varepsilon_q = 1$ (resp. 0) if $q$ is a good (resp. bad) prime and $a_q$ is the $q$-th coefficient of the normalized cusp form $\sum_{n=1}^{\infty} a_n q^n$ which corresponds to the elliptic curve $E$. In this paper, we also call the system of finite elements $(w_M)_{M|N}$ an Euler system if they satisfy the same formulas above.

For a positive integer $N$, let $\theta_N \in \mathbf{Q}[\mathcal{G}_N]$ be the modular element of Mazur and Tate. They satisfy the compatible formulas below

$$\pi_{qN/N}(\theta_{qN}) = \begin{cases} a_q\theta_N - \varepsilon_q \nu_{N/\frac{N}{q}}(\theta_{\frac{N}{q}}) & (q|N) \\ (a_q - \sigma_q - \varepsilon_q\sigma_q^{-1})\theta_N & (q \nmid N)\,. \end{cases}$$

Here, $\pi_{qN/N} : \mathbf{Q}[\mathcal{G}_{qN}] \to \mathbf{Q}[\mathcal{G}_N]$ is the natural restriction map and $\nu_{N/\frac{N}{q}} : \mathbf{Q}[\mathcal{G}_{\frac{N}{q}}] \to \mathbf{Q}[\mathcal{G}_N]$ is defined by $\sigma \mapsto \sum_{\tau\in\mathcal{G}_N, \pi_{N/\frac{N}{q}}(\tau)=\sigma} \tau$ for $\sigma \in \mathcal{G}_{\frac{N}{q}}$. In this paper, we call a system of (finite or infinite) elements of group rings an *admissible system*, when they satisfy the same compatible formulas. The system of the modular elements $(\theta_N)_{N\geq 1}$ is an admissible system.

In this paper, we will generalize Kurihara's result on the homomorphism $\mathcal{P}_{\mathbf{Q}_n}$. We will construct the homomorphism

$$\mathcal{P}_N : \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N), V_pE) \to \mathbf{Q}_p[\mathcal{G}_N]$$

for a good prime $p$ and for the cyclotomic field $\mathbf{Q}(\mu_N)$ with arbitrary positive integer $N$, not only in the case when $E$ is supersingular at $p$ and $N = p^n$, and prove that Euler systems correspond to the admissible systems by the homomorphisms $\mathcal{P}_N$. In particular, the zeta element corresponds to the modular element. From the definition of Euler systems, in the case in which Kurihara and Kobayashi studied, the system of the zeta elements $(z_{p^n})_{n\geq 1}$ was only a norm compatible system (see the upper half of the equation (*)), but we will study general relations between Euler systems. If $E$ is supersingular at $p$, "Kurihara's $\mathcal{P}_{\mathbf{Q}_n}$" above is induced from $\mathcal{P}_{p^{n+1}}$ in this paper.

We also note that our map is defined over local fields of finite degree over $\mathbf{Q}_p$, hence would be useful to study the Selmer group of a number field of finite degree. On the other hand, some important maps by Coleman [2] and Perrin-Riou [10] were defined over the cyclotomic $\mathbf{Z}_p$-extensions, namely extensions of infinite degree.

In the following sections, we will prove the following theorems. We fix a good prime $p$.

THEOREM 0.1 (Theorem 3.4). *If $(w_M)_M \in \prod_{M|N} \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_M), V_pE)$ is an Euler system, then $(\mathcal{P}_M(w_M))_M \in \prod_{M|N} \mathbf{Q}_p[\mathcal{G}_M]$ is an admissible system.*

THEOREM 0.2 (Theorem 3.6). *Let $z_N \in \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N), V_pE)$ be the zeta element, and let $\theta_N \in \mathbf{Q}_p[\mathcal{G}_N]$ be the modular element, then we have*

$$\mathcal{P}_N(z_N) = \theta_N .$$

THEOREM 0.3 (Theorem 4.1). *If $p$ divides $N$, $\widetilde{E}(\mathbf{F}_p(\mu_N))[p] = 0$ and $(w_M)_M$ is an integral Euler system, namely $(w_M)_M \in \prod_{M|N} \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_M), T_pE)$, then $(\mathcal{P}_M(w_M))_M$ is an integral admissible system, namely $(\mathcal{P}_M(w_M))_M \in \prod_{M|N} \mathbf{Z}_p[\mathcal{G}_M]$. Here $\widetilde{E}$ is the reduction of the elliptic curve $E$ mod $p$.*

The author expresses his sincere gratitude to professor Kurihara for his advice and encouragements, and is deeply indebted to professor Matsuno for reading the manuscript carefully and making helpful suggestions. He would also like to thank the referee for pointing out the simplification of some of the notations and proofs.

## 1. Notations

Let $E/\mathbf{Q}$ be an elliptic curve defined over the rational field. For a prime number $l$, we call $l$ a good prime if $E$ has good reduction at $l$, and call $l$ a bad prime if $E$ has bad reduction at $l$.

Here we introduce group rings of cyclic groups because they are important to define the homomorphism. For each integer $N \geq 1$, let $C_N$ be the abstract cyclic group of order $N$ with

generator $\xi_N$. If $M$ divides $N$, we regard $C_M \subset C_N$ and $\xi_M = \xi_N^{N/M}$. Choose a $N$-th root of unity $\zeta_N \in \overline{\mathbf{Q}}$ for each $N$ satisfying $\zeta_M = \zeta_N^{N/M}$ if $M$ divides $N$.

Define the ring homomorphism

$$\upsilon_N : \mathbf{Q}[C_N] \to \mathbf{Q}(\mu_N)$$

by $\xi_N \mapsto \zeta_N$.

If $L$ and $M$ are two natural numbers satisfying $(L, M) = 1$, we identify $\mathbf{Q}[C_{LM}]$ with $\mathbf{Q}[C_L][C_M]$ by $\xi_{LM}^M = \xi_L$ and $\xi_{LM}^L = \xi_M$, and define

$$\upsilon_{L,M} : \mathbf{Q}[C_{LM}] \to \mathbf{Q}(\mu_L)[C_M]$$

by $\xi_L \mapsto \zeta_L$ and $\xi_M \mapsto \xi_M$. The homomorphism $\upsilon_{L,M}$ is often denoted by $\upsilon_L$.

For an integer $a$ which is coprime to $L$, we define

$$\widehat{\sigma}_a : \mathbf{Q}(\mu_L)[C_M] \to \mathbf{Q}(\mu_L)[C_M]$$

by $\zeta_L \mapsto \zeta_L^a$ and $\xi_M \mapsto \xi_M^a$.

If $a$ is coprime to $LM$, then it is easy to show the diagram

$$\begin{array}{ccc} \mathbf{Q}(\mu_L)[C_M] & \xrightarrow{\hat{\sigma}_a} & \mathbf{Q}(\mu_L)[C_M] \\ \upsilon_M \downarrow & \circlearrowleft & \upsilon_M \downarrow \\ \mathbf{Q}(\mu_{LM}) & \xrightarrow{\sigma_a} & \mathbf{Q}(\mu_{LM}) \end{array}$$

is commutative. Here, $\sigma_a \in \mathrm{Gal}(\mathbf{Q}(\mu_{LM})/\mathbf{Q})$ is the unique element satisfying $\sigma_a(\zeta_{LM}) = \zeta_{LM}^a$.

If $L', L, M \geq 1$ are integers which satisfy $L|L'$ and $(L', M) = 1$, then it is easy to show that the diagram

$$\begin{array}{ccc} \mathbf{Q}(\mu_{L'})[C_M] & \xrightarrow{\mathrm{tr}_{L'/L}} & \mathbf{Q}(\mu_L)[C_M] \\ \upsilon_M \downarrow & \circlearrowleft & \upsilon_M \downarrow \\ \mathbf{Q}(\mu_{L'M}) & \xrightarrow{\mathrm{tr}_{L'M/LM}} & \mathbf{Q}(\mu_{LM}) \end{array}$$

is commutative. Here, $\mathrm{tr}_{L'/L}$ in the upper row only acts on the coefficients. It is easy to see that the trace maps $\mathrm{tr}_{L'/L}$ and $\mathrm{tr}_{L'M/LM}$ commute with $\widehat{\sigma}_a$ for each integer $a$ coprime to $L'$. In this paper, the trace map $\mathrm{tr}_{\mathbf{Q}(\mu_N)/\mathbf{Q}(\mu_M)}$ for the extension of cyclotomic fields $\mathbf{Q}(\mu_N)/\mathbf{Q}(\mu_M)$ is simply denoted by $\mathrm{tr}_{N/M}$.

LEMMA 1.1. *Let $l$ be a prime number, then each eigenvalue of $\widehat{\sigma}_l : \mathbf{Q}[C_N] \to \mathbf{Q}[C_N]$ is either a root of unity or 0.*

PROOF. Write $N = l^n M$ with $l \nmid M$ and let $r$ be the order of $l$ mod $M$ in the multiplicative group $(\mathbf{Z}/M\mathbf{Z})^\times$. Then we have $\widehat{\sigma}_l^n = \widehat{\sigma}_l^{n+r}$. Let $\rho$ be an eigenvalue of $\widehat{\sigma}_l$, then we have $\rho^n = \rho^{n+r}$, which implies that if $\rho \neq 0$, then $\rho$ is an $r$-th root of unity. □

DEFINITION 1.2. For a prime number $l$, we define the number $\varepsilon_l$ by

$$\varepsilon_l := \begin{cases} 1 & (l : \text{good}) \\ 0 & (l : \text{bad}), \end{cases}$$

and we define the polynomial $F_l(T) \in \mathbf{Q}[T]$ by

$$F_l(T) := 1 - \frac{a_l}{l}T + \frac{\varepsilon_l}{l}T^2 .$$

Here, $a_l$ is the $l$-th coefficient of the normalized cusp form $\sum_{n=1}^{\infty} a_n q^n$ which corresponds to the elliptic curve $E$.

PROPOSITION 1.3. *The inverse* $F_l(\widehat{\sigma}_l)^{-1}$ *exists in* $\mathrm{End}_{\mathbf{Q}}(\mathbf{Q}[C_N])$. *If* $l \not| N$, *then* $F_l(\sigma_l)^{-1}$ *exists in* $\mathrm{End}_{\mathbf{Q}}(\mathbf{Q}(\mu_N))$.

PROOF. Since $F_l(\widehat{\sigma}_l)$ is a $\mathbf{Q}$-linear map, it is enough to show that the map is injective.

If $l$ is a bad prime, then we have $F_l(\widehat{\sigma}_l) = 1 - \frac{a_l}{l}\widehat{\sigma}_l$. If there exists non-zero $x \in \mathbf{Q}[C_N]$ which satisfy $(1 - \frac{a_l}{l}\widehat{\sigma}_l)x = 0$, then 1 is an eigenvalue of $\frac{a_l}{l}\widehat{\sigma}_l$, but because of $|a_l| \leq 1$ and the previous lemma, the absolute value of an eigenvalue of $\frac{a_l}{l}\widehat{\sigma}_l$ is $\leq \frac{1}{l}$. Hence $1 - \frac{a_l}{l}\widehat{\sigma}_l$ is injective.

If $l$ is a good prime, then we have $F_l(\widehat{\sigma}_l) = 1 - \frac{a_l}{l}\widehat{\sigma}_l + \frac{1}{l}\widehat{\sigma}_l^2$. Let $\alpha, \beta \in \mathbf{C}$ be the two roots of $T^2 - a_l T + l = 0$. Then we have $1 - \frac{a_l}{l}\widehat{\sigma}_l + \frac{1}{l}\widehat{\sigma}_l^2 = (1 - \frac{\alpha}{l}\widehat{\sigma}_l)(1 - \frac{\beta}{l}\widehat{\sigma}_l)$. So by the similar argument as above, if the map is not injective, then $\frac{\alpha}{l}\widehat{\sigma}_l$ or $\frac{\beta}{l}\widehat{\sigma}_l$ has eigenvalue 1. But since we have $|\alpha| = |\beta| = \sqrt{l}$, this does not hold.

The latter is proved similarly. □

For a global or a local field $K$, we denote the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ by $G_K$ and for a $G_K$-module $B$, we denote the cohomology group $\mathrm{H}^1(G_K, B)$ by $\mathrm{H}^1(K, B)$. Let $F$ be an extension of $\mathbf{Q}$. For a $G_F$-module $B$, we denote $\prod_{v|p} \mathrm{H}^1(F_v, B)$ by $\mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, B)$. Here $v$ runs through all the primes of $F$ above $p$ and $F_v$ is the $v$-adic completion of $F$.

For an extension of $p$-adic fields $K'/K$ and $G_K$-module $B$, we denote the corestriction map $\mathrm{H}^1(G_{K'}, B) \to \mathrm{H}^1(G_K, B)$ by

$$\mathrm{Nr}_{K'/K} : \mathrm{H}^1(K', B) \to \mathrm{H}^1(K, B) .$$

For an extension of global fields $F'/F$ and $G_F$-module $B$, we denote the product of norm maps $\prod_{v|p} \sum_{w|v} \mathrm{Nr}_{F'_w/F_v} : \prod_{w|p} \mathrm{H}^1(F'_w, B) = \prod_{v|p} \prod_{w|v} \mathrm{H}^1(F'_w, B) \to \prod_{v|p} \mathrm{H}^1(F_v, B)$ by

$$\mathrm{Nr}_{F'/F} : \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F', B) \to \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, B) .$$

Here, $v$ runs through all the primes of $F$ above $p$ and $w$ runs through all the primes of $F'$ above $v$. For the extension of cyclotomic fields $\mathbf{Q}(\mu_N)/\mathbf{Q}(\mu_M)$ with $M|N$, the map $\mathrm{Nr}_{\mathbf{Q}(\mu_N)/\mathbf{Q}(\mu_M)}$ is simply denoted by $\mathrm{Nr}_{N/M}$.

## 2. Definition of the map

For the rest of the paper, we assume that $p$ is a good prime. Let $\mathcal{E}$ be an elliptic curve over $\mathbf{Z}_p$ whose generic fiber is $E$. We denote its special fiber by $\mathcal{E}_0$. Let $\mathcal{D} := \mathrm{H}^1_{cris}(\mathcal{E}_0/\mathbf{Z}_p)$ be the crystalline cohomology, then $\mathcal{D}$ is a free $\mathbf{Z}_p$-module of rank 2, and Frobenius automorphism $\Phi$ acts on $\mathcal{D}$. Define $D := \mathcal{D} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. We regard Néron differential $\omega = \omega_E$ as an element of $D$. Write $\varphi := \frac{\Phi}{p}$, then $\varphi^{-2} - a_p\varphi^{-1} + p = 0$. The cup product defines a non-degenerate alternating pairing $[\ ,\ ] : D \times D \to \mathbf{Q}_p$ such that $[\varphi(\omega), \omega] \neq 0$. We write $D^0 := \mathbf{Q}_p\omega \subset D$. Let $\omega^* \in D/D^0$ be the unique element satisfying $[\omega^*, \omega] = 1$. For an extension $K/\mathbf{Q}_p$, we can naturally extend the pairing $[\ ,\ ]$ to $[\ ,\ ] : D \otimes_{\mathbf{Q}_p} K \times D \otimes_{\mathbf{Q}_p} K \to K$ and for a number field $F$ we can define the pairing $[\ ,\ ] : D \otimes_{\mathbf{Q}} F \times D \otimes_{\mathbf{Q}} F \to \mathbf{Q}_p \otimes_{\mathbf{Q}} F$.

We introduce the dual exponential map, which was first defined by Bloch and Kato in [1]. The definition below is different from that in [1] but they coincide.

Let $K$ be a finite extension of $\mathbf{Q}_p$, $\mathcal{O}_K$ its ring of integers and $m_K$ its maximal ideal. Let $T_pE$ be the Tate module of $E$, i.e.

$$T_pE := \varprojlim E[p^n]$$

and $V_pE := T_pE \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Let $\widehat{E}$ be the formal group of the elliptic curve $E$. Let $\exp_{\hat{E}}$ be the exponential map of the formal group $\widehat{E}$. Then if $r \in \mathbf{N}$ is large enough, we can define $\mathbf{Z}_p$-linear map $\exp_{\hat{E},K} : m_K^r \to \widehat{E}(m_K^r)$. We consider the composite of the map

$$m_K^r \to \widehat{E}(m_K^r) \to \widehat{E}(m_K) \to E(K) \mathbin{\widehat{\otimes}} \mathbf{Z}_p \to \mathrm{H}^1(K, T_pE)$$

and it is denoted by $\exp_{E,m_K} : m_K^r \to \mathrm{H}^1(K, T_pE)$. Here, the first arrow is $\exp_{\hat{E}}$, the second arrow is the natural inclusion, the third arrow is the composite of the natural inclusion $\widehat{E}(m_K) \to E(K)$ and the induced map from $E(K) \to E(K) \otimes_{\mathbf{Z}} \mathbf{Z}/p^n\mathbf{Z}$, where

$$E(K) \mathbin{\widehat{\otimes}} \mathbf{Z}_p := \varprojlim E(K) \otimes_{\mathbf{Z}} \mathbf{Z}/p^n\mathbf{Z},$$

and the last arrow is the Kummer map.

By tensoring $\mathbf{Q}_p$, we can define the map

$$\exp_{E,K} : K \to \mathrm{H}^1(K, V_pE)$$

and define the map

$$\exp_K : D/D^0 \otimes_{\mathbf{Q}_p} K \to \mathrm{H}^1(K, V_pE)$$

by $\omega^* \otimes x \mapsto \exp_{\hat{E},K}(x)$.

The diagram below is commutative

$$\begin{array}{ccc} \widehat{E}(m_K) & \longrightarrow & \mathrm{H}^1(K, T_pE) \\ \downarrow \log & & \downarrow \\ D/D^0 \otimes_{\mathbf{Q}_p} K & \xrightarrow{\exp_K} & \mathrm{H}^1(K, V_pE)\,. \end{array}$$

Here, $\log : \widehat{E}(m_K) \to D/D^0 \otimes_{\mathbf{Q}_p} K$ is defined by $x \mapsto \omega^* \otimes \log_{\hat{E}}(x)$, where $\log_{\hat{E}} : \widehat{E}(m_K) \to K$ is the formal logarithm map of the formal group $\widehat{E}$.

The dual exponential map $\exp_K^* : \mathrm{H}^1(K, V_pE) \to D^0 \otimes_{\mathbf{Q}_p} K$ is a map which makes the following diagram commutative

$$\begin{array}{ccccc} \mathrm{H}^1(K, V_pE) & \times & \mathrm{H}^1(K, V_pE) & \to & \mathbf{Q}_p \\ \uparrow \exp_K & & \downarrow \exp_K^* & & \| \\ D/D^0 \otimes_{\mathbf{Q}_p} K & \times & D^0 \otimes_{\mathbf{Q}_p} K & \to & \mathbf{Q}_p . \end{array}$$

Here, the upper right arrow is the composite of the cup product and the corestriction map

$$\mathrm{H}^1(K, V_pE) \times \mathrm{H}^1(K, V_pE) \xrightarrow{\cup} \mathrm{H}^2(K, V_p\mu_{p^\infty}) \xrightarrow{\mathrm{Cor}} \mathrm{H}^2(\mathbf{Q}_p, V_p\mu_{p^\infty}) \cong \mathbf{Q}_p$$

and the lower right arrow is the composite

$$D/D^0 \otimes_{\mathbf{Q}_p} K \times D^0 \otimes_{\mathbf{Q}_p} K \xrightarrow{[\ ,\ ]} K \xrightarrow{\mathrm{tr}_{K/\mathbf{Q}_p}} \mathbf{Q}_p .$$

For a number field $F$ with $[F : \mathbf{Q}] < \infty$, we define $\exp_F : D/D^0 \otimes_{\mathbf{Q}} F \to \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, V_pE)$ to be the composite of the isomorphism

$$\begin{aligned} D/D^0 \otimes_{\mathbf{Q}} F &\cong D/D^0 \otimes_{\mathbf{Q}_p} (\mathbf{Q}_p \otimes_{\mathbf{Q}} F) \\ &\cong D/D^0 \otimes_{\mathbf{Q}_p} \left( \prod_{v|p} F_v \right) \\ &\cong \prod_{v|p} (D/D^0 \otimes_{\mathbf{Q}_p} F_v) \end{aligned}$$

and

$$\prod_{v|p} \exp_{F_v} : \prod_{v|p} (D/D^0 \otimes_{\mathbf{Q}_p} F_v) \to \prod_{v|p} \mathrm{H}^1(F_v, V_pE) = \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, V_pE) .$$

We define $\exp_F^* : \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, V_pE) \to D^0 \otimes_{\mathbf{Q}} F$ similarly.

The diagram below is commutative

$$\begin{array}{ccccc} \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, V_pE) & \times & \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, V_pE) & \xrightarrow{[\ ,\ ]_F} & \mathbf{Q}_p \\ \exp_F \uparrow & & \exp_F^* \downarrow & & \| \\ D/D^0 \otimes_{\mathbf{Q}} F & \times & D^0 \otimes_{\mathbf{Q}} F & \xrightarrow{\mathrm{tr}_{F/\mathbf{Q}}[\ ,\ ]} & \mathbf{Q}_p . \end{array}$$

Here, $[\ ,\ ]_F := \sum_{v|p} [\ ,\ ]_{F_v}$, and $\mathrm{tr}_{F/\mathbf{Q}}[\ ,\ ]$ is the composite of

$$D/D^0 \otimes_{\mathbf{Q}} F \times D^0 \otimes_{\mathbf{Q}} F \xrightarrow{[\ ,\ ]} \mathbf{Q}_p \otimes_{\mathbf{Q}} F \xrightarrow{\mathrm{tr}_{F/\mathbf{Q}}} \mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q} \cong \mathbf{Q}_p .$$

For $F = \mathbf{Q}(\mu_N)$ with a positive integer $N$, we denote $\exp_{\mathbf{Q}(\mu_N)}$ by $\exp_N$, $\exp^*_{\mathbf{Q}(\mu_N)}$ by $\exp_N^*$ and $[\ ,\ ]_{\mathbf{Q}(\mu_N)}$ by $[\ ,\ ]_N$. We define $\mathcal{G}_N := \mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q}) \cong (\mathbf{Z}/N\mathbf{Z})^\times$.

DEFINITION 2.1. For each $x \in D/D^0 \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N)$ and $z \in \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N), V_p E)$, we define

$$\begin{aligned} P_N(x,z) &:= \sum_{\sigma \in \mathcal{G}_N} \mathrm{tr}_{N/1}[\sigma(x), \exp_N^*(z)]\sigma \\ &= \sum_{\sigma,\tau \in \mathcal{G}_N} [\sigma(x), \tau(\exp_N^*(z))]\sigma\tau^{-1} \in \mathbf{Q}_p[\mathcal{G}_N]\,. \end{aligned}$$

REMARK 2.2. $P_N(x,z)$ is an analogue of the pairing $P_n(x,z)$ in Kurihara [6] §3.

Define the ring endomorphism $* : \mathbf{Q}_p[\mathcal{G}_N] \to \mathbf{Q}_p[\mathcal{G}_N]$ by $(\sum_{\sigma \in \mathcal{G}_N} a_\sigma \sigma)^* := \sum_{\sigma \in \mathcal{G}_N} a_\sigma \sigma^{-1}$.

LEMMA 2.3. *For an element $A \in \mathbf{Q}_p[\mathcal{G}_N]$, we have*

$$\begin{aligned} P_N(Ax,z) &= A^* P_N(x,z) \\ P_N(x,Az) &= A P_N(x,z)\,. \end{aligned}$$

*In particular, if $A^{-1}$ exists in $\mathbf{Q}_p[\mathcal{G}_N]$, then we have*

$$P_N(A^{-1}x, A^*z) = P_N(x,z)\,.$$

PROOF. To prove the first half of the lemma, it suffices to show it in the case when $A = \rho \in \mathcal{G}_N$. From the definition, we obtain

$$\begin{aligned} P_N(\rho(x),z) &= \sum_{\sigma,\tau \in \mathcal{G}_N} [\sigma\rho(x), \tau(\exp_N^*(z))]\sigma\tau^{-1} \\ &= \rho^{-1} \sum_{\sigma,\tau \in \mathcal{G}_N} [(\sigma\rho)(x), \tau(\exp_N^*(z))](\sigma\rho)\tau^{-1} \\ &= \rho^{-1} \sum_{\sigma,\tau \in \mathcal{G}_N} [\sigma(x), \tau(\exp_N^*(z))]\sigma\tau^{-1} \\ &= \rho^{-1} P_N(x,z) \\ &= \rho^* P_N(x,z)\,. \end{aligned}$$

Thus we have proved $P_N(\rho(x),z) = \rho^* P_N(x,z)$. We can prove $P_N(x,\rho(z)) = \rho P_N(x,z)$ similarly. The latter is obtained from the former immediately. □

DEFINITION 2.4. We define $x'_N$ and $x_N$ by

$$\begin{aligned} x'_N &:= \upsilon_N\left(\left(\prod_{l|N} F_l(\widehat{\sigma_l})^{-1}\right)\xi_N\right) \in \mathbf{Q}(\mu_N) \\ x_N &:= x'_N\omega^* \in D/D^0 \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N)\,, \end{aligned}$$

and define the homomorphism

$$\mathcal{P}_N : \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N), V_p E) \to \mathbf{Q}_p[\mathcal{G}_N]$$

by $\mathcal{P}_N(z) := P_N(x_N, z)$. Here, $F_l(T)$ is the polynomial in Definition 1.2.

PROPOSITION 2.5. *Assume $q$ is a prime number and $N \geq 1$ is an integer. Then, we have*

$$\mathrm{tr}_{qN/N}(x_{qN}) = \begin{cases} a_q x_N - \varepsilon_q x_{N/q} & (q^2|N) \\ a_q x_N - \varepsilon_q F_q(\sigma_q)^{-1} x_{N/q} & (q \| N) \\ (a_q - \varepsilon_q \sigma_q - \sigma_q^{-1}) F_q(\sigma_q)^{-1} x_N & (q \nmid N)\,. \end{cases}$$

Before proving the proposition, we prove a lemma.

LEMMA 2.6. *For a prime number $l$, define the sequence $(c_n^{(l)})_{n\geq 0}$ in $\mathbf{Z}[\frac{1}{l}]$ by $c_0^{(l)} = 0$, $c_1^{(l)} = 1$, and for $n \geq 1$,*

$$c_{n+1}^{(l)} := \frac{a_l}{l} c_n^{(l)} - \frac{\varepsilon_l}{l} c_{n-1}^{(l)}\,,$$

*and define the polynomial $\widetilde{F}_l^{(n)}(T) \in \mathbf{Q}[T]$ by*

$$\widetilde{F}_l^{(n)}(T) := c_{n+1}^{(l)} - \frac{\varepsilon_l}{l} c_n^{(l)} T\,.$$

*Then, we have*

$$F_l(\widehat{\sigma_l})^{-1} = \sum_{i=0}^{n-1} c_{i+1}^{(l)} \widehat{\sigma}_l^i + \widetilde{F}_l^{(n)}(\widehat{\sigma_l}) F_l(\widehat{\sigma_l})^{-1} \widehat{\sigma}_l^n$$

*as an endomorphism of $\mathbf{Q}(\mu_L)[C_M]$ for $L, M \geq 1$ with $(L, M) = 1$ and $l \nmid L$. In particular, we have*

$$F_l(\sigma_l)^{-1} = 1 + \left(\frac{a_l}{l} - \frac{\varepsilon_l}{l}\widehat{\sigma}_l\right) F_l(\sigma_l)^{-1} \widehat{\sigma}_l\,.$$

REMARK 2.7. The sequence $(c_n^{(l)})_{n\geq 0}$ is a generalization of the sequence $(c_n)$ in section 2.2.1 in Kurihara [6].

PROOF. It is enough to show that

$$\sum_{i=0}^{n-1} c_{i+1}^{(l)} F_l(\widehat{\sigma_l}) \widehat{\sigma}_l^i + \widetilde{F}_l^{(n)}(\widehat{\sigma_l}) \widehat{\sigma}_l^n = 1\,. \tag{1}$$

We will prove the equation (1) by induction.

Since we have $\widetilde{F}_l^{(0)}(\widehat{\sigma_l}) = 1$, the equation holds in the case when $n = 0$. To prove the rest part of the induction, it is enough to show that

$$\widetilde{F}_l^{(n)}(\widehat{\sigma_l}) \widehat{\sigma}_l^n = c_{n+1}^{(l)} F_l(\widehat{\sigma_l}) \widehat{\sigma}_l^n + \widetilde{F}_l^{(n+1)}(\widehat{\sigma_l}) \widehat{\sigma}_l^{n+1} \tag{2}$$

for all $n \geq 0$.

From the definitions of the sequence $(c_n^{(l)})_{n\geq 0}$ and the polynomials $\widetilde{F}_l^{(n)}(T)$ and $F_l(T)$, we have

$$\begin{aligned} c_{n+1}^{(l)} F_l(\widehat{\sigma}_l) + \widetilde{F}_l^{(n+1)}(\widehat{\sigma}_l)\widehat{\sigma}_l &= c_{n+1}^{(l)}\left(1 - \frac{a_l}{l}\widehat{\sigma}_l + \frac{\varepsilon_l}{l}\widehat{\sigma}_l^2\right) + \left(c_{n+2}^{(l)}\widehat{\sigma}_l - \frac{\varepsilon_l}{l}c_{n+1}^{(l)}\widehat{\sigma}_l^2\right) \\ &= c_{n+1}^{(l)} + \left(c_{n+2}^{(l)} - \frac{a_l}{l}c_{n+1}^{(l)}\right)\widehat{\sigma}_l \\ &= c_{n+1}^{(l)} - \frac{\varepsilon_l}{l}c_n^{(l)}\widehat{\sigma}_l \\ &= \widetilde{F}_l^{(n)}(\widehat{\sigma}_l)\,. \end{aligned}$$

Multiplying $\widehat{\sigma}_l^n$, we have proved the equation (2). Thus, we have proved the lemma. □

PROOF OF PROPOSITION 2.5. We will prove the same formula for $x'_N$. Put $N = q^n M$ with $(q, M) = 1$.

Since we have $F_l(\widehat{\sigma}_l)^{-1} = 1 + (\frac{a_l}{l} - \frac{\varepsilon_l}{l}\widehat{\sigma}_l)F_l(\widehat{\sigma}_l)^{-1}\widehat{\sigma}_l$ from Lemma 2.6 and $\widehat{\sigma}_q(\xi_{qN}) = \xi_N$, we have

$$\begin{aligned} \mathrm{tr}_{qN/N}(x'_{qN}) &= \mathrm{tr}_{qN/N}\left(\upsilon_{qN}\left(\left(\prod_{l|qN} F_l(\widehat{\sigma}_l)^{-1}\right)\xi_{qN}\right)\right) \\ &= \mathrm{tr}_{qN/N}\left(\upsilon_{qN}\left(F_q(\widehat{\sigma}_q)^{-1}\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)\xi_{qN}\right)\right) \\ &= \mathrm{tr}_{qN/N}\left(\upsilon_{qN}\left(\left(1 + \left(\frac{a_q}{q} - \frac{\varepsilon_q}{q}\widehat{\sigma}_q\right)F_q(\widehat{\sigma}_q)^{-1}\widehat{\sigma}_q\right)\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)\xi_{qN}\right)\right) \\ &= \mathrm{tr}_{qN/N}\left(\upsilon_{qN}\left(\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)\xi_{qN}\right)\right) \\ &\quad + \frac{a_q}{q}\mathrm{tr}_{qN/N}\left(\upsilon_N\left(F_q(\widehat{\sigma}_q)^{-1}\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)\xi_N\right)\right) \\ &\quad - \frac{\varepsilon_q}{q}\mathrm{tr}_{qN/N}\left(\upsilon_N\left(F_q(\widehat{\sigma}_q)^{-1}\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)\widehat{\sigma}_q(\xi_N)\right)\right). \end{aligned} \tag{3}$$

First, we treat the first term of the right hand side of the equation (3). As we have seen in §1, we have

$$\mathrm{tr}_{qN/N} \circ \upsilon_{qN} = \mathrm{tr}_{q^{n+1}M/q^n M} \circ \upsilon_M \circ \upsilon_{q^n} = \upsilon_M \circ \mathrm{tr}_{q^{n+1}/q^n} \circ \upsilon_{q^n}\,,$$

and the trace map commutes with $\widehat{\sigma}_a$ for each positive integer $a$. We also have $\xi_{q^{n+1}M} = \widehat{\sigma}_M^{-1}(\xi_{q^{n+1}})\widehat{\sigma}_{q^{n+1}}^{-1}(\xi_M)$. Thus we have

$$\begin{aligned}
&\mathrm{tr}_{qN/N}\left(\upsilon_{qN}\left(\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)\xi_{qN}\right)\right)\\
&\quad = \mathrm{tr}_{qN/N}\left(\upsilon_{qN}\left(\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)(\widehat{\sigma}_M^{-1}(\xi_{q^{n+1}})\widehat{\sigma}_{q^{n+1}}^{-1}(\xi_M))\right)\right)\\
&\quad = \upsilon_{qN}\left(\mathrm{tr}_{q^{n+1}/q^n}\left(\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)(\widehat{\sigma}_M^{-1}(\zeta_{q^{n+1}})\widehat{\sigma}_{q^{n+1}}^{-1}(\xi_M))\right)\right)\\
&\quad = \upsilon_{qN}\left(\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)(\widehat{\sigma}_M^{-1}(\mathrm{tr}_{q^{n+1}/q^n}(\zeta_{q^{n+1}}))\widehat{\sigma}_{q^{n+1}}^{-1}(\xi_M))\right).
\end{aligned}$$

Since we have $\mathrm{tr}_{q^{n+1}/q^n}(\zeta_{q^{n+1}}) = 0$ if $n \geq 1$, we have

$$\upsilon_{qN}\left(\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)(\widehat{\sigma}_M^{-1}(\mathrm{tr}_{q^{n+1}/q^n}(\zeta_{q^{n+1}}))\widehat{\sigma}_{q^{n+1}}^{-1}(\xi_M))\right) = 0$$

if $n \geq 1$. Since we have $\upsilon_M \circ \widehat{\sigma}_q = \sigma_q \circ \upsilon_M$, $M = N$ and $\mathrm{tr}_{q/1}(\zeta_q) = -1$ if $n = 0$, we have

$$\begin{aligned}
&\upsilon_{qN}\left(\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)(\widehat{\sigma}_M^{-1}(\mathrm{tr}_{q/1}(\zeta_q))\widehat{\sigma}_q^{-1}(\xi_M))\right)\\
&\quad = -\upsilon_{qN}\left(\left(\prod_{l|N} F_l(\widehat{\sigma}_l)^{-1}\right)\widehat{\sigma}_q^{-1}(\xi_N)\right)\\
&\quad = -\sigma_q^{-1}\left(\upsilon_{qN}\left(\left(\prod_{l|N} F_l(\widehat{\sigma}_l)^{-1}\right)\xi_N\right)\right)\\
&\quad = -\sigma_q^{-1}x'_N\\
&\quad = -\left(\sigma_q^{-1} - \frac{a_q}{q} + \frac{\varepsilon_q}{q}\sigma_q\right)F_q(\sigma_q)^{-1}x'_N\,.
\end{aligned}$$

Thus we have

$$\begin{aligned}
&\mathrm{tr}_{qN/N}\left(\upsilon_{qN}\left(\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)\xi_{qN}\right)\right)\\
&\quad = \begin{cases} 0 & (n \geq 1)\\ -\left(\sigma_q^{-1} - \dfrac{a_q}{q} + \dfrac{\varepsilon_q}{q}\sigma_q\right)F_q(\sigma_q)^{-1}x'_N & (n = 0)\,. \end{cases}
\end{aligned} \tag{4}$$

Next, we treat the second term of the equation (3). Since we have $\upsilon_N(F_q(\widehat{\sigma}_q)^{-1}(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1})\xi_N) \in \mathbf{Q}(\mu_N)$, the trace map $\mathrm{tr}_{qN/N}$ is multiplication by $q$ if $q|N$ and multiplication by $q-1$ if $q \not| N$. We also have

$$F_q(\widehat{\sigma}_q)^{-1}\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right) = \prod_{l|N} F_l(\widehat{\sigma}_l)^{-1}$$

if $q|N$. Thus we obtain

$$\begin{aligned}\frac{a_q}{q}\mathrm{tr}_{qN/N}&\left(\upsilon_N\left(F_q(\widehat{\sigma}_q)^{-1}\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)\xi_N\right)\right)\\ &= \begin{cases} a_q x'_N & (n \geq 1) \\ \dfrac{(q-1)a_q}{q} F_q(\sigma_q)^{-1} x'_N & (n = 0)\,. \end{cases}\end{aligned} \tag{5}$$

We then treat the third term of the equation (3). Since we have $\widehat{\sigma}_q(\xi_N) = \xi_{\frac{N}{q}}$ if $q|N$ and $F_q(\widehat{\sigma}_q)^{-1}(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}) = \prod_{l|\frac{N}{q}} F_l(\widehat{\sigma}_l)^{-1}$ if $q^2|N$, we have

$$\begin{aligned}\frac{\varepsilon_q}{q}\mathrm{tr}_{qN/N}&\left(\upsilon_N\left(F_q(\widehat{\sigma}_q)^{-1}\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)\widehat{\sigma}_q(\xi_N)\right)\right)\\ &= \begin{cases} \varepsilon_q x'_{\frac{N}{q}} & (n \geq 2) \\ \varepsilon_q F_q(\sigma_q)^{-1} x'_{\frac{N}{q}} & (n = 1) \\ \dfrac{\varepsilon_q}{q}(q-1)\sigma_q F_q(\sigma_q)^{-1} x'_N & (n = 0)\,. \end{cases}\end{aligned} \tag{6}$$

Combining the equations (4), (5) and (6), if $q^2|N$, we have

$$\begin{aligned}\mathrm{tr}_{qN/N}(x'_{qN}) &= 0 + a_q x'_N - \varepsilon_q x'_{\frac{N}{q}} \\ &= a_q x'_N - \varepsilon_q x'_{\frac{N}{q}}\,.\end{aligned}$$

If $q||N$, we have

$$\begin{aligned}\mathrm{tr}_{qN/N}(x'_{qN}) &= 0 + a_q x'_N - \varepsilon_q F_q(\sigma_q)^{-1} x'_{\frac{N}{q}} \\ &= a_q x'_N - \varepsilon_q F_q(\sigma_q)^{-1} x'_{\frac{N}{q}}\,.\end{aligned}$$

If $q \not| N$, we have

$$\mathrm{tr}_{qN/N}(x'_{qN}) = -\left(\sigma_q^{-1} - \frac{a_q}{q} + \frac{\varepsilon_q}{q}\sigma_q\right) F_q(\sigma_q)^{-1} x'_N$$

$$
\begin{aligned}
&+\frac{(q-1)a_q}{q}F_q(\sigma_q)^{-1}x'_N-\frac{\varepsilon_q}{q}(q-1)\sigma_q F_q(\sigma_q)^{-1}x_N\\
&=\left(-\sigma_q^{-1}+\frac{a_q}{q}-\frac{\varepsilon_q}{q}\sigma_q+\frac{(q-1)a_q}{q}-\frac{\varepsilon_q}{q}(q-1)\sigma_q\right)F_q(\sigma_q)^{-1}x'_N\\
&=(a_q-\varepsilon_q\sigma_q-\sigma_q^{-1})F_q(\sigma_q)^{-1}x'_N\,.
\end{aligned}
$$

Thus, we have proved the proposition. □

### 3. The zeta elements and the modular elements

Kato defined an Euler system in cohomology groups $\mathrm{H}^1(\mathbf{Z}[\mu_N,\frac{1}{S}],V_pE)$ in [4]. Here $\mathrm{H}^1(\mathbf{Z}[\mu_N,\frac{1}{S}],V_pE)=\mathrm{H}^1_{et}(\mathrm{Spec}\mathbf{Z}[\mu_N,\frac{1}{S}],V_pE)$ and $S$ is the set of bad primes, the infinite prime and $p$. It is called the zeta element. We regard $z_N\in\mathrm{H}^1(\mathbf{Q}_p\otimes_{\mathbf{Q}}\mathbf{Q}(\mu_N),V_pE)$ through the natural map $\mathrm{H}^1(\mathbf{Z}[\mu_N,\frac{1}{S}],V_pE)\to\mathrm{H}^1(\mathbf{Q}_p\otimes_{\mathbf{Q}}\mathbf{Q}(\mu_N),V_pE)$. We normalize the zeta element as follows.

PROPOSITION 3.1. *Let $\chi$ be a character of conductor $N$, then the zeta element $z_N\in\mathrm{H}^1(\mathbf{Q}_p\otimes_{\mathbf{Q}}\mathbf{Q}(\mu_N),V_pE)$ satisfies*

$$
\sum_{\sigma\in\mathcal{G}_N}\chi(\sigma)\exp_N^*(\sigma(z_N))=\frac{L(E,\chi,1)}{\Omega_E^{\pm}}\omega\quad(\chi(-1)=\pm1)\,.
$$

Here, $\exp_N^*$ is the dual exponential map and $\Omega_E^{\pm}$ are Néron periods. See Kato [4], Theorem 12.5.

We call a system of elements $(w_M)_M\in\prod_{M|N}\mathrm{H}^1(\mathbf{Q}_p\otimes_{\mathbf{Q}}\mathbf{Q}(\mu_M),V_pE)$ an Euler system, when they satisfy

$$
\mathrm{Nr}_{qM/M}(w_{qM})=\begin{cases}w_M & (q|M)\\ F_q(\sigma_q^{-1})w_M & (q\not|M)\,.\end{cases}
$$

PROPOSITION 3.2. *The zeta elements $(z_M)_M$ form an Euler system.*

See Kato [4], Theorem 8.12.

On the other hand, Mazur-Tate [8] defined the modular element $\theta_N\in\mathbf{Q}[\mathcal{G}_N]$ by

$$
\theta_N:=\sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times}\left(\left[\frac{a}{N}\right]_E^+-\left[\frac{a}{N}\right]_E^-\right)\sigma_a\,.
$$

Here, for $r\in\mathbf{Q}$, $[r]_E^{\pm}\in\mathbf{R}$ are defined by

$$
2\pi\int_0^\infty f(r+iy)dy=[r]_E^+\Omega_E^+-[r]_E^-\Omega_E^-
$$

where $f(z) = \sum_{n=1}^{\infty} a_n q^n$ is the modular form corresponding to $E$. From Manin-Drinfeld theorem, we know $[r]_E^{\pm} \in \mathbf{Q}$. They satisfy

$$\chi(\theta_N) = \tau(\chi)\frac{L(E, \chi^{-1}, 1)}{\Omega_E^{\pm}} \quad (\chi(-1) = \pm 1)$$

for each character $\chi$ of conductor $N$, where $\tau(\chi) := \sum_{\sigma \in \mathcal{G}_N} \chi(\sigma)\sigma(\zeta_N)$ is the Gauss sum. For each prime number $q$, they satisfy compatible formulas below.

$$\pi_{qM/M}(\theta_{qM}) = \begin{cases} a_q\theta_M - \varepsilon_q \nu_{M/\frac{M}{q}}(\theta_{\frac{M}{q}}) & (q|M) \\ (a_q - \sigma_q - \varepsilon_q\sigma_q^{-1})\theta_M & (q \not| M)\,. \end{cases}$$

Here, for integers $L$ and $M$ with $L$ dividing $M$, the map $\pi_{M/L} : \mathbf{Q}_p[\mathcal{G}_M] \to \mathbf{Q}_p[\mathcal{G}_L]$ is defined by the restriction map of the Galois group $\mathcal{G}_M \to \mathcal{G}_L$, and the map $\nu_{M/L} : \mathbf{Q}_p[\mathcal{G}_L] \to \mathbf{Q}_p[\mathcal{G}_M]$ is defined by

$$\sigma \mapsto \sum_{\tau \in \mathcal{G}_M, \pi_{M/L}(\tau) = \sigma} \tau$$

for $\sigma \in \mathcal{G}_L$.

In this paper, we call a system of elements $(\eta_M)_M \in \prod_{M|N} \mathbf{Q}_p[\mathcal{G}_M]$ an *admissible system*, when they satisfy the same compatible formulas.

REMARK 3.3. In [8], the modular elements are defined by $\theta_N := \frac{1}{2}\sum_{a \in \mathcal{G}_{\mathcal{N}}/\{\pm 1\}} [\frac{a}{N}]_E^{+}\sigma_a \in \mathbf{Q}[\mathcal{G}_N/\{\pm 1\}]$.

THEOREM 3.4. *If $(w_M)_M \in \prod_{M|N} \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_M), V_pE)$ is an Euler system, then $(\mathcal{P}_M(w_M))_M \in \prod_{M|N} \mathbf{Q}_p[\mathcal{G}_M]$ is an admissible system.*

Before proving the theorem, we will prove a lemma.

LEMMA 3.5. *Let $L$ be a positive integer and let $q$ be a prime number. For $x \in D \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{qL})$ and $z \in \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{qL}), V_pE)$, we have*

$$\pi_{qL/L}(P_{qL}(x, z)) = P_L(\mathrm{tr}_{qL/L}(x), \mathrm{Nr}_{qL/L}(z))\,.$$

*For $x \in D \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_L)$ and $z \in \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{qL}), V_pE)$, we have*

$$P_{qL}(x, z) = \nu_{qL/L}(P_L(x, \mathrm{Nr}_{qL/L}(z)))\,.$$

PROOF. For $x \in D \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{qL})$ and $z \in \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{qL}), V_pE)$, an easy calculation shows that

$$\pi_{qL/L}(P_{qL}(x, z)) = \pi_{qL/L}\Big(\sum_{s,t \in \mathcal{G}_{qL}} [s(x), \exp_{qL}^*(t(z))]st^{-1}\Big)$$

$$
\begin{aligned}
&= \sum_{s,t\in\mathcal{G}_{qL}} [s(x), \exp^*_{qL}(t(z))]\pi_{qL/L}(st^{-1}) \\
&= \sum_{\sigma,\tau\in\mathcal{G}_L} \Bigg( \sum_{s,t\in\mathcal{G}_{qL},\pi_{qL/L}(s)=\sigma,\pi_{qL/L}(t)=\tau} [s(x), t(\exp^*_{qL}(z))] \Bigg) \sigma\tau^{-1} \\
&= \sum_{\sigma,\tau\in\mathcal{G}_L} \Bigg[ \sum_{s\in\mathcal{G}_{qL},\pi_{qL/L}(s)=\sigma} s(x), \sum_{t\in\mathcal{G}_{qL},\pi_{qL/L}(t)=\tau} t(\exp^*_{qL}(z)) \Bigg] \sigma\tau^{-1} \\
&= \sum_{\sigma,\tau\in\mathcal{G}_L} [\sigma(\mathrm{tr}_{qL/L}(x)), \tau(\mathrm{tr}_{qL/L}(\exp^*_{qL}(z)))]\sigma\tau^{-1} \\
&= \sum_{\sigma,\tau\in\mathcal{G}_L} [\sigma(\mathrm{tr}_{qL/L}(x)), \exp^*_L(\tau(\mathrm{Nr}_{qL/L}(z)))]\sigma\tau^{-1} \\
&= P_L(\mathrm{tr}_{qL/L}(x), \mathrm{Nr}_{qL/L}(z)) .
\end{aligned}
$$

Thus, we have proved the first half of the lemma.

Similarly, for $x \in D \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_L)$ and $z \in \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{qL}), V_p E)$, we have

$$
\begin{aligned}
&v_{qL/L}(P_L(x, \mathrm{Nr}_{qL/L}(z))) \\
&\quad = v_{qL/L}\Bigg( \sum_{\sigma,\tau\in\mathcal{G}_L} [\sigma(x), \exp^*_L(\tau(\mathrm{Nr}_{qL/L}(z)))]\sigma\tau^{-1} \Bigg) \\
&\quad = \sum_{\rho\in\mathcal{G}_{qL}} \Bigg( \sum_{\sigma,\tau\in\mathcal{G}_L,\pi_{qL/L}(\rho)=\sigma\tau^{-1}} [\sigma(x), \exp^*_L(\tau(\mathrm{Nr}_{qL/L}(z)))] \Bigg) \rho \\
&\quad = \sum_{\rho\in\mathcal{G}_{qL}} \Bigg( \sum_{\sigma,\tau\in\mathcal{G}_L,\pi_{qL/L}(\rho)=\sigma\tau^{-1}} [\sigma(x), \tau(\mathrm{tr}_{qL/L}(\exp^*_{qL}(z)))] \Bigg) \rho \\
&\quad = \sum_{\rho\in\mathcal{G}_{qL}} \Bigg( \sum_{\sigma,\tau\in\mathcal{G}_L,\pi_{qL/L}(\rho)=\sigma\tau^{-1}} \Bigg[ \sigma(x), \sum_{t\in\mathcal{G}_{qL},\pi_{qL/L}(t)=\tau} t(\exp^*_{qL}(z)) \Bigg] \Bigg) \rho \\
&\quad = \sum_{\rho,t\in\mathcal{G}_{qL},\sigma,\tau\in\mathcal{G}_L,\pi_{qL/L}(\rho)=\sigma\tau^{-1},\pi_{qL/L}(t)=\tau} [\sigma(x), t(\exp^*_{qL}(z))]\rho .
\end{aligned}
$$

The condition $\pi_{qL/L}(\rho) = \sigma\tau^{-1}$ and $\pi_{qL/L}(t) = \tau$ is equivalent that $\pi_{qL/L}(\rho t) = \sigma$ and $\pi_{qL/L}(t) = \tau$. Putting $s = \rho t \in \mathcal{G}_{qL}$, we obtain

$$
\begin{aligned}
&\sum_{\rho,t\in\mathcal{G}_{qL},\sigma,\tau\in\mathcal{G}_L,\pi_{qL/L}(\rho)=\sigma\tau^{-1},\pi_{qL/L}(t)=\tau} [\sigma(x), t(\exp^*_{qL}(z))]\rho \\
&\qquad = \sum_{s,t\in\mathcal{G}_{qL},\sigma,\tau\in\mathcal{G}_L,\pi_{qL/L}(s)=\sigma,\pi_{qL/L}(t)=\tau} [\sigma(x), t(\exp^*_{qL}(z))]st^{-1}
\end{aligned}
$$

$$= \sum_{s,t \in \mathcal{G}_{qL}} [s(x), \exp^*_{qL}(t(z))] st^{-1}$$
$$= P_{qL}(x, z) .$$

Thus, we have proved the lemma. □

PROOF OF THEOREM 3.4. From Definition 2.4 and Lemma 3.5, we have

$$\pi_{qM/M}(\mathcal{P}_{qM}(w_{qM})) = \pi_{qM/M}(P_{qM}(x_{qM}, w_{qM}))$$
$$= P_M(\mathrm{tr}_{qM/M}(x_{qM}), \mathrm{Nr}_{qM/M}(w_{qM})) .$$

If $q^2|M$, from Proposition 2.5, we have

$$P_M(\mathrm{tr}_{qM/M}(x_{qM}), \mathrm{Nr}_{qM/M}(w_{qM})) = P_M(a_q x_M - \varepsilon_q x_{\frac{M}{q}}, w_M)$$
$$= a_q P_M(x_M, w_M) - \varepsilon_q P_M(x_{\frac{M}{q}}, w_M) .$$

Applying Lemma 3.5 by $L = \frac{M}{q}$, we have

$$P_M(x_{\frac{M}{q}}, w_M) = \nu_{M/\frac{M}{q}}(P_{\frac{M}{q}}(x_{\frac{M}{q}}, \mathrm{Nr}_{M/\frac{M}{q}}(w_M)))$$
$$= \nu_{M/\frac{M}{q}}(P_{\frac{M}{q}}(x_{\frac{M}{q}}, w_{\frac{M}{q}})) .$$

Thus, we have proved that

$$\pi_{qM/M}(\mathcal{P}_{qM}(w_{qM})) = a_q P_M(x_M, w_M) - \varepsilon_q \nu_{M/\frac{M}{q}}(P_{\frac{M}{q}}(x_{\frac{M}{q}}, w_{\frac{M}{q}}))$$
$$= a_q \mathcal{P}_M(w_M) - \varepsilon_q \nu_{M/\frac{M}{q}}(\mathcal{P}_{\frac{M}{q}}(w_{\frac{M}{q}})) .$$

If $q||M$, then we have

$$P_M(\mathrm{tr}_{qM/M}(x_{qM}), \mathrm{Nr}_{qM/M}(w_{qM}))$$
$$= P_M(a_q x_M - \varepsilon_q F_q(\sigma_q)^{-1} x_{\frac{M}{q}}, w_M)$$
$$= a_q P_M(x_M, w_M) - \varepsilon_q P_M(F_q(\sigma_q)^{-1} x_{\frac{M}{q}}, w_M)$$
$$= a_q P_M(x_M, w_M) - \varepsilon_q \nu_{M/\frac{M}{q}}(P_{\frac{M}{q}}(F_q(\sigma_q)^{-1} x_{\frac{M}{q}}, \mathrm{Nr}_{M/\frac{M}{q}}(w_M)))$$
$$= a_q P_M(x_M, w_M) - \varepsilon_q \nu_{M/\frac{M}{q}}(P_{\frac{M}{q}}(F_q(\sigma_q)^{-1} x_{\frac{M}{q}}, F_q(\sigma_q^{-1}) w_{\frac{M}{q}}))$$
$$= a_q P_M(x_M, w_M) - \varepsilon_q \nu_{M/\frac{M}{q}}(P_{\frac{M}{q}}(x_{\frac{M}{q}}, w_{\frac{M}{q}}))$$
$$= a_q \mathcal{P}_M(w_M) - \varepsilon_q \nu_{M/\frac{M}{q}}(\mathcal{P}_{\frac{M}{q}}(w_{\frac{M}{q}})) .$$

Here, we used Lemma 2.3.

If $q \not| M$, then we have

$$P_M(\mathrm{tr}_{qM/M}(x_{qM}), \mathrm{Nr}_{qM/M}(w_{qM})) = P_M((a_q - \varepsilon_q \sigma_q - \sigma_q^{-1}) F_q(\sigma_q)^{-1} x_M, F_q(\sigma_q^{-1}) w_M)$$

$$= (a_q - \sigma_q - \varepsilon_q \sigma_q^{-1}) \mathcal{P}_M(w_M)\,.$$

Thus, we have proved the theorem. □

THEOREM 3.6. *From the notations as above, we have* $\mathcal{P}_N(z_N) = \theta_N$.

To prove this theorem, we need some lemmas.

LEMMA 3.7. *Let* $(\eta_M)_M, (\kappa_M)_M \in \prod_{M|N} \mathbf{Q}_p[\mathcal{G}_M]$ *be two admissible systems. Fix a positive integer* $M$ *dividing* $N$. *If* $\eta_L = \kappa_L$ *for each positive integer* $L$ *with* $L$ *dividing* $M$ *and* $L \neq M$, *and* $\chi(\eta_M) = \chi(\kappa_M)$ *for each character* $\chi$ *of conductor* $M$, *then* $\eta_M = \kappa_M$.

PROOF. To prove $\eta_M = \kappa_M$, it suffices to show that $\chi(\eta_M) = \chi(\kappa_M)$ for each character $\chi$ of $\mathcal{G}_M$. From the assumption, $\chi(\eta_M) = \chi(\kappa_M)$ for each character $\chi$ of conductor $M$. If the conductor of $\chi$ is not equal to $M$, then we can regard $\chi$ as a character of the group $\mathcal{G}_{\frac{M}{q}}$ for some prime number $q$ dividing $M$, and we obtain $\chi(\eta_M) = \chi(\pi_{M/\frac{M}{q}}(\eta_M))$. So it suffices to show that $\pi_{M/\frac{M}{q}}(\eta_M) = \pi_{M/\frac{M}{q}}(\kappa_M)$ for each prime number $q$ dividing $M$.

First, we assume that $q^2$ divides $M$. Then, we get $\pi_{M/\frac{M}{q}}(\eta_M) = a_q \eta_{\frac{M}{q}} - \varepsilon_q \nu_{\frac{M}{q}/\frac{M}{q^2}}(\eta_{\frac{M}{q^2}})$ and $\pi_{M/\frac{M}{q}}(\kappa_M) = a_q \kappa_{\frac{M}{q}} - \varepsilon_q \nu_{\frac{M}{q}/\frac{M}{q^2}}(\kappa_{\frac{M}{q^2}})$. Since we have $\eta_{\frac{M}{q}} = \kappa_{\frac{M}{q}}$ and $\eta_{\frac{M}{q^2}} = \kappa_{\frac{M}{q^2}}$ from the assumption, we obtain $\pi_{M/\frac{M}{q}}(\eta_M) = \pi_{M/\frac{M}{q}}(\kappa_M)$. If $q||M$, then we have $\pi_{M/\frac{M}{q}}(\eta_M) = (a_q - \sigma_q - \varepsilon_q \sigma_q^{-1})\eta_{\frac{M}{q}} = (a_q - \sigma_q - \varepsilon_q \sigma_q^{-1})\kappa_{\frac{M}{q}} = \pi_{M/\frac{M}{q}}(\kappa_M)$. Thus we have proved the lemma. □

LEMMA 3.8. *Let* $(\eta_M)_M, (\kappa_M)_M \in \prod_{M|N} \mathbf{Q}_p[\mathcal{G}_M]$ *be two admissible systems. Suppose that for each positive integer* $M$ *dividing* $N$, *we have* $\chi(\eta_M) = \chi(\kappa_M)$ *for each character* $\chi$ *of conductor* $M$. *Then we have* $\eta_N = \kappa_N$.

PROOF. We will prove that $\eta_M = \kappa_M$ for each positive integer $M$ dividing $N$ by induction. First, we show that $\eta_1 = \kappa_1$. From the assumption, $\chi^0(\eta_1) = \chi^0(\kappa_1)$ for the character $\chi^0$ of conductor 1. Since $\chi^0 : \mathbf{Q}_p[\mathcal{G}_1] \simeq \mathbf{Q}_p$, we have $\eta_1 = \kappa_1$.

Next, suppose that $M$ divides $N$ and $\eta_L = \kappa_L$ for each positive integer $L$ such that $L$ divides $N$ and $L < M$. From the assumption, we have $\chi(\eta_M) = \chi(\kappa_M)$ for each character $\chi$ of conductor $M$. We also have $\eta_L = \kappa_L$ for each positive integer $L$ with $L$ dividing $M$ and $L \neq M$. Applying Lemma 3.7, we have $\eta_M = \kappa_M$. Thus we have proved the lemma. □

PROOF OF THEOREM 3.6. From Lemma 3.8, it is enough to show that for a character $\chi$ of conductor $N$, the $\chi$ part of the both hands are equal.

A direct calculation shows that

$$\chi(\mathcal{P}_N(z_N)) = \sum_{\sigma,\tau \in \mathcal{G}_N} [\sigma(x_N), \tau(\exp_N^*(z_N))]\chi(\sigma)\chi(\tau^{-1})$$

$$= \Big[ \sum_{\sigma \in \mathcal{G}_N} \sigma(x_N)\chi(\sigma), \sum_{\tau \in \mathcal{G}_N} \tau(\exp_N^*(z_N))\chi^{-1}(\tau) \Big]. \tag{7}$$

We first treat the right half of the pairing of the equation (7). From the properties of the zeta elements, we get

$$\begin{aligned} \sum_{\tau \in \mathcal{G}_N} \tau(\exp_N^*(z_N))\chi^{-1}(\tau) &= \sum_{\tau \in \mathcal{G}_N} \exp_N^*(\tau(z_N))\chi^{-1}(\tau) \\ &= \frac{L(E, \chi^{-1}, 1)}{\Omega_E^{\pm}}\omega . \end{aligned}$$

Next, we treat the left half. Put $\widetilde{F}_l(T) := \widetilde{F}_l^{(1)}(T)$, and let $l_1, l_2, \ldots, l_s$ be all the prime numbers dividing $N$ such that $l_1 < l_2 < \cdots < l_s$, then we have

$$\begin{aligned} \prod_{l|N} F_l(\widehat{\sigma}_l)^{-1} &= F_{l_1}(\widehat{\sigma}_{l_1})^{-1} \prod_{l'|N, l'>l_1} F_{l'}(\widehat{\sigma}_{l'})^{-1} \\ &= (1 + \widetilde{F}_{l_1}(\widehat{\sigma}_{l_1})F_{l_1}(\widehat{\sigma}_{l_1})^{-1}\widehat{\sigma}_{l_1}) \prod_{l'|N, l'>l_1} F_{l'}(\widehat{\sigma}_{l'})^{-1} \\ &= \prod_{l'|N, l'>l_1} F_{l'}(\widehat{\sigma}_{l'})^{-1} + \Big( \prod_{l'|N, l'>l_1} F_{l'}(\widehat{\sigma}_{l'})^{-1} \Big) \widetilde{F}_{l_1}(\widehat{\sigma}_{l_1})F_{l_1}(\widehat{\sigma}_{l_1})^{-1}\widehat{\sigma}_{l_1} \\ &= F_{l_2}(\widehat{\sigma}_{l_2})^{-1} \prod_{l'|N, l'>l_2} F_{l'}(\widehat{\sigma}_{l'})^{-1} + \Big( \prod_{l'|N, l'>l_1} F_{l'}(\widehat{\sigma}_{l'})^{-1} \Big) \widetilde{F}_{l_1}(\widehat{\sigma}_{l_1})F_{l_1}(\widehat{\sigma}_{l_1})^{-1}\widehat{\sigma}_{l_1} \\ &= \cdots \\ &= 1 + \sum_{l|N} \Big( \prod_{l'|N, l'>l} F_{l'}(\widehat{\sigma}_{l'})^{-1} \Big) \widetilde{F}_l(\widehat{\sigma}_l)F_l(\widehat{\sigma}_l)^{-1}\widehat{\sigma}_l . \end{aligned}$$

So, if we denote $H_l = (\prod_{l'|N, l'>l} F_{l'}(\widehat{\sigma}_{l'})^{-1})\widetilde{F}_l(\widehat{\sigma}_l)F_l(\widehat{\sigma}_l)^{-1}$, then we have

$$\prod_{l|N} F_l(\widehat{\sigma}_l)^{-1} = 1 + \sum_{l|N} H_l\widehat{\sigma}_l .$$

From the definition of $x_N$, we get

$$\begin{aligned} x_N &= \upsilon_N \Big( \Big( \prod_{l|N} F_l(\widehat{\sigma}_l)^{-1} \Big) \xi_N \Big) \omega^* \\ &= \upsilon_N \Big( \Big( 1 + \sum_{l|N} H_l\widehat{\sigma}_l \Big) \xi_N \Big) \omega^* \\ &= \upsilon_N \Big( \xi_N + \sum_{l|N} H_l \xi_{\frac{N}{l}} \Big) \omega^* \end{aligned}$$

$$= \left(\zeta_N + \sum_{l|N} \upsilon_N(H_l \xi_{\frac{N}{l}})\right)\omega^* .$$

Since $\upsilon_N(H_l\xi_{\frac{N}{l}}) \in \mathbf{Q}(\mu_{\frac{N}{l}})$, we obtain $\sum_{\sigma\in\mathcal{G}_N} \sigma(\upsilon_N(H_l\xi_{\frac{N}{l}}))\chi(\sigma) = 0$. So we have

$$\sum_{\sigma\in\mathcal{G}_N} \sigma(x_N)\chi(\sigma) = \sum_{\sigma\in\mathcal{G}_N} \sigma(\zeta_N)\chi(\sigma)\omega^* = \tau(\chi)\omega^* .$$

Therefore, it follows from (7) that

$$\begin{aligned}\chi(\mathcal{P}_N(z_N)) &= \left[\tau(\chi)\omega^*, \frac{L(E,\chi^{-1},1)}{\Omega_E^{\pm}}\omega\right] \\ &= \tau(\chi)\frac{L(E,\chi^{-1},1)}{\Omega_E^{\pm}} \\ &= \chi(\theta_N) .\end{aligned}$$

Thus, we have proved the equality. □

## 4. Integrality of the map

In this section, we will prove the following theorem.

THEOREM 4.1. *If $\widetilde{E}(\mathbf{F}_p(\mu_N))[p] = 0$, $(w_M)_M \in \prod_{M|N} \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_M), T_pE)$ is an integral Euler system and $p$ divides $N$, then $(\mathcal{P}_M(w_M))_M \in \prod_{M|N} \mathbf{Z}_p[\mathcal{G}_M]$ is an integral admissible system. Here $\widetilde{E}$ is the reduction of the elliptic curve $E$ mod $p$.*

Before proving the theorem, we make some preparations.

For a positive integer $N = \prod_l l^{e_l}$, where each $l$ is a prime number and $e_l$ is a non-negative integer, define $S(N)$ to be $S(N) := \{l : \text{prime number} \mid e_l > 0\}$, and for a set of prime numbers $S$, define $N_S$ to be $N_S := \prod_{l\notin S} l^{e_l} = N/\prod_{l\in S} l^{e_l}$.

For the rest of the section, we write $N = Mp^n$ with $p \nmid M$ and $n \geq 1$. From Lemma 2.6, we have

$$\begin{aligned}x_N &= \upsilon_N\left(\left(\prod_{l|N} F_l(\widehat{\sigma}_l)^{-1}\right)\xi_N\right)\omega^* \\ &= \upsilon_N\left(F_p(\widehat{\sigma}_p)^{-1}\left(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1}\right)\xi_N\right)\omega^* \\ &= \upsilon_N\left(F_p(\widehat{\sigma}_p)^{-1}\left(\prod_{l|M}\left(\sum_{i=0}^{e_l-1} c_i^{(l)}\widehat{\sigma}_l^i + \widetilde{F}_l^{(e_l)}(\widehat{\sigma}_l)F_l(\widehat{\sigma}_l)^{-1}\widehat{\sigma}_l^{e_l}\right)\right)\xi_N\right)\omega^*\end{aligned}$$

$$= \upsilon_N\Bigg(F_p(\widehat{\sigma}_p)^{-1}\sum_{S\subset S(M)}\Bigg(\prod_{l'\notin S}\sum_{i=0}^{e_{l'}-1}c_i^{(l')}\widehat{\sigma}_{l'}^{i}\Bigg)\Bigg(\prod_{l\in S}\widetilde{F}_l^{(e_l)}(\widehat{\sigma}_l)F_l(\widehat{\sigma}_l)^{-1}\widehat{\sigma}_l^{e_l}\Bigg)\xi_N\Bigg)\omega^*$$

$$= \sum_{S\subset S(M)}\upsilon_N\Bigg(F_p(\widehat{\sigma}_p)^{-1}\Bigg(\prod_{l'\notin S}\sum_{i=0}^{e_{l'}-1}c_i^{(l')}\widehat{\sigma}_{l'}^{i}\Bigg)\Bigg(\prod_{l\in S}\widetilde{F}_l^{(e_l)}(\widehat{\sigma}_l)F_l(\widehat{\sigma}_l)^{-1}\Bigg)\xi_{N_S}\Bigg)\omega^*.$$

So, if we put $\gamma_S := (\prod_{l'\notin S}(\sum_{i=0}^{e_{l'}-1}c_i^{(l')}\widehat{\sigma}_{l'}^{i})\prod_{l\in S}\widetilde{F}_l^{(e_l)}(\widehat{\sigma}_l))\xi_{N_S} \in \mathbf{Z}_{(p)}[C_{N_S}]$, then we obtain

$$x_N = \sum_{S\subset S(M)}\Bigg(\prod_{l\in S}F_l(\sigma_l)^{-1}\Bigg)\upsilon_N(F_p(\widehat{\sigma}_p)^{-1}\gamma_S)\omega^*.$$

Here, the coefficients of $\gamma_S$ are in $\mathbf{Z}_{(p)} = \{\frac{a}{b} \in \mathbf{Q} \mid a, b \in \mathbf{Z},\ p \not| b\}$ because $c_i^{(l')} \in \mathbf{Z}_{(p)}$ and $\widetilde{F}_l^{(e_l)}(T) \in \mathbf{Z}_{(p)}[T]$ from their definitions.

In the next lemma, $\log_{\hat{E}}$ is the formal logarithm of the formal group $\widehat{E}$ and $\log_{\hat{E}}(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S})) := \prod_{v|p}\log_{\hat{E}}(\mathbf{Q}(\mu_{N_S})_v)$, where $\log_{\hat{E}}(\mathbf{Q}(\mu_{N_S})_v) := \log_{\hat{E}}(\widehat{E}(m_{\mathbf{Q}(\mu_{N_S})_v}))$, and we put $\log(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S})) := \log_{\hat{E}}(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S}))\omega^* \subset D/D^0 \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N)$.

LEMMA 4.2. *If* $\alpha_S \in \log(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S}))$ *for all* $S \subset S(M)$, $y = \sum_{S\subset S(M)}(\prod_{l\in S}F_l(\sigma_l)^{-1})\alpha_S$ *and* $(w_L)_L \in \prod_{L|N}\mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_L), T_pE)$ *is an integral Euler system, then*

$$\mathcal{P}_N(y, w_N) \in \mathbf{Z}_p[\mathcal{G}_N].$$

From the lemma above, what we need to show to prove the theorem is that $\upsilon_N(F_p(\widehat{\sigma}_p)^{-1}\gamma_S) \in \log_{\hat{E}}(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S}))$ for all $S \subset S(M)$.

PROOF OF LEMMA 4.2. From the definition, we get

$$\begin{aligned}\mathcal{P}_N(y, w_N) &= \sum_{\sigma\in\mathcal{G}_N}\mathrm{tr}_{N/1}[\sigma(y), \exp_N^*(w_N)]\sigma\\ &= \sum_{\sigma\in\mathcal{G}_N}\mathrm{tr}_{N/1}\Bigg[\sigma\Bigg(\sum_{S\subset S(M)}\Bigg(\prod_{l\in S}F_l(\sigma_l)^{-1}\Bigg)\alpha_S\Bigg), \exp_N^*(w_N)\Bigg]\sigma\\ &= \sum_{\sigma\in\mathcal{G}_N}\sum_{S\subset S(M)}\mathrm{tr}_{N/1}\Bigg[\Bigg(\prod_{l\in S}F_l(\sigma_l)^{-1}\Bigg)\sigma(\alpha_S), \exp_N^*(w_N)\Bigg]\sigma.\end{aligned}$$

So, it is enough to show that $\mathrm{tr}_{N/1}[(\prod_{l\in S}F_l(\sigma_l)^{-1})\sigma(\alpha_S), \exp_N^*(w_N)] \in \mathbf{Z}_p$ for all $\sigma \in \mathcal{G}_N$ and $S \subset S(M)$.

From basic properties of Res and Nr, for a positive integer $L$ dividing $N$, the diagram

$$\begin{array}{ccc} \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N), V_pE) \times \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N), V_pE) & \xrightarrow{[\,,\,]_N} & \mathbf{Q}_p \\ \uparrow \mathrm{Res}_{N/L} \qquad\qquad \downarrow \mathrm{Nr}_{N/L} & & \| \\ \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_L), V_pE) \times \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_L), V_pE) & \xrightarrow{[\,,\,]_L} & \mathbf{Q}_p \end{array}$$

is commutative. Here, $\mathrm{Res}_{N/L}$ is the restriction map and $\mathrm{Nr}_{N/L}$ is the norm map, namely the corestriction map.

Thus, we have

$$\begin{aligned} &\mathrm{tr}_{N/1}\left[\left(\prod_{l\in S} F_l(\sigma_l)^{-1}\right)\sigma(\alpha_S), \exp_N^*(w_N)\right] \\ &= \left[\exp_N\left(\left(\prod_{l\in S} F_l(\sigma_l)^{-1}\right)\sigma(\alpha_S)\right), w_N\right]_N \\ &= \left[\mathrm{Res}_{N/N_S}\left(\exp_{N_S}\left(\left(\prod_{l\in S} F_l(\sigma_l)^{-1}\right)\sigma(\alpha_S)\right)\right), w_N\right]_N \\ &= \left[\exp_{N_S}\left(\left(\prod_{l\in S} F_l(\sigma_l)^{-1}\right)\sigma(\alpha_S)\right), \mathrm{Nr}_{N/N_S}(w_N)\right]_{N_S} \\ &= \left[\exp_{N_S}\left(\left(\prod_{l\in S} F_l(\sigma_l)^{-1}\right)\sigma(\alpha_S)\right), \left(\prod_{l\in S} F_l(\sigma_l^{-1})\right)w_{N_S}\right]_{N_S} \\ &= \left[\left(\prod_{l\in S} F_l(\sigma_l)^{-1}\right)\exp_{N_S}(\sigma(\alpha_S)), \left(\prod_{l\in S} F_l(\sigma_l^{-1})\right)w_{N_S}\right]_{N_S} \\ &= [\exp_{N_S}(\sigma(\alpha_S)), w_{N_S}]_{N_S} \\ &= \mathrm{tr}_{N_S/1}[\sigma(\alpha_S), \exp_{N_S}^*(w_{N_S})]\,. \end{aligned}$$

Here, we used the fact that $[A^{-1}x, A^*y]_{N_S} = [x, y]_{N_S}$ for $A \in \mathbf{Q}_p[\mathcal{G}_{N_S}]$ such that $A^{-1}$ exists in $\mathbf{Q}_p[\mathcal{G}_{N_S}]$.

So what we have to prove is that $\mathrm{tr}_{N_S/1}[\sigma(\alpha_S), \exp_{N_S}^* w_{N_S}]_{N_S} \in \mathbf{Z}_p$ for all $\sigma \in \mathcal{G}_N$ and $S \subset S(M)$. But this follows from the fact that $\sigma(\alpha_S)$ is in the image of log because the formal logarithm map is Galois compatible, and the commutativity of the following diagram

$$\begin{array}{ccc} \widehat{E}(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S})) & \times \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S}), T_pE) \to & \mathbf{Z}_p \\ \downarrow \log & \downarrow \exp_{N_S}^* & \downarrow \\ D/D_0 \otimes_{\mathbf{Q}_p} (\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S})) \times D_0 \otimes_{\mathbf{Q}_p} (\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S})) & \to & \mathbf{Q}_p\,. \end{array}$$

where the pairing in the upper row is the composite of the Kummer map $\widehat{E}(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S})) \to \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S}), T_pE)$ and $[\,,\,]_{N_S} : \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S}), T_pE) \times \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S}), T_pE) \to \mathbf{Z}_p$, and the pairing in the lower row is $\mathrm{tr}_{N_S/1}[\,,\,]$. □

For the rest of this section, we will prove that $\upsilon_{p^n}(F_p(\widehat{\sigma}_p)^{-1}\upsilon_{M_S}(\gamma_S))$ is in the image of $\log_{\hat{E}}$ in $\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_{N_S})$ because we have

$$\begin{aligned}\upsilon_{N_S}(F_p(\widehat{\sigma}_p)^{-1}\gamma_S) &= \upsilon_{p^n}(\upsilon_{M_S}(F_p(\widehat{\sigma}_p)^{-1}\gamma_S)) \\ &= \upsilon_{p^n}(F_p(\widehat{\sigma}_p)^{-1}\upsilon_{M_S}(\gamma_S))\,.\end{aligned}$$

Let $v$ be a prime of $\mathbf{Q}(\mu_{M_S})$ dividing $p$, it is easy to show that the diagram below is commutative,

$$\begin{array}{ccc}\mathbf{Q}(\mu_{M_S})[C_{p^n}] & \xrightarrow{\hat{\sigma}_p} & \mathbf{Q}(\mu_{M_S})[C_{p^n}] \\ \downarrow & \circlearrowleft & \downarrow \\ \mathbf{Q}(\mu_{M_S})_v[C_{p^n}] & \xrightarrow{\hat{\sigma}_v} & \mathbf{Q}(\mu_{M_S})_v[C_{p^n}]\,.\end{array}$$

Here, $\widehat{\sigma}_v$ denotes a ring endomorphism of $\mathbf{Q}(\mu_{M_S})_v[C_{p^n}]$ defined by

$$\begin{aligned}\alpha &\mapsto \sigma_v(\alpha) \\ \xi_{p^n} &\mapsto \xi_{p^n}^p\end{aligned}$$

for $\alpha \in \mathbf{Q}(\mu_{M_S})_v$, where $\sigma_v$ denotes the Frobenius automorphism of the unramified extension $\mathbf{Q}(\mu_{M_S})_v/\mathbf{Q}_p$.

Later on, we regard $\upsilon_{M_S}(\gamma_S) \in \mathbf{Q}(\mu_{M_S})_v[C_{p^n}]$ and we will show that $\upsilon_{p^n}(F_p(\widehat{\sigma}_v)^{-1}\upsilon_{M_S}(\gamma_S)) \in \log_{\hat{E}}(m_{\mathbf{Q}(\mu_{N_S})_v})$ by the following arguments.

Let $K$ be a finite unramified extension of $\mathbf{Q}_p$, $\mathcal{O}_K$ its ring of integers, $m_K := p\mathcal{O}_K$ its maximal ideal, $k := \mathcal{O}_K/m_K$ and $\sigma \in \mathrm{Gal}(K/\mathbf{Q}_p)$ the Frobenius automorphism (i.e. $\sigma(x) \equiv x \pmod{p}$ for all $x \in \mathcal{O}_K$). Let $\mathcal{M}_K := (p, T)$ be the maximal ideal of the ring of power series $\mathcal{O}_K[[T]]$.

We define the ring $\mathcal{C}_K$ by $\mathcal{C}_K := \{f(T) \in K[[T]] \mid f(x)$ converges for any $x \in \overline{\mathbf{Q}_p}$ such that $|x|_p < 1\}$, i.e. the ring of power series whose radius of convergence is $\geq 1$. Here, $|\cdot|_p$ is the normalized $p$-adic absolute value.

For each integer $n \geq 1$, let $\mathcal{I}_{K,n}$ be the ideal of $\mathcal{C}_K$ defined by

$$\mathcal{I}_{K,n} := \{f(T) \in \mathcal{C}_K \mid f(\zeta_{p^i} - 1) = 0 \text{ for } i = 0, 1, \ldots, n\}\,.$$

For $f(T) \in K[[T]]$, we define

$$\phi f(T) := \sigma f((1+T)^p - 1)\,.$$

Here, $\sigma f(T) := \sum_{i=0}^{\infty} \sigma(b_i)T^i$ for $f(T) = \sum_{i=0}^{\infty} b_i T^i \in K[[T]]$. Note that we have $\phi\mathcal{I}_{K,n} \subset \mathcal{I}_{K,n}$, so $x \mapsto \phi(x)$ induces a map $\mathcal{C}_K/\mathcal{I}_{K,n} \to \mathcal{C}_K/\mathcal{I}_{K,n}$. It is also denoted by $\phi$.

We define $\widehat{\sigma} : K[C_{p^n}] \to K[C_{p^n}]$ by

$$\alpha \mapsto \sigma(\alpha)$$

$$\xi_{p^n} \mapsto \xi_{p^n}^{p}$$

for $\alpha \in K$.

For $i = 0, 1, \ldots, n$, we define $\psi_i : C_{p^n} \to \mu_{p^n}$ to be a character of $C_{p^n}$ of conductor $p^i$ by $\xi_{p^n} \mapsto \zeta_{p^i}$ and define $\varsigma_i : \mathcal{C}_K \to K(\mu_{p^n})$ by $f(T) \mapsto f(\zeta_{p^i} - 1)$. From the definition of $\mathcal{I}_{K,n}$, we have an injection

$$\begin{array}{rccc} \prod_{i=0}^{n} \varsigma_i : & \mathcal{C}_K/\mathcal{I}_{K,n} & \to & \prod_{i=0}^{n} K(\mu_{p^i}) \\ & f(T) \bmod \mathcal{I}_{K,n} & \mapsto & (f(\zeta_{p^i} - 1))_i \,. \end{array}$$

LEMMA 4.3. *There is an isomorphism*

$$\mathcal{C}_K/\mathcal{I}_{K,n} \simeq K[C_{p^n}]\,,$$

*and the diagrams*

$$\begin{array}{ccc} \mathcal{C}_K/\mathcal{I}_{K,n} & \xrightarrow{\phi} & \mathcal{C}_K/\mathcal{I}_{K,n} \\ \downarrow & \circlearrowleft & \downarrow \\ K[C_{p^n}] & \xrightarrow{\hat{\sigma}} & K[C_{p^n}] \end{array}$$

*and*

$$\begin{array}{ccccc} \varsigma_n : \mathcal{C}_K/\mathcal{I}_{K,n} & \to & K(\mu_{p^n}) \\ \downarrow & \circlearrowleft & \| \\ \upsilon_{p^n} : K[C_{p^n}] & \to & K(\mu_{p^n}) \end{array}$$

*are commutative. Here, the vertical arrows are isomorphisms.*

PROOF. Note that the natural inclusion $K[T] \subset \mathcal{C}_K$ induces an injection $K[T]/((1+T)^{p^n} - 1) \to \mathcal{C}_K/\mathcal{I}_{K,n}$ and comparing the dimensions of $K$-vector spaces $K[T]/((1+T)^{p^n} - 1) \simeq \prod_{i=0}^{n} K(\mu_{p^i})$ and $\mathcal{C}_K/\mathcal{I}_{K,n}$, it is an isomorphism $K[T]/((1+T)^{p^n} - 1) \simeq \mathcal{C}_K/\mathcal{I}_{K,n}$. The ring homomorphism $K[T] \to K[C_{p^n}]$ defined by $1 + T \mapsto \xi_{p^n}$ also induces the isomorphism $K[T]/((1+T)^{p^n} - 1) \simeq K[C_{p^n}]$. So we have an isomorphism $\mathcal{C}_K/\mathcal{I}_{K,n} \simeq K[C_{p^n}]$. It is easy to see that both $\phi$ and $\widehat{\sigma}$ correspond to the ring homomorphism $K[T]/((1+T)^{p^n} - 1) \to K[T]/((1+T)^{p^n} - 1)$ defined by $f(T) \bmod ((1+T)^{p^n} - 1) \mapsto f((1+T)^{p} - 1) \bmod ((1+T)^{p^n} - 1)$, and both $\varsigma_n$ and $\upsilon_{p^n}$ correspond to the ring homomorphism $K[T]/((1+T)^{p^n} - 1) \to K(\mu_{p^n})$ defined by $f(T) \bmod ((1+T)^{p^n} - 1) \mapsto f(\zeta_{p^n} - 1)$. □

Put $K = \mathbf{Q}(\mu_{M_S})_v$ here. Let $\tilde{\gamma}_S(T) \in K[T]$ be a polynomial which corresponds to $\gamma_S \in \mathcal{O}_K[C_{p^n}]$ through the isomorphism above. We can take $\tilde{\gamma}_S(T) \in \mathcal{O}_K[T]$. To prove $\upsilon_{p^n}(F_p(\widehat{\sigma}_v)^{-1}\upsilon_{M_S}(\gamma_S)) \in \log_{\hat{E}}(m_K)$, it is enough to show that there exists $g(T) \in \mathcal{C}_K$ such that $F_p(\phi)g(T) = \tilde{\gamma}_S(T)$ and $g(\zeta_{p^n} - 1) \in \log_{\hat{E}}(m_K)$.

We will prove this by the following arguments, which is an analogue of Coleman's paper [2].

PROPOSITION 4.4. *We have*

$$\left(1-\frac{a_p}{p}\phi+\frac{1}{p}\phi^2\right)\log_{\hat{E}}(\mathcal{M}_K)\subset\mathcal{O}_K[[T]]\,.$$

PROOF. Let $e(T)\in\mathcal{M}_K$. It is easy to see that

$$\phi e(T)\equiv e(T)^p \pmod{p\mathcal{O}_K[[T]]}$$

and for $X, Y\in\mathcal{M}_K$ with $X\equiv Y \pmod{p\mathcal{O}_K[[T]]}$, we have

$$\log_{\hat{E}}(X)\equiv\log_{\hat{E}}(Y) \pmod{p\mathcal{O}_K[[T]]}\,.$$

Thus, we have

$$\phi\log_{\hat{E}}(e(T))\equiv\log_{\hat{E}}(e(T)^p) \pmod{p\mathcal{O}_K[[T]]}\,.$$

From Honda's theory [3] section 6, we have

$$\log_{\hat{E}}(X^{p^2})-a_p\log_{\hat{E}}(X^p)+p\log_{\hat{E}}(X)\equiv 0 \pmod{p\mathcal{O}_K[[T]]}\,.$$

Combining all the above, we obtain

$$\begin{aligned}(p-a_p\phi+\phi^2)\log_{\hat{E}}(e(T)) &\equiv p\log_{\hat{E}}(e(T))-a_p\log_{\hat{E}}(e(T)^p)+\log_{\hat{E}}(e(T)^{p^2})\\ &\equiv 0 \pmod{p\mathcal{O}_K[[T]]}\,.\end{aligned}$$

Dividing the equation by $p$, we obtain $(1-\frac{a_p}{p}\phi+\frac{1}{p}\phi^2)\log_{\hat{E}}(e(T))\in\mathcal{O}_K[[T]]$. □

PROPOSITION 4.5. *Assume that $\widetilde{E}(k)[p]=0$. Then we have*

$$\left(1-\frac{a_p}{p}\phi+\frac{1}{p}\phi^2\right)\log_{\hat{E}}(\mathcal{M}_K)=\mathcal{O}_K[[T]]\,.$$

PROOF. Since we have $\mathcal{M}_K=m_K+_{\hat{E}}T\mathcal{O}[[T]]$ where $+_{\hat{E}}$ is the formal group law of the formal group $\widehat{E}$, it is enough to show that $(1-\frac{a_p}{p}\phi+\frac{1}{p}\phi^2)\log_{\hat{E}}(m_K)=\mathcal{O}_K$ and $(1-\frac{a_p}{p}\phi+\frac{1}{p}\phi^2)\log_{\hat{E}}(T\mathcal{O}_K[[T]])=T\mathcal{O}_K[[T]]$ separately.

First, we will show that $(1-\frac{a_p}{p}\phi+\frac{1}{p}\phi^2)\log_{\hat{E}}(T\mathcal{O}_K[[T]])=T\mathcal{O}_K[[T]]$. It is enough to show that for each $i\geq 1$, the induced map $T^i\mathcal{O}_K[[T]]\to T^i\mathcal{O}_K[[T]]/T^{i+1}\mathcal{O}_K[[T]]$ by $(1-\frac{a_p}{p}\phi+\frac{1}{p}\phi^2)\log_{\hat{E}}$ is surjective. Since we have

$$\left(1-\frac{a_p}{p}\phi+\frac{1}{p}\phi^2\right)\log_{\hat{E}}(\alpha T^i)=(\alpha-a_pp^{i-1}\alpha^{\sigma}+p^{2i-1}\alpha^{\sigma^2})T^i+r(T)$$

with $r(T)\in T^{i+1}\mathcal{O}_K[[T]]$ for each $\alpha\in\mathcal{O}_K$, it is enough to show the surjectivity of the map

$$\begin{aligned}&\mathcal{O}_K\to\mathcal{O}_K\\ &\quad\alpha\mapsto\alpha-a_pp^{i-1}\alpha^{\sigma}+p^{2i-1}\alpha^{\sigma^2}.\end{aligned}$$

Since the above map is $\mathbf{Z}_p$-linear, it is enough to show that the map mod $p$ is surjective by Nakayama's lemma.

If $i \geq 2$, then the map mod $p$ is the identity map $\alpha \mapsto \alpha$. If $i = 1$, the map mod $p$ is

$$\begin{aligned} k &\to k \\ \alpha &\mapsto \alpha - \overline{a_p}\alpha^p \,. \end{aligned}$$

Here $\overline{a_p}$ is the image of $a_p \in \mathbf{Z}$ under the natural map $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} \simeq \mathbf{F}_p$. Note that $\alpha^\sigma \equiv \alpha^p \pmod{p}$.

Since $k$ is a finite field, the surjectivity is equivalent to the injectivity of the map mod $p$. We will prove the injectivity.

Suppose that the map mod $p$ is not injective. Then, there exists a non-zero element $\alpha \in k$ such that $\alpha = \overline{a_p}\alpha^p$. Since we have $\overline{a_p}^p = \overline{a_p}$, we have

$$\alpha = \overline{a_p}\alpha^p = \overline{a_p}^2\alpha^{p^2} = \cdots = \overline{a_p}^d\alpha^{p^d} = \overline{a_p}^d\alpha \,,$$

where $d = [k : \mathbf{F}_p]$. Since $\alpha \neq 0$, we have $\overline{a_p}^d = 1$ in $\mathbf{F}_p$.

We will show that the assumption $\widetilde{E}(k)[p] = 0$ implies that $a_p^d \not\equiv 1 (\mathrm{mod}\ p)$. From basic facts about elliptic curves over finite field, we get $\#\widetilde{E}(k) = p^d - \alpha_p^d - \beta_p^d + 1$, where $\alpha_p, \beta_p$ are two roots of the equation $T^2 - a_pT + p = 0$. Since $\alpha_p + \beta_p = a_p$ and $\alpha_p\beta_p = p$, we obtain

$$\begin{aligned} \alpha_p^d + \beta_p^d &\equiv (\alpha_p + \beta_p)^d \pmod{p} \\ &= a_p^d. \end{aligned}$$

Thus, we get $a_p^d - 1 \equiv -p^d + \alpha_p^d + \beta_p^d - 1 = -\#\widetilde{E}(k) \not\equiv 0 \pmod{p}$ and we have proved that $(1 - \frac{a_p}{p}\phi + \frac{1}{p}\phi^2)\log_{\hat{E}}(T\mathcal{O}_K[[T]]) = T\mathcal{O}_K[[T]]$.

Next, we will show that $(1 - \frac{a_p}{p}\phi + \frac{1}{p}\phi^2)\log_{\hat{E}}(m_K) = \mathcal{O}_K$. First, we will show that the assumption $\widetilde{E}(k)[p] = 0$ implies that $\log_{\hat{E}}(x) \equiv x \pmod{p^{i+1}}$ for $x \in p^i\mathcal{O}_K$ and for $i \geq 1$. From basic properties of $\log_{\hat{E}}$, we see that for $x \in \overline{\mathbf{Q}_p}$ such that $\mathrm{ord}_p(x) > \frac{1}{p^h-1}$, we have $\log_{\hat{E}}(x) \equiv x \pmod{\{y \in \overline{\mathbf{Q}_p} | \mathrm{ord}_p(y) > \mathrm{ord}_p(x)\}}$, where $h$ is the height of the formal group $\widehat{E}$ and $\mathrm{ord}_p$ is the normalized $p$-adic valuation. So, it is enough to show that $\frac{1}{p^h-1} < 1$. If $p \geq 3$, then it is obvious. If $p = 2$, then the assumption $\widetilde{E}(k)[2] = 0$ implies that $E$ is supersingular at 2. Since the height of the formal group $\widehat{E}$ is 2, $\frac{1}{p^h-1} = \frac{1}{2^2-1} = \frac{1}{3} < 1$. Thus, we have proved the statement.

Let $j \in \mathbf{Z}$, $j \geq 1$ and $u \in \mathcal{O}_K$. We compute

$$\left(1 - \frac{a_p}{p}\phi + \frac{1}{p}\phi^2\right)\log_{\hat{E}}(p^j u) \equiv -a_p p^{j-1}u^\sigma + p^{j-1}u^{\sigma^2} \pmod{p^j} \,.$$

To prove the surjectivity of the map $(1-\frac{a_p}{p}\phi+\frac{1}{p}\phi^2)\log_{\hat{E}} : m_K \to \mathcal{O}_K$, it is enough to show the surjectivity of the induced map $p^j\mathcal{O}_K \to p^{j-1}\mathcal{O}_K/p^j\mathcal{O}_K$ for each $j \geq 1$. But by the similar arguments as above, the induced map is essentially

$$\begin{aligned} k &\to k \\ u &\mapsto -\overline{a_p}u^p + u^{p^2}, \end{aligned}$$

and we can show that it is injective, hence surjective.

Thus, we have proved the lemma. □

Let $e_S(T) \in \mathcal{O}_{\mathbf{Q}(\mu_M)_v}[[T]]$ be an power series satisfying

$$\left(1-\frac{a_p}{p}\phi+\frac{1}{p}\phi^2\right)\log_{\hat{E}}(e_S(T)) = \tilde{\gamma}_S(T)\,.$$

Then, from the arguments above,

$$\upsilon_{p^n}(F_p(\widehat{\sigma}_p)^{-1}\upsilon_{M_S}(\gamma_S)) = \log_{\hat{E}}(e_S(\zeta_{p^n}-1)) \in \log_{\hat{E}}(\mathbf{Q}(\mu_{N_S})_v)\,.$$

It is in the image of $\log_{\hat{E}}$. This is what we wanted to show.

## References


[1] BLOCH, S. and KATO, K.: $L$-functions and Tamagawa number of motives, in *Grothendieck Festschrift* (Vol. I), Prog. in Math. **86** (1990), 333–400.

[2] COLEMAN, R.: Division values in local fields, Invent. Math. **53** (1979), 91–116.

[3] HONDA, T.: On the theory of commutative formal groups, J. Math. Soc. Japan **22** (1970), 213–246.

[4] KATO, K.: $p$-adic Hodge theory and values of zeta functions of modular forms, Astérisque vol. **295** (2004), 117–290.

[5] KOBAYASHI, S.: Iwasawa theory for elliptic curves at supersingular primes, Invent. Math. **152** (2003), 1–36.

[6] KURIHARA, M.: On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction, I, Invent. Math. **149** (2002), 195–224.

[7] KURIHARA, M. and POLLACK, R.: Two $p$-adic $L$-functions and rational points on elliptic curves with supersingular reduction, London Math. Soc. Lecture Note Series **320** (2007), 300–332.

[8] MAZUR, B. and TATE, J.: Refined conjectures of the "Birch and Swinnerton-Dyer type", Duke Math. J. vol. **54**, No. 2 (1987), 711–750.

[9] MAZUR, B., TATE, J. and TEITELBAUM, J.: On $p$-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. Math. **84** (1986), 1–48.

[10] PERRIN-RIOU, B.: Fonctions $L$ $p$-adiques d'une courbe elliptique et points rationnels, Ann. Inst. Fourier **43**, 4 (1993), 945–995.



*Present Address*:
CENTER FOR MATHEMATICS, SCHOOL OF FUNDAMENTAL SCIENCE AND TECHNOLOGY,
GRADUATE SCHOOL OF SCIENCE AND TECHNOLOGY,
KEIO UNIVERSITY,
HIYOSHI, KOHOKU-KU, YOKOHAMA-SHI, KANAGAWA, 223–8522 JAPAN.
*e-mail*: ray_otsuki@math.keio.ac.jp