On the modular elements and the Euler systems for an elliptic curve

Rei Otsuki

Contents

1 Introduction **3**

1.1 Arithmetic of elliptic curves, the modular elements and Euler systems . . . 3

1.2 Results of this paper . . . 5

1.2.1 Selmer groups of an elliptic curve with supersingular reduction in the cyclotomic $\mathbf{Z}_2$-extension . . . 5

1.2.2 Homomorphisms concerning Euler systems . . . 8

2 Iwasawa theory for elliptic curves with supersingular reduction **14**

2.1 The Selmer groups in the $\mathbf{Z}_2$-extension of $\mathbf{Q}$ . . . 14

2.2 The modular elements . . . 16

2.3 The zeta elements . . . 17

2.4 Proof of the theorem . . . 18

2.4.1 Conductor . . . 18

2.4.2 Formal groups . . . 19

2.4.3 The behavior of the modular elements . . . 21

2.4.4 The Selmer groups and cohomology groups . . . 22

2.4.5 The Selmer groups and the zeta elements . . . 27

2.4.6 The Selmer groups and the modular elements . . . 29

3 A homomorphism concerning the zeta elements and the modular elements **38**

3.1 Theorems . . . 38

3.2 Group rings . . . 39

3.3 Definition of the map . . . 41

3.4 Euler systems and admissible systems . . . 50

3.5 Integrality of the map . . . 56

3.6 Kernel of the map 64

Chapter 1

Introduction

1.1 Arithmetic of elliptic curves, the modular elements and Euler systems

In the arithmetic of elliptic curves, arithmetic objects such as Mordell-Weil groups, Selmer groups and Tate-Shafarevich groups have been studied by many mathematicians. There are several interesting conjectures about the relation between the structures of these arithmetic objects and the special values of L-functions of an elliptic curve. One is the Birch Swinnerton-Dyer conjecture, which states that the order of vanishing of the L-function is equal to the rank of the Mordell-Weil group, and some important arithmetic invariants appear in the leading term of the L-function. Another is the Iwasawa Main Conjecture, which states that the structure of the Selmer group of a certain infinite extension is dominated by a p-adic L-function which interpolates the special values of the L-function. There is also a difficult conjecture that the Tate-Shafarevich groups are finite.

There are some important elements which are related to the above conjectures. In 1987, Mazur and Tate [12] defined the modular element for the maximal real subfield $\mathbf{Q}(\mu_N)^+$ of the cyclotomic field $\mathbf{Q}(\mu_N)$ and for modular elliptic curves defined over the field $\mathbf{Q}$. They formulated some conjectures as "refined" Birch Swinnerton-Dyer conjecture without p-adic L-function, which states that the modular elements are related to the structure of the Selmer group over the field $\mathbf{Q}(\mu_M)^+$. The modular elements are related to the special values of the L-function of the elliptic curve E, and by taking p-adic limits of the modular elements, we can obtain the p-adic L-function

of E.

On the other hand, around 1990, a new method was developed to study arithmetic objects such as the ideal class group of an algebraic number field or the Tate-Shafarevich group of an elliptic curve, by using a system of elements which satisfy formulas involving the Euler factors of the Riemann zeta function or the Hasse-Weil L-function of the elliptic curve. These systems were named Euler systems. Kolyvagin [9] and Rubin proved that Tate-Shafarevich groups of certain elliptic curves are finite using the Euler system coming from the Heegner points (see also Rubin [16] [17]).

In the 1990's, Kato [7] constructed a new Euler system of a modular form for cyclotomic fields in cohomology groups, which is called the zeta elements. By using this Euler system, he obtained significant results about the Selmer groups, such as the Λ-cotorsionness of the Selmer groups and a partial result of the Iwasawa Main Conjecture for modular forms. The zeta elements are related to the special values of the L-functions. Moreover, it was proved that the image of the system of the zeta elements in the ordinary case for $\mathbf{Q}(\mu_{Np^\infty})$ through the Perrin-Riou's homomorphism is essentially the p-adic L-function.

Now that we know every elliptic curve defined over the field $\mathbf{Q}$ is modular, the modular elements and the zeta elements are defined for every elliptic curve over $\mathbf{Q}$ (See [1]).

The relation between the two elements had not been studied. The first result on the relation between the two systems was Kurihara's result when he studied the Selmer groups in the supersingular case. 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 nice integrality. He used the above correspondence to determine the structure of the Selmer groups in the simplest case, and showed that the modular elements are in the Fitting ideal of the Selmer groups, which was conjectured by Mazur and Tate. He also showed that the behavior of the orders of the Tate-Shafarevich groups in the supersingular case is different from that in the ordinary case.

The purpose of this paper is to study the relation between the modular elements and the zeta elements in general. For an elliptic curve E 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 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.

We will also prove the similar result to the above Kurihara's result about the Selmer groups, in the case when $p = 2$. Namely, we will determine the structures of the Selmer groups of elliptic curves with supersingular reduction at 2 in the simplest case. But this case has a difference that the corank of the Selmer groups is positive while the Selmer groups are finite in Kurihara's result for odd prime number p.

1.2 Results of this paper

Let E be an elliptic curve defined over $\mathbf{Q}$ and let $f(z) = \sum_{n=1}^{\infty} a_n q^n$ be the cusp form of weight 2 corresponding to E. We will introduce the results of this paper.

1.2.1 Selmer groups of an elliptic curve with supersingular reduction in the cyclotomic $\mathbf{Z}_2$-extension

The purpose of this paper is to study the correspondence between the modular elements and the zeta elements, and we first introduce the results obtained from the correspondence. We will generalize the correspondence in Chapter 3.

In Chapter 2, we will prove the following theorem about the structures of the Selmer groups in the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}$ for an elliptic curve with supersingular reduction in the simplest case, using the zeta elements and the modular elements. The following theorems show that the behavior of the Selmer groups in the supersingular case is different from that in the ordinary case.

Theorem 1.2.1 (Theorem 2.1.1)**.** *Let $\mathbf{Q}_\infty/\mathbf{Q}$ be the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}$ and $\mathbf{Q}_n$ be its n-th layer. We assume that $a_2 \neq 0$, namely $a_2 = \pm 2$, and*

$$\mathrm{ord}_2(L(E,1)/\Omega_E) = \mathrm{ord}_2(\mathrm{Tam}(E)) = 0$$

where $\mathrm{ord}_2 : \mathbf{Q}^\times \to \mathbf{Z}$ is the normalized additive valuation at 2. Then,

1. *For any $n \geq 0$, let $\theta_{\mathbf{Q}_n}$ be the modular element. Suppose $n \geq 1$. Then, the Pontrjagin dual $\mathrm{Sel}(E/\mathbf{Q}_n)^\vee$ of the Selmer group over $\mathbf{Q}_n$ with respect to $E[2^\infty]$ is isomorphic to*

$$\mathbf{Z}_2[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]/(\theta_{\mathbf{Q}_n}, \nu_n(\theta_{\mathbf{Q}_{n-1}}))$$

as $\mathbf{Z}_2[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$-modules.

2. *For $n \geq 2$, put*

$$q_n = \sum_{k=0}^{n-1} (-1)^k 2^{n-1-k} = \frac{1}{3}(2^n - (-1)^n).$$

Then, we have $\mathrm{Sel}(E/\mathbf{Q}) = 0, \mathrm{Sel}(E/\mathbf{Q}_1) \cong \mathrm{Sel}(E/\mathbf{Q}_2) \cong \mathbf{Q}_2/\mathbf{Z}_2$ as abelian groups, and

$$\mathrm{Sel}(E/\mathbf{Q}_n) = \mathbf{Q}_2/\mathbf{Z}_2 \oplus (\mathbf{Z}/2^{n-2}\mathbf{Z})^{q_3-q_2} \oplus (\mathbf{Z}/2^{n-3}\mathbf{Z})^{q_4-q_3} \oplus \cdots \oplus (\mathbf{Z}/2\mathbf{Z})^{q_n-q_{n-1}}$$

for all $n \geq 3$. Hence, if we assume the finiteness of the 2-primary component of the Tate-Shafarevich group $Ш(E/\mathbf{Q}_1)[2^\infty]$, we have

$$\begin{gathered}\mathrm{rank}\ E(\mathbf{Q}_n) = 1 \text{ for all } n \geq 1, \\ Ш(E/\mathbf{Q}_1)[2^\infty] = Ш(E/\mathbf{Q}_2)[2^\infty] = 0, \text{ and} \\ Ш(E/\mathbf{Q}_n)[2^\infty] \cong (\mathbf{Z}/2^{n-2}\mathbf{Z})^{q_3-q_2} \oplus (\mathbf{Z}/2^{n-3}\mathbf{Z})^{q_4-q_3} \oplus \cdots \oplus (\mathbf{Z}/2\mathbf{Z})^{q_n-q_{n-1}}\end{gathered}$$

for all $n \geq 3$.

3. $\mathrm{Sel}(E/\mathbf{Q}_\infty)^\vee \cong \mathbf{Z}_2[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$.

The above theorem is an analogue of the following Kurihara's theorem [10] for odd prime number p.

Theorem 1.2.2 (Kurihara)**.** *Let p be an odd prime and assume that E has supersingular reduction at p, $\mathrm{ord}_p \frac{L(E,1)}{\Omega_E} = \mathrm{ord}_p \mathrm{Tam}(E) = 0$, and the Galois action*

$$\rho_{E[p]} : G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbf{F}_p)$$

is surjective. Let $\mathbf{Q}_\infty/\mathbf{Q}$ *be the cyclotomic* $\mathbf{Z}_p$*-extension of* $\mathbf{Q}$ *and* $\mathbf{Q}_n$ *be its* n*-th layer. Then, for all* $n \geq 1$

$$\begin{aligned} \text{rank } E(\mathbf{Q}_n) &= 0 \\ \text{Sel}(E/\mathbf{Q}_n) &= Ш(E/\mathbf{Q}_n)[p^\infty] \end{aligned}$$

and

1. $\text{Sel}(E/\mathbf{Q}_n)^\vee \simeq \mathbf{Z}_p[\text{Gal}(\mathbf{Q}_n/\mathbf{Q})]/(\theta_{\mathbf{Q}_n}, \nu_n(\theta_{\mathbf{Q}_{n-1}}))$ $\quad (n \geq 1)$
   as $\mathbf{Z}_p[\text{Gal}(\mathbf{Q}_n/\mathbf{Q})]$*-modules.*
2. *Put*

$$q_n = \begin{cases} p^{n-1} - p^{n-2} + p^{n-3} - p^{n-4} + \ldots + p - 1 & (\textit{for even } n \geq 2) \\ p^{n-1} - p^{n-2} + p^{n-3} - p^{n-4} + \ldots + p^2 - p & (\textit{for odd } n \geq 3) \end{cases}$$

   then

$$\begin{aligned} \text{Sel}(E/\mathbf{Q}) &= \text{Sel}(E/\mathbf{Q}_1) = 0 \\ \text{Sel}(E/\mathbf{Q}_n) &\simeq (\mathbf{Z}/p^{n-1}\mathbf{Z})^{q_2} \oplus (\mathbf{Z}/p^{n-2}\mathbf{Z})^{q_3 - q_2} \oplus \cdots \oplus (\mathbf{Z}/p\mathbf{Z})^{q_n - q_{n-1}} \\ &\quad (\textit{for all } n \geq 2) \end{aligned}$$

   as abelian groups.
3. $\text{Sel}(E/\mathbf{Q}_\infty)^\vee \simeq \mathbf{Z}_p[[\text{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$ (*as* $\mathbf{Z}_p[[\text{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$*-modules*).

Although the zeta elements did not appear explicitly in the above statements, the proofs of the above theorems are based on the behavior of the modular elements and the zeta elements. An important part of the proof is to prove that the modular elements annihilate the dual of the Selmer groups $\text{Sel}(E/\mathbf{Q}_n)^\vee$, which is proved by using certain homomorphism which sends the zeta element to the modular element. This homomorphism will be discussed in Chapter 3 of this paper in more general situations.

We will make some remarks about the difference between the ordinary case and the supersingular case.

In the ordinary case, we have the following theorem.

Theorem 1.2.3 (Mazur)**.** *Let* F *be a number field, and let* p *be a prime number. Let* F_∞/F *be the cyclotomic* $\mathbf{Z}_p$*-extension and* F_n *its* n*-th layer. Put* $\Lambda := \mathbf{Z}_p[[\text{Gal}(F_\infty/F)]]$*. Assume that* E *has good ordinary reduction at all primes of* F *lying over* p*. Assume that* $\text{Sel}(E/F_\infty)$ *is* Λ*-cotorsion and that* $Ш(E/F_n)$ *is finite for all* $n \geq 0$*. Then there exist* $\lambda, \mu, \nu \in \mathbf{Z}$ *such that* $\sharp Ш(E/F_n)[p^\infty] = p^{e_n}$*, where* $e_n = \lambda n + \mu p^n + \nu$ *for all* $n \gg 0$*.*

This is an analogue of Iwasawa's class number formula. This is proved by Mazur's Control theorem.

Remark 1.2.4.

1. The assumption that $\mathrm{Sel}(E/F_\infty)$ is Λ-cotorsion is believed to be always true in the ordinary case. More precisely, there exists the following conjecture.

Conjecture 1.2.5. For every prime number p,

$$\mathrm{rank}_\Lambda \mathrm{Sel}(E/F_\infty)^\vee = \sum_v [F_v : \mathbf{Q}_p].$$

Here, v runs through all the primes above p such that E has potential supersingular reduction at v.

This conjecture is proved in some cases, for example, it was proved by Kato that this holds for $F = \mathbf{Q}$. But 3. of Theorem 1.2.1 and Theorem 1.2.2 in the supersingular case show that $\mathrm{Sel}(E/\mathbf{Q}_\infty)$ is not Λ-cotorsion.

2. The structures of the Tate-Shafarevich groups have been rarely determined, but in the above theorems, the structures of the Selmer groups as abelian groups are determined.

3. We know that the orders of the Tate-Shafarevich groups from the structures of the Tate-Shafarevich groups. The above theorems show that the growth of the orders of the Tate-Shafarevich groups is different from that in the ordinary case.

4. Concerning the structure of the Selmer groups as Galois modules, Mazur and Tate [12] conjectured that the modular element is in the Fitting ideal of the Pontrjagin dual of the Selmer group. From above theorems, the Fitting ideal of the Pontrjagin dual of the Selmer group $\mathrm{Sel}(E/\mathbf{Q}_n)$ is proved to be $(\theta_{\mathbf{Q}_n}, \nu_n(\theta_{\mathbf{Q}_{n-1}}))$. Hence, we have also proved that the conjecture of Mazur and Tate holds in the above case.

1.2.2 Homomorphisms concerning Euler systems

In Chapter 3, we will construct a 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, and study the homomorphism. Here, $V_pE = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} T_pE$,

where T_pE is the Tate module, and $\mathcal{G}_N := \mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q})$. The main result of Chapter 3 is the construction of this homomorphism $\mathcal{P}_N$. This homomorphism $\mathcal{P}_N$ is defined in §3.3. We will also study some important properties of $\mathcal{P}_N$.

We make a very rough sketch of the construction. As we will see in Chapter 3, the homomorphism $\mathcal{P}_N$ is defined, using a certain pairing

$$P_N : D/D^0 \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N) \times \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N), V_pE) \to \mathbf{Q}_p[\mathcal{G}_N]$$

and a special element $x_N \in D/D^0 \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N)$. The construction of the element x_N is the main part of the construction of the homomorphism $\mathcal{P}_N$.

Kurihara first constructed such a homomorphism in [10] in the case when $N = p^n$ for a positive integer n and when the elliptic curve E has supersingular reduction at p, inspired by Perrin-Riou's work [14], in which it was proved that the p-adic L-function is the image of the Kato's Euler system through a certain homomorphism.

Our homomorphism $\mathcal{P}_N$ with $N = p^n$ 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 [8]. 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.

From the definition of Euler systems described below, in the case in which Kurihara and Kobayashi studied, the system of the zeta elements $(z_{p^n})_{n\geq 1}$ is only a norm compatible system (see the upper half of the formulas (1.1) of Euler systems), but we will study general relations between Euler systems, which is the main difference between this paper and their works.

We will introduce two systems related to the above homomorphism. One is an admissible system. We will introduce the notion of the admissible system in this paper. The other is an Euler system.

The modular elements and an admissible system

We will introduce the modular elements defined by Mazur and Tate [12], and the compatible formulas which the modular elements satisfy.

For $N \geq 1$, let $\mathcal{G}_N := \mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q})$. Mazur-Tate [12] defined the modular elements. We define the modular element θ_N by

$$\theta_N := \sum_{a \in (\mathbf{Z}/N\mathbf{Z})^\times} ([\frac{a}{N}]_E^+ + [\frac{a}{N}]_E^-)\sigma_a \in \mathbf{Q}[\mathcal{G}_N].$$

This definition is slightly different from the original work of Mazur and Tate. 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 and $\Omega_E^{\pm}$ are Néron periods. From Manin-Drinfeld theorem, we know $[r]_E^{\pm} \in \mathbf{Q}$.

They are related to the special values of the L-functions as follows.

Proposition 1.2.6 (Mazur, Tate)**.** *Let χ be a character of conductor N and let $\tau(\chi) := \sum_{\sigma \in \mathcal{G}_N} \chi(\sigma)\sigma(\zeta_N)$ be the Gauss sum. Then we have*

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

For each prime number q, they satisfy compatible formulas below

$$\pi_{qM/M}(\theta_{qM}) = \begin{cases} a_q\theta_M - \epsilon_q \nu_{M/\frac{M}{q}}(\theta_{\frac{M}{q}}) & (q \mid M) \\ (a_q - \sigma_q - \epsilon_q\sigma_q^{-1})\theta_M & (q \nmid M). \end{cases}$$

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

The zeta elements and an Euler system

On the other hand, 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

$$\mathrm{Nr}_{qM/M}(w_{qM}) = \begin{cases} w_M & (q \mid M) \\ F_q(\sigma_q^{-1})w_M & (q \nmid M) \end{cases} \tag{1.1}$$

for a prime number q and a positive integer M. Here $F_q(T) := 1 - \frac{a_q}{q}T + \frac{\epsilon_q}{q}T^2$ is the polynomial in Definition 3.2.2, where $\epsilon_q = 1$ (resp. 0) if q is a good prime (resp. bad prime).

In [7], Kato constructed an Euler system in the cohomology groups

$$\mathrm{H}^1(\mathbf{Z}[\mu_N, \frac{1}{S}], V_pE) = \mathrm{H}^1_{et}(\mathrm{Spec}\mathbf{Z}[\mu_N, \frac{1}{S}], V_pE)$$

using Beilinson elements in the K-groups. Here $\mathrm{H}^1_{et}(\mathrm{Spec}\mathbf{Z}[\mu_N, \frac{1}{S}], V_pE)$ is an étale cohomology group (or a Galois cohomology group) 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 $\mathrm{H}^1(\mathbf{Z}[\mu_N, \frac{1}{S}], V_pE) \to \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_N), V_pE)$.

The zeta elements are related to the special values of the L-function as follows.

Proposition 1.2.7 (Kato)**.** *Let χ 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*

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

Here, $\exp^*_N$ is the dual exponential map, $\omega = \omega_E$ is the Néron differential and $\Omega^{\pm}_E$ are Néron periods.

The properties of the homomorphism $\mathcal{P}_N$

We will prove the following three theorems, which state the important properties of the homomorphism $\mathcal{P}_N$. The theorems were proved by Kurihara [10] in the case when $N = p^n$ for odd supersingular prime p. The first theorem states that Euler systems correspond to admissible systems through the homomorphisms $\mathcal{P}_N$. The second theorem states that as a special case of the correspondence, the zeta element corresponds to the modular element. The third theorem is about a nice integral property of the homomorphism.

First, we will introduce two theorems.

Theorem 1.2.8 (Theorem 3.4.1)**.** *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.*

In other words, the system of the homomorphisms $(\mathcal{P}_M)_M$ constructed in this paper sends Euler systems to admissible systems. As we have mentioned, we have a special Euler system and a special admissible system, namely the system of the zeta elements and the system of the modular elements. The system of the zeta elements corresponds to the system of the modular elements through the homomorphisms.

Theorem 1.2.9 (Theorem 3.4.3)**.** *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*

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

The first theorem will be proved by showing that the system $(x_M)_M$ in the definition of $\mathcal{P}_N$ satisfies some formulas, and we will prove that the formulas of admissible systems are obtained by combining the formulas of $(x_M)_M$ and the formulas of Euler systems. Thus, Euler systems correspond to admissible systems. The second theorem will be proved by the relations between the special values of L-function and each elements.

We have introduced the correspondence between Euler systems and admissible systems. The next statement is the most important property of the correspondence. We will introduce the last theorem in Chapter 3, which states that the homomorphism has a nice integral property in many cases.

Theorem 1.2.10 (Theorem 3.5.1)**.** *If p divides N, $\widetilde{E}(\mathbf{F}_p(\mu_N))[p] = 0$ and an Euler system $(w_M)_M$ is integral, namely*

$$(w_M)_M \in \prod_{M|N} \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_M), T_pE),$$

then the admissible system $(\mathcal{P}_M(w_M))_M$ is integral, 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 above integral property was important in the results about the Selmer groups, because the Selmer groups are $\mathbf{Z}_p$-modules but not $\mathbf{Q}_p$-modules.

Proving the integrality is the longest part of this paper. The proof is based on the study of the image of the formal logarithm map of the elliptic curve E. In the supersingular case, the proof was easier since the height of the formal logarithm map is 2. But the height is 1 in the ordinary case, so the arguments in [10] can not be applied. We will use the similar arguments to the result of Coleman [4] to study the formal logarithm map.

We will also determine the kernel of the homomorphism $\mathcal{P}_{p^n}$ where p is a supersingular prime, which will be used in Chapter 2.

Unfortunately, we have not yet obtained results about the Selmer groups like the theorem in Chapter 2, or Kurihara [10] in more general case. But we hope that the homomorphism will be used to study the structures of the Selmer groups.

Acknowledgement

I would like to express my sincere gratitude to my supervisor Professor Masato Kurihara for his warm encouragement and invaluable advices.

Chapter 2

Iwasawa theory for elliptic curves with supersingular reduction

2.1 The Selmer groups in the $\mathbf{Z}_2$-extension of $\mathbf{Q}$

Let E be an elliptic curve defined over $\mathbf{Q}$. If E has good ordinary reduction at a prime p, the growth of Tate-Shafarevich groups (and Selmer groups) of E in a $\mathbf{Z}_p$-extension can be understood by usual Iwasawa theory. But if E has supersingular reduction at p, the growth of Selmer and Tate-Shafarevich groups is more complicated. For an odd prime p, the most basic case was dealt with in Kurihara [10] where the main assumption was that p does not divide the L-value $L(E,1)/\Omega_E$ (where Ω_E is the Néron period). The aim of this chapter is to study the case $p = 2$ under the same assumption on the L-value, namely $2 \nmid L(E,1)/\Omega_E$.

For a prime number p, we consider the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty/\mathbf{Q}$ whose n-th layer we denote by $\mathbf{Q}_n$, namely $\mathbf{Q}_n$ is the intermediate field with $[\mathbf{Q}_n : \mathbf{Q}] = p^n$. For an odd p, the condition $p \nmid L(E,1)/\Omega_E$ implies $\mathrm{rank}E(\mathbf{Q}_\infty) = 0$ (see [10]), but for $p = 2$ this does not hold. We will see that for $p = 2$ the condition $p = 2 \nmid L(E,1)/\Omega_E$ would imply that the Selmer groups over $\mathbf{Q}_n$ always have positive corank for $n \geq 1$, hence would imply $\mathrm{rank}E(\mathbf{Q}_n) > 0$ if we assume the Birch and Swinnerton-Dyer conjecture. So the situation is different.

As usual, put $a_p = p + 1 - \#E(\mathbf{F}_p)$. In the following, we suppose $p = 2$ and E has good supersingular reduction at 2. When $a_2 = 0$, we have two nice Iwasawa functions which describe the p-adic L-function of E by Pollack [15], and we can define $\pm$ Selmer groups as in Kobayashi [8], and can study them by the same method as for $p > 2$. In this chapter, we consider the case $a_2 \neq 0$ (so $a_2 = \pm 2$). Let $\mathrm{Sel}(E/\mathbf{Q}_n)$ be the Selmer group of E over $\mathbf{Q}_n$ of $E[2^\infty]$. We will determine the Galois module structure (and the structure as an abelian group) of $\mathrm{Sel}(E/\mathbf{Q}_n)$ completely in the case $a_2 = \pm 2$ under the assumption $2 \nmid L(E,1)/\Omega_E$, in particular $\mathrm{Sel}(E/\mathbf{Q}_n)$ is of corank 1. (When $a_2 = 0$, the condition $2 \nmid L(E,1)/\Omega_E$ does not determine the structure of $\mathrm{Sel}(E/\mathbf{Q}_n)$ as an abelian group.)

Our main assumption is just $2 \nmid L(E,1)/\Omega_E$. If the Birch and Swinnerton-Dyer conjecture is true, this would imply that 2 does not divide the Tamagawa factor $\mathrm{Tam}(E) = \Pi c_\ell = \Pi(E(\mathbf{Q}_\ell) : E_0(\mathbf{Q}_\ell))$ (where $E_0(\mathbf{Q}_\ell)$ is the subgroup consisting of points whose images in $E(\mathbf{F}_\ell)$ are nonsingular.) We will prove

Theorem 2.1.1. *We assume that $a_2 \neq 0$, namely $a_2 = \pm 2$, and*

$$\mathrm{ord}_2(L(E,1)/\Omega_E) = \mathrm{ord}_2(\mathrm{Tam}(E)) = 0$$

where $\mathrm{ord}_2 : \mathbf{Q}^\times \to \mathbf{Z}$ is the normalized additive valuation at 2. Then,

1. *For any $n \geq 0$, let $\theta_{\mathbf{Q}_n}$ be the modular element. Suppose $n \geq 1$. Then, the Pontrjagin dual $\mathrm{Sel}(E/\mathbf{Q}_n)^\vee$ of the Selmer group over $\mathbf{Q}_n$ with respect to $E[2^\infty]$ is isomorphic to*

$$\mathbf{Z}_2[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]/(\theta_{\mathbf{Q}_n}, \nu_n(\theta_{\mathbf{Q}_{n-1}}))$$

   as $\mathbf{Z}_2[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$-modules.

2. *For $n \geq 2$, put*

$$q_n = \sum_{k=0}^{n-1} (-1)^k 2^{n-1-k} = \frac{1}{3}(2^n - (-1)^n).$$

   Then, we have $\mathrm{Sel}(E/\mathbf{Q}) = 0, \mathrm{Sel}(E/\mathbf{Q}_1) \cong \mathrm{Sel}(E/\mathbf{Q}_2) \cong \mathbf{Q}_2/\mathbf{Z}_2$ as abelian groups, and

$$\mathrm{Sel}(E/\mathbf{Q}_n) = \mathbf{Q}_2/\mathbf{Z}_2 \oplus (\mathbf{Z}/2^{n-2}\mathbf{Z})^{q_3 - q_2} \oplus (\mathbf{Z}/2^{n-3}\mathbf{Z})^{q_4 - q_3} \oplus \cdots \oplus (\mathbf{Z}/2\mathbf{Z})^{q_n - q_{n-1}}$$

for all $n \geq 3$. Hence, if we assume the finiteness of the 2-primary component of of the Tate-Shafarevich group $Ш(E/\mathbf{Q}_1)[2^\infty]$, we have

$$\begin{gathered}\text{rank } E(\mathbf{Q}_n) = 1 \text{ for all } n \geq 1, \\ Ш(E/\mathbf{Q}_1)[2^\infty] = Ш(E/\mathbf{Q}_2)[2^\infty] = 0, \text{ and} \\ Ш(E/\mathbf{Q}_n)[2^\infty] \cong (\mathbf{Z}/2^{n-2}\mathbf{Z})^{q_3-q_2} \oplus (\mathbf{Z}/2^{n-3}\mathbf{Z})^{q_4-q_3} \oplus \cdots \oplus (\mathbf{Z}/2\mathbf{Z})^{q_n-q_{n-1}}\end{gathered}$$

for all $n \geq 3$.

3. $\mathrm{Sel}(E/\mathbf{Q}_\infty)^\vee \cong \mathbf{Z}_2[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$.

2.2 The modular elements

In this section and the following section, we will introduce the modular elements and the zeta elements again. For $N \geq 1$, let $\mathcal{G}_N := \mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q})$. We define the modular element $\theta_N \in \mathbf{Q}[\mathcal{G}_N]$ by

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

For the original definition, see Remark 2.2.1

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 χ 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.

$$\pi_{qM/M}(\theta_{qM}) = \begin{cases} a_q\theta_M - \epsilon_q \nu_{M/\frac{M}{q}}(\theta_{\frac{M}{q}}) & (q \mid M) \\ (a_q - \sigma_q - \epsilon_q\sigma_q^{-1})\theta_M & (q \nmid M). \end{cases}$$

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 2.2.1. In [12], the modular elements are defined by

$$\theta_N := \sum_{a \in (\mathbf{Z}/N\mathbf{Z})^\times/\{\pm 1\}} [\frac{a}{N}]_E^+ \sigma_a \in \mathbf{Q}[\mathcal{G}_N/\{\pm 1\}].$$

2.3 The zeta elements

Kato defined an Euler system in cohomology groups $\mathrm{H}^1(\mathbf{Z}[\mu_N, \frac{1}{S}], V_pE)$ in [7]. 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 2.3.1. *Let χ 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*

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

Here, $\exp_N^*$ is the dual exponential map and $\Omega_E^{\pm}$ are Néron periods. See Kato [7], 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

$$\mathrm{Nr}_{qM/M}(w_{qM}) = \begin{cases} w_M & (q \mid M) \\ F_q(\sigma_q^{-1}) w_M & (q \nmid M). \end{cases}$$

Here $F_q(T)$ is the polynomial in Definition 3.2.2.

Proposition 2.3.2. *The zeta elements $(z_M)_M$ form an Euler system.*

See Kato [7], Theorem 8.12.

2.4 Proof of the theorem

2.4.1 Conductor

Proposition 2.4.1. *Suppose that E has supersingular reduction at 2, and 2 does not divide* $\mathrm{Tam}(E)$*. Then, the conductor of N satisfies*

$$N \equiv 3, 5 \pmod 8.$$

Proof. Let

$$y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6$$

be the minimal Weierstrass equation of E over $\mathbf{Z}$. If $\mathcal{E}$ is a supersingular elliptic curve over $\mathbf{F}_2$, then its j-invariant is 0, and it has a Weierstrass equation of the form $y^2 + y = x^3 + \beta_4 x + \beta_6 (\beta_4, \beta_6 \in \mathbf{F}_2$, cf. [19] p.325). Hence, considering all possible changes of variables of the Weierstrass equation, we know that α_1 is even and α_3 is odd. This implies that the minimal discriminant $\Delta_E = \Delta_E(a_1, \ldots, a_6)$ satisfies $\Delta_E \equiv 5 \pmod 8$.

On the other hand, suppose that l is a bad reduction prime for E. Since $\mathrm{Tam}(E)$ is odd, $c_l = [E(\mathbf{Q}_l) : E^0(\mathbf{Q}_l)]$ is also odd, and the table by Néron and Kodaira tells us that the number of irreducible components of the Néron model of E over $\mathbf{Z}_l$ is odd. It follows from Ogg's formula that

$$\mathrm{ord}_l(N) \equiv \mathrm{ord}_l(\Delta_E) \pmod 2.$$

Hence, the absolute value of Δ_E / N is a square. Thus we have

$$N \equiv 3, 5 \pmod 8.$$

□

Corollary 2.4.2. Let E' be the quadratic twist of E by the Dirichlet character corresponding to $\mathbf{Q}(\sqrt{2})$. If E has supersingular reduction at 2 and $\mathrm{ord}_2(\frac{L(E,1)}{\Omega_E}) = \mathrm{ord}_2(\mathrm{Tam}(E)) = 0$, then we have $L(E', 1) = 0$.

Proof. By proposition 2.4.1, the conductor N of E satisfies $N \equiv 3, 5 \pmod 8$. Hence, the sign of the functional equation of E' is -1. So we have $L(E', 1) = 0$. □

2.4.2 Formal groups

Lemma 2.4.3. *Let $\mathcal{F}$ be a formal group of height h. Let $L/K/\mathbf{Q}_p$ are finite extensions of local fields. Let m_K and m_L be the maximal ideal of K and L respectively, let k_K and k_L be the residue field of K and L respectively, and let e_K, e_L and e be the index of ramification of the extension $K/\mathbf{Q}_p, L/\mathbf{Q}_p$ and L/K respectively. Let $D_{L/K} = m_L^f$ be the different of the extension L/K. Let*

$$N_{L/K} : \mathcal{F}(m_L) \to \mathcal{F}(m_K)$$

be the norm map.

1. *If $f \leq 2e-2$, then $N_{L/K}$ is surjective.*

2. *Let s be an integer such that $s > \frac{e_L}{p^h-1}$. Put $t := [\frac{s+f}{e}]$. Then*

$$\sharp(\mathcal{F}(m_K)/N_{L/K}(\mathcal{F}(m_L))) \geq (\sharp k_K)^{t-1}/(\sharp k_L)^{s-1}.$$

Proof. From [18], $\mathrm{tr}_{L/K}(m_L^i) = m_K^j$ with $j = [\frac{i+f}{e}]$.

First, we will prove 1. of the lemma.

To prove the surjectivity, it suffices to show that for each $j \geq 1$, there exists $i \geq 1$ such that $N_{L/K}(\mathcal{F}(m_L^i)) = m_K^j$ and the induced map

$$N_{L/K} : \mathcal{F}(m_L^i) \to \mathcal{F}(m_K^j)/\mathcal{F}(m_K^{j+1})$$

is surjective.

Put $i_j := e(j+1) - f - 1$. From the assumption, we have $i_j \geq 1$ for each $j \geq 1$. We have $\mathrm{tr}_{L/K}(m_L^{i_j}) = m_K^j$ and $\mathrm{tr}_{L/K}(m_L^{i_j+1}) = m_K^{j+1}$. Thus, the trace map induces the isomorphism

$$\mathrm{tr}_{L/K} : m_L^{i_j}/m_L^{i_j+1} \xrightarrow{\cong} m_K^j/m_K^{j+1}.$$

The composite of the map

$$\mathcal{F}(m_L^{i_j})/\mathcal{F}(m_L^{i_j+1}) \cong m_L^{i_j}/m_L^{i_j+1} \xrightarrow{\mathrm{tr}_{L/K}} m_K^j/m_K^{j+1} \cong \mathcal{F}(m_K^j)/\mathcal{F}(m_K^{j+1})$$

coincides with the map induced from the norm map

$$N_{L/K} : \mathcal{F}(m_L^{i_j})/\mathcal{F}(m_L^{i_j+1}) \to \mathcal{F}(m_K^j)/\mathcal{F}(m_K^{j+1}).$$

Thus, we have proved the surjectivity of the norm map.

Next, we will prove 2. of the lemma. Since $s > \frac{e_L}{p^h-1}$, the formal logarithm induces the isomorphism

$$\log_{\mathcal{F}} : \mathcal{F}(m_L^s) \xrightarrow{\cong} m_L^s.$$

We have a commutative diagram below.

$$\begin{array}{ccccc} N_{L/K}: & \mathcal{F}(m_L) & \to & \mathcal{F}(m_K) \\ & \downarrow & \circlearrowleft & \downarrow \\ \mathrm{tr}_{L/K}: & L & \to & K \end{array}$$

Here, the vertical arrows are the logarithm map of the formal group $\log_{\mathcal{F}}$. $\mathrm{tr}_{L/K}(m_L^s) = m_K^t$. Since $f \geq e-1$, we have

$$t = [\frac{s+f}{e}] \geq [\frac{s+e-1}{e}] \geq \frac{s}{e} > \frac{e_L}{e(p^h-1)} = \frac{e_K}{p^h-1}.$$

Thus, we have an isomorphism

$$\log_{\mathcal{F}}(m_L^t) \xrightarrow{\cong} m_L^t.$$

So, we have $N_{L/K}(\mathcal{F}(m_L^s)) = \mathcal{F}(m_K^t)$. Since we have $[\mathcal{F}(m_L) : \mathcal{F}(m_L^s)] = (\sharp k_L)^{s-1}$ and $[\mathcal{F}(m_K) : \mathcal{F}(m_K^t)] = (\sharp k_K)^{t-1}$, we obtain

$$\sharp(\mathcal{F}(m_K)/N_{L/K}(\mathcal{F}(m_L))) \geq (\sharp k_K)^{t-1}/(\sharp k_L)^{s-1}.$$

□

A consequence of the above lemma is as follows. For $n \geq 1$, put

$$q_n := \begin{cases} 0 & (n=1) \\ p^{n-1} - p^{n-2} + p^{n-3} - p^{n-4} + \cdots + p - 1 & (n \geq 2, n : \text{even}) \\ p^{n-1} - p^{n-2} + p^{n-3} - p^{n-4} + \cdots + p^2 - p & (n \geq 3, n : \text{odd}) \end{cases}$$

if p is an odd prime number and

$$q_n := \sum_{k=0}^{n-1} (-1)^k 2^{n-1-k} = \frac{1}{3}(2^n - (-1)^n)$$

if $p = 2$. Let $\mathbf{Q}_\infty/\mathbf{Q}$ be the cyclotomic $\mathbf{Z}_p$-extension and $\mathbf{Q}_n$ its n-th layer. Let k_n be the p-adic completion of $\mathbf{Q}_n$. Then for the extension $\mathbf{Q}_n/\mathbf{Q}_{n-1}$, we have $e = p$ and $f = p^n + p - 2$ if p is odd and $f = 2^n + 1$ if $p = 2$. We have the next lemma.

Lemma 2.4.4. *Let $E/\mathbf{Q}$ be an elliptic curve which has supersingular reduction at a prime p. Then we have*

$$\mathrm{ord}_p(\sharp(\widehat{E}(m_{k_{n-1}})/N_{k_n/k_{n-1}}(\widehat{E}(m_{k_n})))) \geq q_n.$$

2.4.3 The behavior of the modular elements

We put $G_n := \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})$. We denote the map $\pi_{\mathbf{Q}_{n+1}/\mathbf{Q}_n} : \mathbf{Q}[G_{n+1}] \to \mathbf{Q}[G_n]$ by π_n and the map $\nu_{\mathbf{Q}_n/\mathbf{Q}_{n-1}} : \mathbf{Q}[G_{n-1}] \to \mathbf{Q}[G_n]$ by ν_n. We define the modular element $\theta_{\mathbf{Q}_n}$ by the image of $\theta_{2^{n+2}}$ through the restriction map $\mathbf{Q}[\mathcal{G}_{2^{n+2}}] \to \mathbf{Q}[G_n]$. Note that $\theta_{\mathbf{Q}}$ is not θ_1 but the image of θ_4.

Proposition 2.4.5. *Let $\mathbf{Q}_\infty/\mathbf{Q}$ be the cyclotomic $\mathbf{Z}_2$-extension. Let E be an elliptic curve defined over $\mathbf{Q}$. Suppose that $p = 2$, $a_2 = \pm 2$ and $\mathrm{ord}_2 \frac{L(E,1)}{\Omega_E} = 0$. Let ψ_n be a faithful character of the group G_n. Put $q_n := \sum_{k=0}^{n-1}(-1)^k 2^{n-1-k} = \frac{1}{3}(2^n - (-1)^n)$ as in the previous subsection. Then we have $\mathrm{ord}_2\theta_{\mathbf{Q}} = 0$, $\psi_1(\theta_{\mathbf{Q}_1}) = 0$ and*

$$\mathrm{ord}_{\zeta_{2^n}-1}\psi_n(\theta_{\mathbf{Q}_n}) = q_n$$

for $n \geq 2$.

Proof. First we prove $\psi_1(\theta_{\mathbf{Q}_1}) = 0$. We have $\psi_1(\theta_{\mathbf{Q}_1}) = \tau(\chi_8)\frac{L(E,\chi_8,1)}{\Omega_E}$ where χ_8 is the Dirichlet character corresponding to $\mathbf{Q}_1 = \mathbf{Q}(\sqrt{2})$. From Corollary 2.4.2, we have $L(E, \chi_8, 1) = 0$, so $\psi_1(\theta_1) = 0$. We put $\theta_{\mathbf{Q}_1} = a(1 + \gamma)$ for some $a \in \mathbf{Z}_2$. We have $\pi_0(\theta_{\mathbf{Q}_1}) = 2a$.

On the other hand, we have

$$\begin{aligned}
\pi_0(\theta_{\mathbf{Q}_1}) &= \pi_{8/1}(\theta_8) \\
&= \pi_{4/1}(a_2\theta_4 - \nu_{4/2}(\theta_2)) \\
&= \pi_{2/1}(a_2(a_2\theta_2 - \nu_{2/1}(\theta_1)) - 2\theta_2) \\
&= \pi_{2/1}((a_2^2 - 2)\theta_2 - a_2\nu_{2/1}(\theta_1)) \\
&= (a_2^2 - 2)(a_2 - 1 - 1)\theta_1 - a_2\theta_1 \\
&= (a_2^3 - 2a_2^2 - 3a_2 + 4)\frac{L(E,1)}{\Omega_E} \\
&= (a_2 - 1)(a_2^2 - a_2 - 4)\frac{L(E,1)}{\Omega_E}.
\end{aligned}$$

So $\mathrm{ord}_2(\pi_0(\theta_{\mathbf{Q}_1})) = 1$. Thus we get $a \in \mathbf{Z}_2^\times$. We also have $\mathrm{ord}_2(\theta_{\mathbf{Q}}) = 0$ since

$$\begin{aligned}
\theta_{\mathbf{Q}} &= \pi_{4/1}(\theta_4) \\
&= \pi_{2/1}(a_2\theta_2 - \nu_{2/1}(\theta_1)) \\
&= (a_2(a_2 - 2) - 1)\theta_1 \\
&= (a_2^2 - 2a_2 - 1)\frac{L(E,1)}{\Omega_E}.
\end{aligned}$$

Since $\pi_1(\theta_{\mathbf{Q}_2}) = a_2\theta_{\mathbf{Q}_1} - \nu_1(\theta_{\mathbf{Q}})$. We have $\theta_{\mathbf{Q}_2} = a_2\theta_{\mathbf{Q}_1} - \nu_1(\theta_{\mathbf{Q}}) + \alpha(\gamma^2 - 1)$ for some $\beta \in \Lambda_2$. Since $\psi_2(\gamma) = \zeta_4$ and $\nu_1 = (1+\gamma)$, the $(\zeta_4 - 1)$-adic orders of the three terms are $3, 1, \geq 2$ respectively. Thus we have $\mathrm{ord}_{\zeta_4 - 1}(\psi_1(\theta_{\mathbf{Q}_1})) = 1$. Similarly we have $\mathrm{ord}_{\zeta_8 - 1}(\psi_2(\theta_{\mathbf{Q}_2})) = 3$ and $\mathrm{ord}_{\zeta_{2^{n+1}} - 1}\psi_{n+1}(\theta_{\mathbf{Q}_{n+1}}) = 2^{n-1} + \mathrm{ord}_{\zeta_{2^{n-1}}}\psi_{n-1}(\theta_{\mathbf{Q}_{n-1}})$ for $n \geq 3$. By induction, we have $\mathrm{ord}_{\zeta_{2^n} - 1}(\psi_n(\theta_{\mathbf{Q}_n})) = q_n$. □

Proposition 2.4.5 is an analogue of Proposition 1.2 in Kurihara [10].

Proposition 2.4.6 (Proposition 1.2 in Kurihara [10])**.** *Let p be an odd prime number, let $\mathbf{Q}_\infty/\mathbf{Q}$ be the cyclotomic $\mathbf{Z}_p$-extension and let E be an elliptic curve defined over $\mathbf{Q}$. Assume that E is supersingular at p and $\mathrm{ord}_p \frac{L(E,1)}{\Omega_E} = 0$. Let ψ_n be a faithful character of the group G_n. Then $\mathrm{ord}_p\theta_{\mathbf{Q}} = 0$ and*

$$\mathrm{ord}_{\zeta_{p^n} - 1}\psi_n(\theta_{\mathbf{Q}_n}) = q_n.$$

2.4.4 The Selmer groups and cohomology groups

In this section, we assume that F is a number field, E/F is an elliptic curve which has good reduction at all the primes above a prime number p. Let F_∞/F be the cyclotomic $\mathbf{Z}_p$-extension of F and let F_n be its n-th layer for an integer $n \geq 0$. Let $\Gamma := \mathrm{Gal}(F_\infty/F)$ and $\Gamma_n := \mathrm{Gal}(F_n/F)$. We fix a generator of Γ and denote it by γ. We also denote the image of γ through the natural map $\Gamma \to \Gamma_n$ by γ.

Definition 2.4.7. *For an algebraic extension F'/F, we define the Selmer group $\mathrm{Sel}(E/F')$ with respect to $E[p^\infty]$ by*

$$\mathrm{Sel}(E/F') := \mathrm{Ker}(\mathrm{H}^1(F', E[p^\infty]) \to \prod_v \mathrm{H}^1(F'_v, E[p^\infty])/(E(F'_v) \otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p)),$$

the fine Selmer group $\mathrm{Sel}_0(E/F')$ by

$$\mathrm{Sel}_0(E/F') := \mathrm{Ker}(\mathrm{H}^1(F', E[p^\infty]) \to \prod_v \mathrm{H}^1(F'_v, E[p^\infty])),$$

and $\mathrm{Sel}'(E/F')$ by

$$\mathrm{Sel}'(E/F') := \mathrm{Ker}(\mathrm{H}^1(F', E[p^\infty]) \to \prod_{v \nmid p} \mathrm{H}^1(F'_v, E[p^\infty])).$$

We define the Selmer group $\mathrm{Sel}(E/F', T_pE)$ *with respect to* T_pE *by*

$$\mathrm{Sel}(E/F', T_pE) := \mathrm{Ker}(\mathrm{H}^1(F', T_pE) \to \prod_v \mathrm{H}^1(F'_v, T_pE)/(E(F'_v)\widehat{\otimes}\mathbf{Z}_p)).$$

Here, v *runs through all the prime of* F'*.*

From the definitions above, we have

$$\mathrm{Sel}_0(E/F') \subset \mathrm{Sel}(E/F') \subset \mathrm{Sel}'(E/F').$$

Let S be a finite set of primes of F containing primes above p, bad primes and infinite primes. For a number field F' over F, let $\mathcal{O}_{F'}$ be the ring of integers of F' and $\mathcal{O}_{F'}[1/S]$ be the ring of S-integers of F'. We consider étale cohomology groups $\mathrm{H}^*(\mathcal{O}_F[1/S], A) = \mathrm{H}^*(G_{F',S}, A)$ where $G_{F',S}$ is the Galois group of the maximal unramified extension of F' outside S.

For a $\mathbf{Z}$-module M, $M\widehat{\otimes}\mathbf{Z}_p := \varprojlim M \otimes_{\mathbf{Z}} \mathbf{Z}/p^n\mathbf{Z}$.

For a group G and G-module, M^G denotes the G-invariant part and M_G denotes the G-coinvariant.

In this paper, a commutative diagram means a commutative diagram with exact rows and columns.

Lemma 2.4.8. *For a number field* F*, the sequence*

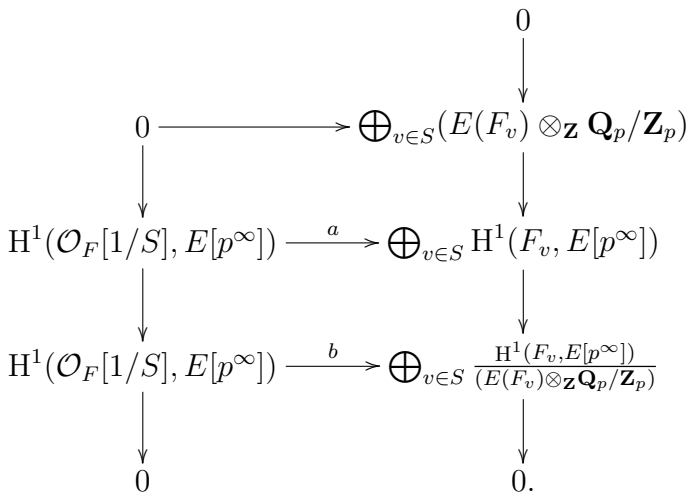
$$\begin{aligned} & \mathrm{H}^1(\mathcal{O}_F[1/S], T_pE) \to \bigoplus_{v\in S} \mathrm{H}^1(F_v, T_pE)/(E(F_v)\widehat{\otimes}\mathbf{Z}_p) \\ \to\ & \mathrm{Sel}(E/F)^\vee \to \mathrm{Sel}_0(E/F)^\vee \to 0 \end{aligned}$$

and the sequence

$$\begin{aligned} 0 \ \to\ & \mathrm{Sel}(E/F) \to \mathrm{H}^1(\mathcal{O}_F[1/S], E[p^\infty]) \to \bigoplus_{v\in S} \frac{\mathrm{H}^1(F_v, E[p^\infty])}{E(F_v)\otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p} \\ \to\ & \mathrm{Sel}(E/F, T_pE)^\vee \to \mathrm{Sel}_0(E/F, T_pE)^\vee \to 0 \end{aligned}$$

are exact. Here, S *is a finite set of primes of* F *containing bad primes, primes above* p*, and infinite primes.*

Proof. We have a commutative diagram



From the snake lemma, we have an exact sequence

$$0 \to \mathrm{Ker}a \to \mathrm{Ker}b \to \bigoplus_{v\in S}(E(F_v)\otimes_{\mathbf{Z}}\mathbf{Q}_p/\mathbf{Z}_p) \to \mathrm{Coker}a.$$

From Cassels-Tate-Poitou duality, we have an exact sequence

$$\mathrm{H}^1(\mathcal{O}_F[1/S],E[p^\infty]) \to \bigoplus_{v\in S}\mathrm{H}^1(F_v,E[p^\infty]) \to \mathrm{H}^1(\mathcal{O}_F[1/S],T_pE)^\vee.$$

Thus, there is an injection $\mathrm{Coker}a \to \mathrm{H}^1(\mathcal{O}_F[1/S],T_pE)^\vee$. By the definitions, we have

$$\begin{aligned}\mathrm{Ker}a &= \mathrm{Sel}_0(E/F)\\ \mathrm{Ker}b &= \mathrm{Sel}(E/F).\end{aligned}$$

Thus, we have an exact sequence

$$0 \to \mathrm{Sel}_0(E/F) \to \mathrm{Sel}(E/F) \to \bigoplus_{v\in S}(E(F_v)\otimes_{\mathbf{Z}}\mathbf{Q}_p/\mathbf{Z}_p) \to \mathrm{H}^1(\mathcal{O}_F[1/S],T_pE)^\vee.$$

Since we have $(E(F_v)\otimes_{\mathbf{Z}}\mathbf{Q}_p/\mathbf{Z}_p)^\vee = \mathrm{H}^1(F_v,T_pE)/(E(F_v)\widehat{\otimes}\mathbf{Z}_p)$ for $v\in S$, we have obtained the dual of the first exact sequence of the lemma.

Similarly, we have a commutative diagram

$$\begin{array}{ccc}
 & & 0 \\
 & & \downarrow \\
0 & \longrightarrow & \bigoplus_{v\in S}(E(F_v)\widehat{\otimes}\mathbf{Z}_p) \\
\downarrow & & \downarrow \\
\mathrm{H}^1(\mathcal{O}_F[1/S], T_pE) & \xrightarrow{c} & \bigoplus_{v\in S}\mathrm{H}^1(F_v, T_pE) \\
\downarrow & & \downarrow \\
\mathrm{H}^1(\mathcal{O}_F[1/S], T_pE) & \xrightarrow{d} & \bigoplus_{v\in S}\mathrm{H}^1(F_v, T_pE)/(E(F_v)\widehat{\otimes}\mathbf{Z}_p) \\
\downarrow & & \downarrow \\
0 & & 0
\end{array}$$

By the snake lemma, we have an exact sequence

$$0 \;\to\; \mathrm{Ker}c \to \mathrm{Ker}d \to \bigoplus_{v\in S}(E(F_v)\widehat{\otimes}\mathbf{Z}_p) \to \mathrm{Coker}c$$

By the similar arguments using Cassels-Tate-Poitou duality as above, we have an exact sequence

$$\begin{aligned}
&\mathrm{H}^1(\mathcal{O}_F[1/S], E[p^\infty]) \to \bigoplus_{v\in S}\mathrm{H}^1(F_v, E[p^\infty])/E(F_v)\otimes_{\mathbf{Z}}\mathbf{Q}_p/\mathbf{Z}_p \\
\to\;& \mathrm{Sel}(E/F, T_pE)^\vee \to \mathrm{Sel}_0(E/F, T_pE)^\vee \to 0.
\end{aligned}$$

Since the kernel of the first map is $\mathrm{Sel}(E/F)$, we have obtained the second exact sequence. □

The next proposition is control theorems for the Selmer groups.

Proposition 2.4.9. *We assume that $E(F_v)[p] = 0$ for any prime v of F above p and $p \nmid \mathrm{Tam}(E)$, then we have isomorphisms*

$$\begin{aligned}
\mathrm{Sel}_0(E/F) &\cong \mathrm{Sel}_0(E/F_\infty)^\Gamma \\
\mathrm{Sel}'(E/F) &\cong \mathrm{Sel}'(E/F_\infty)^\Gamma.
\end{aligned}$$

Proof. The proof is based on the arguments in Greenberg's article [5] about Mazur's control theorem. The assumption $E(F_v)[p] = 0$ for all $v \mid p$ implies that $\mathrm{Sel}_0(E/F) \to \mathrm{Sel}_0(E/F_\infty)^\Gamma$ is injective. The assumption $p \nmid \mathrm{Tam}(E)$ implies that the cokernel is 0. Thus, it is an isomorphism. We can show $\mathrm{Sel}'(E/F) \cong \mathrm{Sel}'(E/F_\infty)^\Gamma$ similarly. □

We define

$$\mathbf{H}^1(\mathcal{O}_{F_\infty}[1/S], T_pE) := \varprojlim \mathrm{H}^1(\mathcal{O}_{F_n}[1/S], T_pE).$$

Proposition 2.4.10. *We assume that $E(F_v)[p] = 0$ for any prime v of F above p, $p \nmid \mathrm{Tam}(E)$ and $\mathrm{Sel}_0(E/F) = 0$. Then, the natural map*

$$\mathbf{H}^1(\mathcal{O}_{F_\infty}[1/S], T_pE)_{\Gamma_n} \to \mathrm{H}^1(\mathcal{O}_{F_n}[1/S], T_pE)$$

is surjective for all $n \geq 0$.

Proof. It suffices to show the proposition under the assumption that $n = 0$. From proposition 2.4.9, we have $\mathrm{Sel}_0(E/F) = \mathrm{Sel}_0(E/F_\infty) = 0$. From Cassels-Tate-Poitou duality, we have an exact sequence

$$0 \to \mathrm{H}^2(\mathcal{O}_F[1/S], T_pE) \to \bigoplus_{v \in S} \mathrm{H}^2(F_v, T_pE) \to \mathrm{H}^0(\mathcal{O}_F[1/S], E[p^\infty])^\vee \to 0.$$

Here, the injectivity of the first right arrow follows from $\mathrm{Sel}_0(E/F) = 0$. Since the second term is finite, $\mathrm{H}^2(\mathcal{O}_F[1/S], T_pE)$ is finite. Hence,

$$\mathrm{H}^2(\mathcal{O}_F[1/S], E[p^\infty]) = 0.$$

Applying Cassels-Tate-Poitou duality again, we have an exact sequence

$$\begin{array}{ccc}
0 & & 0 \\
\downarrow & & \downarrow \\
\mathrm{H}^1(\mathcal{O}_F[1/S], E[p^\infty]) & \longrightarrow & \mathrm{H}^1(\mathcal{O}_{F_\infty}[1/S], E[p^\infty])^\Gamma \\
\downarrow & & \downarrow \\
\bigoplus_{v \in S} \mathrm{H}^1(F_v, E[p^\infty]) & \longrightarrow & (\bigoplus_{v \in S_\infty} \mathrm{H}^1((F_\infty)_v, E[p^\infty]))^\Gamma \\
\downarrow & & \downarrow \\
\mathrm{H}^1(\mathcal{O}_F[1/S], T_pE)^\vee & \longrightarrow & (\mathbf{H}^1(\mathcal{O}_{F_\infty}[1/S], T_pE)^\vee)^\Gamma \\
\downarrow & & \\
0 & &
\end{array}$$

Here, the injectivity of the left vertical sequence follows from $\mathrm{Sel}_0(E/F) = 0$ and the surjectivity follows from $\mathrm{H}^2(\mathcal{O}_F[1/S], E[p^\infty]) = 0$.

The top right arrow is an isomorphism from the inflation-restriction sequence. The center right arrow is injective by the same argument of the proof of the control theorem for $\mathrm{Sel}_0(E/F)$. The bottom right arrow is injective. Taking dual, we have proved the proposition. □

2.4.5 The Selmer groups and the zeta elements

Let $\mathbf{Q}_\infty/\mathbf{Q}$ be the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. Put $k := \mathbf{Q}_p$ and k_n be the p-adic completion of $\mathbf{Q}_n$ for $n \geq 0$. Let $E/\mathbf{Q}$ be an elliptic curve. We assume that E has supersingular reduction at p and $\mathrm{ord}_p \frac{L(E,1)}{\Omega_E} = \mathrm{ord}_p \mathrm{Tam}(E) = 0$. If $G_{\mathbf{Q}} \to \mathrm{Aut}(E[p])$ is surjective, then we have

$$\mathbf{z} := (z_{\mathbf{Q}_n}) \in \varprojlim \mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n}[1/S], T_pE).$$

Namely, the system of the zeta elements is an integral Euler system. In the case of Theorem 2.1.1, the system is an integral system. We define $\Lambda_n := \mathbf{Z}_p[G_n]$ and $\Lambda := \mathbf{Z}_p[[\Gamma]] = \varprojlim \Lambda_n$.

Proposition 2.4.11. *We have*

$$\mathrm{Sel}(E/\mathbf{Q}) = 0.$$

Proof. This follows from the arguments of Euler system in §14 of Kato [7]. □

Lemma 2.4.12. *For $n \geq 0$, we have*

$$\mathrm{Sel}_0(E/\mathbf{Q}_n) = 0.$$

Proof. From Proposition 2.4.11, we have $\mathrm{Sel}_0(E/\mathbf{Q}) = 0$. From the control theorem, we have $\mathrm{Sel}_0(E/\mathbf{Q}_\infty) = 0$. Applying the control theorem again, we have $\mathrm{Sel}_0(E/\mathbf{Q}_n)$ for $n \geq 0$. □

Proposition 2.4.13. *The cohomology group $\mathbf{H}^1(\mathcal{O}_{\mathbf{Q}_\infty}[1/S], T_pE)$ is a free Λ-module of rank 1.*

Proof. This follows from the arguments in §13 of Kato [7]. □

Lemma 2.4.14. *We have*

$$\mathbf{H}^1(\mathcal{O}_{\mathbf{Q}_\infty}[1/S], T_pE)_{\Gamma_n} \cong \mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n}[1/S], T_pE).$$

Hence $\mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n}[1/S], T_pE)$ is a free Λ_n-module of rank 1.

Proof. From proposition 2.4.10, there is a surjective map

$$\mathbf{H}^1(\mathcal{O}_{\mathbf{Q}_\infty}[1/S], T_pE)_{\Gamma_n} \to \mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n}[1/S], T_pE). \tag{2.1}$$

Since $\mathbf{H}^1(\mathcal{O}_{\mathbf{Q}_\infty}[1/S], T_pE)_{\Gamma_n} \cong \Lambda$, the left hand side of the equation 2.1 is isomorphic to $\Lambda_{\Gamma_n} \cong \Lambda_n$. Hence, the kernel of the map is trivial and the equation 2.1 is actually an isomorphism. □

Lemma 2.4.15. *The cohomology group* $\mathrm{H}^1(\mathbf{Z}[1/S], T_pE)$ *is a free* $\mathbf{Z}_p$*-module of rank* 1 *generated by* $z_{\mathbf{Q}}$.

Proof. The dual exponential map induces an isomorphism

$$\exp^* : \mathrm{H}^1(\mathbf{Q}_p, T_pE)/(E(\mathbf{Q}_p)\widehat{\otimes}\mathbf{Z}_p) \to p^{-1}\mathbf{Z}_p\omega_E.$$

From Lemma 2.4.14, $\mathrm{H}^1(\mathbf{Z}[1/S], T_pE)$ is a free $\mathbf{Z}_p$-module of rank 1. Since we have

$$\exp^*(z_{\mathbf{Q}}) = (1 - \frac{a_p}{p} + \frac{1}{p})\omega_E,$$

the image of $z_{\mathbf{Q}}$ in $\mathrm{H}^1(\mathbf{Q}_p, T_pE)$ generates $\mathrm{H}^1(\mathbf{Q}_p, T_pE)/(E(\mathbf{Q}_p)\widehat{\otimes}\mathbf{Z}_p)$. Hence $z_{\mathbf{Q}}$ generates $\mathrm{H}^1(\mathbf{Z}[1/S], T_pE)$. □

Lemma 2.4.16. *We have*

$$\mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n}[1/S], T_pE) = \langle z_{\mathbf{Q}_n}\rangle_{\Lambda_n}.$$

Proof. From Proposition 2.4.14, Lemma 2.4.15 and Nakayama's lemma, $\mathbf{z}$ generates $\mathbf{H}^1(\mathcal{O}_{\mathbf{Q}_\infty}[1/S], T_pE)$. Again by the isomorphism in Lemma 2.4.14

$$\mathbf{H}^1(\mathcal{O}_{\mathbf{Q}_\infty}[1/S], T_pE)_{\Gamma_n} \cong \mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n}[1/S], T_pE),$$

$z_{\mathbf{Q}_n}$ generates $\mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n})[1/S], T_pE)$. □

Proposition 2.4.17. *We have*

$$\mathrm{Sel}(E/\mathbf{Q}_n)^\vee \cong \mathrm{H}^1(k_n, T_pE)/(E(k_n)\widehat{\otimes}\mathbf{Z}_p + \langle z_{\mathbf{Q}_n}\rangle_{\Lambda_n}).$$

Proof. Since $\mathrm{Sel}_0(E/\mathbf{Q}) = 0$ and there is only one prime of $\mathbf{Q}_n$ above p, we have an exact sequence

$$\mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n}[1/S], T_pE) \to \mathrm{H}^1(k_n, T_pE)/(E(k_n)\widehat{\otimes}\mathbf{Z}_p) \to \mathrm{Sel}(E/\mathbf{Q}_n)^\vee \to 0$$

by Lemma 2.4.8. Since the module $\mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n}[1/S], T_pE)$ is generated by $z_{\mathbf{Q}_n}$ by Lemma 2.4.16, we have proved the proposition. □

Theorem 2.4.18. *The dual of the Selmer group* $\mathrm{Sel}(E/\mathbf{Q}_\infty)^\vee$ *is a free* Λ*-module of rank* 1.

Proof. Since we know that Λ-rank of $\mathrm{Sel}(E/\mathbf{Q}_\infty)^\vee$ is ≥ 1 (see Theorem 2.6 in Coates-Sujatha [3]), we only have to show that $\mathrm{Sel}(E/\mathbf{Q}_\infty)^\vee$ is generated by one element. By the definition of the Selmer groups, we have an exact sequence

$$0 \to \mathrm{Sel}(E/\mathbf{Q}) \to \mathrm{Sel}'(E/\mathbf{Q}) \to \mathrm{H}^1(\mathbf{Q}_p, E[p^\infty])/E(\mathbf{Q}_p) \otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p.$$

Since we have $\mathrm{Sel}(E/\mathbf{Q}) = 0$ and the dual of the last term is isomorphic to $\mathbf{Z}_p$, $\mathrm{Sel}'(E/\mathbf{Q})^\vee$ is generated by one element. From the control theorem and Nakayama's lemma, $\mathrm{Sel}'(E/\mathbf{Q}_\infty)$ is generated by one element as a Λ-module. We have another exact sequence

$$0 \to \mathrm{Sel}(E/\mathbf{Q}_\infty) \to \mathrm{Sel}'(E/\mathbf{Q}_\infty) \to \mathrm{H}^1(k_\infty, E[p^\infty])/E(k_\infty) \otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p.$$

Since E has supersingular reduction at p, the last term is 0. Hence, $\mathrm{Sel}(E/\mathbf{Q}_\infty)^\vee$ is generated by one element. Thus we have proved the theorem. □

Lemma 2.4.19. *The dual of the Selmer group* $\mathrm{Sel}(E/\mathbf{Q}_n)^\vee$ *is a cyclic* Λ_n*-module.*

Proof. Since the restriction map

$$\mathrm{Sel}(E/\mathbf{Q}_n) \to \mathrm{Sel}(E/\mathbf{Q}_\infty)$$

is injective, the map

$$\mathrm{Sel}(E/\mathbf{Q}_\infty)^\vee \to \mathrm{Sel}(E/\mathbf{Q}_n)^\vee$$

is surjective. From the above theorem, $\mathrm{Sel}(E/\mathbf{Q}_\infty)^\vee$ is a cyclic Λ-module. So $\mathrm{Sel}(E/\mathbf{Q}_n)^\vee$ is a cyclic Λ_n-module. □

2.4.6 The Selmer groups and the modular elements

Proposition 2.4.20. $\mathrm{Sel}(E/\mathbf{Q}_n)^\vee$ *is annihilated by* $\theta_{\mathbf{Q}_n}$ *and* $\nu_n(\theta_{\mathbf{Q}_{n-1}})$.

Proof. From Proposition 2.4.17, we have

$$\mathrm{Sel}(E/\mathbf{Q}_n)^\vee \cong \mathrm{H}^1(k_n, T_pE)/(E(k_n)\widehat{\otimes}\mathbf{Z}_p + \langle z_{\mathbf{Q}_n}\rangle_{\Lambda_n}).$$

From the properties of the map $\widehat{P}_n$ in §3.6, the map

$$\mathrm{H}^1(k_n, T_pE)/(E(k_n)\widehat{\otimes}\mathbf{Z}_p + \langle z_{\mathbf{Q}_n}\rangle_{\Lambda_n}) \to \Lambda_n \oplus \Lambda_n/\langle(\theta_{\mathbf{Q}_n}, \nu_n(\theta_{\mathbf{Q}_{n-1}}))\rangle_{\Lambda_n}$$

is injective. So, it suffices to show that $\mathrm{Im}\widehat{P}_n/\langle(\theta_{\mathbf{Q}_n}, \nu_n(\theta_{\mathbf{Q}_{n-1}}))\rangle_{\Lambda_n}$ is annihilated by $\theta_{\mathbf{Q}_n}$ and $\nu_n(\theta_{\mathbf{Q}_{n-1}})$. We denote $\mathrm{Nr}_{\mathbf{Q}_n/\mathbf{Q}_{n-1}}$ by Nr_n. Let $w \in \mathrm{H}^1(k_n, T_pE)$, we have

$$\begin{aligned}
\theta_{\mathbf{Q}_n}\widehat{P}_n(w) &= \theta_{\mathbf{Q}_n}(\mathcal{P}_{\mathbf{Q}_n}(w), \nu_n(\mathcal{P}_{\mathbf{Q}_{n-1}}(\mathrm{Nr}_n(w)))) \\
&= (\theta_{\mathbf{Q}_n}\mathcal{P}_{\mathbf{Q}_n}(w), \theta_{\mathbf{Q}_n}\nu_n(\mathcal{P}_{\mathbf{Q}_{n-1}}(\mathrm{Nr}_n(w))) \\
&= (\theta_{\mathbf{Q}_n}\mathcal{P}_{\mathbf{Q}_n}(w), \nu_n(\theta_{\mathbf{Q}_n-1})\mathcal{P}_{\mathbf{Q}_n}(w)) \\
&= \mathcal{P}_{\mathbf{Q}_n}(w)(\theta_{\mathbf{Q}_n}, \nu_n(\theta_{\mathbf{Q}_{n-1}})) \in \langle(\theta_{\mathbf{Q}_n}, \nu_n(\theta_{\mathbf{Q}_{n-1}}))\rangle_{\Lambda_n}.
\end{aligned}$$

In the third line, we used the Lemma 3.6.6 in §3.6. Thus, it is annihilated by $\theta_{\mathbf{Q}_n}$. Similarly, $\nu_n(\theta_{\mathbf{Q}_{n-1}})$ annihilates it. Thus we have proved the proposition. □

For $n \geq 1$, put $I_n := (\theta_{\mathbf{Q}_n}, \nu_n(\theta_{\mathbf{Q}_{n-1}}))$. From now on, we assume that $a_2 = \pm 2$ if $p = 2$. Put $R_n := \mathrm{Ker}(\Lambda_n/I_n \to \Lambda_1/I_1)$. Thus, the sequence

$$0 \to R_n \to \Lambda_n/I_n \to \Lambda_1/I_1 \to 0$$

is exact.

The numbers $(q_i)_{i\geq 1}$ in Lemma 2.4.4 often appear in the following arguments. Note that $q_1 = 0$ if p is odd and $q_1 = 1$ if $p = 2$.

Lemma 2.4.21. *We have* $\Lambda_1/I_1 \cong (\mathbf{Z}_p)^{q_1}$.

Proof. Since the sequence

$$\mathbf{Z}_p/(\theta_{\mathbf{Q}}) \xrightarrow{\nu_1} \Lambda_1/I_1 \xrightarrow{\psi_1} \mathbf{Z}_p/(\psi_1(\theta_{\mathbf{Q}_1})) \to 0$$

is exact and $\theta_{\mathbf{Q}}$ is a p-adic unit, it suffices to show that

$$\mathbf{Z}_p/(\psi_1(\theta_{\mathbf{Q}_1})) \cong (\mathbf{Z}_p)^{q_1}.$$

Since $\psi_1(\theta_{\mathbf{Q}_1})$ is a p-adic unit if p is odd and $\psi_1(\theta_{\mathbf{Q}_1}) = 0$ if $p = 2$, we have proved the lemma. □

Lemma 2.4.22. *We have* $\mathrm{rank}_{\mathbf{Z}_p}\mathrm{Sel}(E/F, T_pE) \leq \mathrm{corank}_{\mathbf{Z}_p}\mathrm{Sel}(E/F)$.

Proof. This follows from the exact sequence

$$\mathrm{Sel}(E/F, T_pE) \to \mathrm{Sel}(E/F, V_pE) \to \mathrm{Sel}(E/F).$$

□

Lemma 2.4.23. *We have*

$$\mathrm{Sel}(E/\mathbf{Q}_1)^\vee \cong \Lambda_1/I_1$$

and

$$\mathrm{Sel}(E/\mathbf{Q}_1, T_pE) \cong (\mathbf{Z}_p)^{q_1}.$$

Proof. We first prove that $\mathrm{Sel}(E/\mathbf{Q}_1)^\vee \cong \Lambda_1/I_1$. Since the map

$$\Lambda_1/I_1 \to \mathrm{Sel}(E/\mathbf{Q}_1)^\vee$$

is surjective, it suffices to show the injectivity. From Lemma 2.4.21, we have $\Lambda_1/I_1 = 0$ for odd p. Hence the isomorphism holds as $0 \cong 0$. We assume that $p = 2$. Since $\Lambda_1/I_1 \cong \mathbf{Z}_2$, $\mathrm{Sel}(E/\mathbf{Q}_1)^\vee$ is a cyclic $\mathbf{Z}_2$-module. We will prove $\mathrm{rank}_{\mathbf{Z}_2}\mathrm{Sel}(E/\mathbf{Q}_1)^\vee > 0$. Since $\psi_1(\theta_{\mathbf{Q}_1}) = 0$ implies that $L(E, \psi_1, 1) = 0$, we have $\exp^*((\gamma - 1)z_{\mathbf{Q}_1}) = 0$. Thus we have $(\gamma - 1)z_{\mathbf{Q}_1} \in \mathrm{Sel}(E/\mathbf{Q}_1, T_2E)$. Since $\mathrm{H}^1(\mathbf{Q}_1, T_2E)$ is a free Λ_1-module generated by $z_{\mathbf{Q}_1}$, we have

$$\mathrm{rank}_{\mathbf{Z}_2}\mathrm{Sel}(E/\mathbf{Q}_1, T_2E) > 0.$$

From Lemma 2.4.22, we have $\mathrm{corank}_{\mathbf{Z}_2}\mathrm{Sel}(E/\mathbf{Q}_1) > 0$. Thus we have

$$\mathrm{Sel}(E/\mathbf{Q}_1)^\vee \cong \Lambda_1/I_1.$$

We prove the second isomorphism. Since $E(\mathbf{Q}_1)[p] = 0$, $\mathrm{Sel}(E/\mathbf{Q}_1, T_pE)[p] = 0$. Since we have

$$\mathrm{rank}_{\mathbf{Z}_p}\mathrm{Sel}(E/\mathbf{Q}_1, T_pE) \leq \mathrm{corank}_{\mathbf{Z}_p}\mathrm{Sel}(E/\mathbf{Q}_1) = q_1,$$

the isomorphism holds as $0 \cong 0$ if p is odd. If $p = 2$, we have seen that

$$\mathrm{rank}_{\mathbf{Z}_2}\mathrm{Sel}(E/\mathbf{Q}_1, T_2E) > 0,$$

so $\mathrm{rank}_{\mathbf{Z}_2}\mathrm{Sel}(E/\mathbf{Q}_1, T_2E) = 1$. We have proved the isomorphism. □

We put

$$r_n := \sum_{i=1}^{n}(q_i - q_1).$$

Namely, $r_n = \sum_{i=1}^{n} q_i$ if p is odd and $r_n = \sum_{i=0}^{n}(q_i - 1)$ if $p = 2$.

Lemma 2.4.24. *1.* $R_n = (\Lambda_n/I_n)_{\mathrm{tors}}$ *and* $\mathrm{ord}_2(\sharp R_n) \leq r_n$.

2. $\mathrm{ord}_2(\sharp(\mathrm{Sel}(E/\mathbf{Q}_n)^\vee)_{\mathrm{tors}}) \geq r_n$.

Proof of 1. of Theorem 2.1.1. Assuming this, we will prove the main theorem. Since $\mathrm{Sel}(E/\mathbf{Q}_n)^\vee$ is a cyclic Λ_n-module, there exists a surjective homomorphism $f : \Lambda_n/I_n \to \mathrm{Sel}(E/\mathbf{Q}_n)^\vee$.

We proved the isomorphism in the case $n = 1$ in Lemma 2.4.23, we treat the case when $n \geq 2$. The diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R_n & \longrightarrow & \Lambda_n/I_n & \longrightarrow & \Lambda_1/I_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \simeq} & & \\ 0 & \longrightarrow & \mathrm{Ker}\alpha & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_n)^\vee & \xrightarrow{\alpha} & \mathrm{Sel}(E/\mathbf{Q}_1)^\vee & \longrightarrow & 0 \end{array}$$

is commutative. From the snake lemma, the homomorphism f' is also surjective. So $\mathrm{Ker}\alpha$ is finite, we have $\mathrm{Ker}\alpha = (\mathrm{Sel}(E/\mathbf{Q}_n)^\vee)_{\mathrm{tors}}$ and from the above lemma, f' is bijective. So f is also bijective. □

Lemma 2.4.25. *We have* $\dim_{\mathbf{F}_p} \mathbf{F}_p \otimes_{\mathbf{Z}_p} \Lambda_n/I_n = q_n$.

Proof. We have

$$\Lambda_n \cong \Lambda/((1+T)^{p^n} - 1).$$

Let $t_1(T) = u_1(T)p^{\mu_1}d_1(T)$ and $t_2(T) := u_2(T)p^{\mu_2}d_2(T)$ be the power series corresponding to $\theta_{\mathbf{Q}_n}$ and $\nu_n(\theta_{\mathbf{Q}_{n-1}})$ respectively. Here, $u_1(T), u_2(T) \in \Lambda^\times$ and $d_1(T), d_2(T)$ are distinguished polynomials. Since $\psi_n(\theta_{\mathbf{Q}_n}) = t_1(\zeta_{p^n} - 1)$ and comparing the orders, the degree of $\mu_1 = 0$ and the degree of $d_1(T)$ is q_n. We have

$$\begin{aligned} & \mathbf{F}_p \otimes_{\mathbf{Z}_p} \Lambda_n/I_n \\ \cong\ & \Lambda/(t_1(T), t_2(T), (1+T)^{p^n} - 1, p) \\ =\ & \Lambda/(T^{q_n}, p). \end{aligned}$$

Since the dimension of the last space is q_n. We have proved the lemma. □

Proof of 1. of Lemma 2.4.24. By the definitions, $R_1 = 0$ and $r_1 = 0$, thus $\mathrm{ord}_p(\sharp R_1) = r_1$. We have a commutative diagram

$$\begin{array}{ccccccccc} & & & & & & 0 & & \\ & & & & & & \downarrow & & \\ 0 & \longrightarrow & R_{n-1} & \longrightarrow & \Lambda_{n-1}/I_{n-1} & \longrightarrow & \Lambda_1/I_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \beta_n} & & \downarrow{\scriptstyle \nu_n} & & \downarrow{\scriptstyle \times p} & & \\ 0 & \longrightarrow & R_n & \longrightarrow & \Lambda_n/I_n & \longrightarrow & \Lambda_1/I_1 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \psi_n} & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Coker}\beta_n & \longrightarrow & \mathcal{O}_{\psi_n}/(\psi_n(\theta_{\mathbf{Q}_n})) & \longrightarrow & (\mathbf{Z}/p\mathbf{Z})^{q_1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \cdot \end{array} \tag{2.2}$$

Here, the injectivity of the first right arrow of the third line is deduced from the snake lemma. Thus we have

$$\begin{aligned} & \mathrm{ord}_p(\sharp R_n) \\ \leq\ & \mathrm{ord}_p(\sharp R_{n-1}) + \mathrm{ord}_p(\sharp \mathrm{Coker}\beta_n) \\ =\ & r_{n-1} + \mathrm{ord}_p(\mathcal{O}_{\psi_n}/(\psi_n(\theta_{\mathbf{Q}_n}))) - \mathrm{ord}_p(\sharp \mathbf{Z}/p\mathbf{Z})^{q_1} \\ =\ & r_{n-1} + q_n - q_1 \\ =\ & r_n. \end{aligned}$$

□

Proposition 2.4.26. *We have $R_1 = 0$ and*

$$R_n \cong (\mathbf{Z}/p^{n-1}\mathbf{Z})^{q_2-q_1} \oplus (\mathbf{Z}/p^{n-2}\mathbf{Z})^{q_3-q_2} \oplus \cdots \oplus (\mathbf{Z}/p\mathbf{Z})^{q_n-q_{n-1}}$$

for $n \geq 2$.

Proof. First we show $\mathbf{F}_p \otimes_{\mathbf{Z}_p} R_n$. Since the last term of the middle sequence of the diagram (2.2) is a free $\mathbf{Z}_p$-module, the sequence is split. Thus tensoring $\mathbf{F}_p$ preserves the exactness. Since p-rank of R_n and $\mathrm{Coker}\beta_n$ in the diagram (2.2) are both $q_n - q_1$ from Proposition 2.4.5 and Proposition 2.4.6, we have proved the proposition. □

As a corollary of the above proposition, we have 2. of Theorem 2.1.1 if $p = 2$ and Theorem 7.4 in Kurihara [10] if p is odd.

Corollary 2.4.27 (2. of Theorem 2.1.1, Theorem 7.4 in Kurihara [10])**.** For $n \geq 1$, we have

$$\mathrm{Sel}(E/\mathbf{Q}_n) \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{q_1} \oplus (\mathbf{Z}/p^{n-1}\mathbf{Z})^{q_2-q_1} \oplus (\mathbf{Z}/p^{n-2}\mathbf{Z})^{q_3-q_2} \oplus \cdots \oplus (\mathbf{Z}/p\mathbf{Z})^{q_n-q_{n-1}}.$$

Lemma 2.4.28. *For $n \geq 1$, we have* $\mathrm{rank}_{\mathbf{Z}_p}\Lambda_n/I_n = q_1$.

Proof. This follows from the finiteness of R_n. □

We put $G_{n/n-1} := \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q}_{n-1})$.

Lemma 2.4.29. *We have an isomorphism*

$$\mathrm{Sel}(E/\mathbf{Q}_1, T_pE) \cong \mathrm{Sel}(E/\mathbf{Q}_n, T_pE)$$

through the restriction map for $n \geq 1$.

Proof. Since $E(\mathbf{Q}_n)[p] = 0$, $\mathrm{Sel}(E/\mathbf{Q}_n, T_pE)$ is a torsion-free module. From the above lemma, we have

$$q_1 = \mathrm{rank}_{\mathbf{Z}_p}\Lambda_n/I_n \geq \mathrm{corank}_{\mathbf{Z}_p}\mathrm{Sel}(E/\mathbf{Q}_n) \geq \mathrm{rank}_{\mathbf{Z}_p}\mathrm{Sel}(E/\mathbf{Q}_n, T_pE) \geq q_1.$$

Thus $\mathrm{Sel}(E/\mathbf{Q}_n, T_pE)$ is a free $\mathbf{Z}_p$-module of rank q_1. From the inflation-restriction sequence, the restriction map

$$\mathrm{Sel}(E/\mathbf{Q}_{n-1}, T_pE) \to \mathrm{Sel}(E/\mathbf{Q}_n, T_pE)^{G_{n/n-1}}$$

induces an isomorphism. Since $\mathrm{Sel}(E/\mathbf{Q}_n, T_pE)$ has no torsion points, we have $\mathrm{Sel}(E/\mathbf{Q}_n, T_pE)^{G_{n/n-1}} = \mathrm{Sel}(E/\mathbf{Q}_n, T_pE)$. Thus we have proved the lemma. □

Lemma 2.4.30. *For $n \geq 0$, we have*

$$\mathrm{Sel}_0(E/\mathbf{Q}_n, T_pE) = 0.$$

Proof. This follows immediately from $\mathrm{Sel}_0(E/\mathbf{Q}_n) = 0$. □

We will prove 2. of Lemma 2.4.24.

By Proposition 2.4.5, we have $\mathrm{ord}_{\zeta_{2^n-1}}\psi_n(\theta_{\mathbf{Q}_n}) = q_n$. Let S_n be the set of primes of $\mathbf{Q}_n$ above S. By Lemma 2.4.8 and Lemma 2.4.30, we have an exact sequence

$$\begin{aligned} 0 \;&\to\; \mathrm{Sel}(E/\mathbf{Q}_n) \to \mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n}[1/S_n], E[p^\infty]) \to \bigoplus_{v\in S_n} \frac{\mathrm{H}^1((\mathbf{Q}_n)_v, E[p^\infty])}{E((\mathbf{Q}_n)_v)\otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p} \\ &\to\; \mathrm{Sel}(E/\mathbf{Q}_n, T_pE)^\vee \to 0. \end{aligned}$$

Put

$$\begin{aligned} C_n \;&:=\; \mathrm{Im}\Big(\mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n}[1/S_n], E[p^\infty]) \to \bigoplus_{v\in S_n} \frac{\mathrm{H}^1((\mathbf{Q}_n)_v, E[p^\infty])}{E((\mathbf{Q}_n)_v)\otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p}\Big) \\ &=\; \mathrm{Ker}\Big(\bigoplus_{v\in S_n} \frac{\mathrm{H}^1((\mathbf{Q}_n)_v, E[p^\infty])}{E((\mathbf{Q}_n)_v)\otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p} \to \mathrm{Sel}(E/\mathbf{Q}_n, T_pE)^\vee\Big). \end{aligned}$$

Put $G_{n/n-1} = \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q}_{n-1})$. Then we have two commutative diagrams

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_{n-1}) & \longrightarrow & \mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_{n-1}}[1/S_{n-1}], E[p^\infty]) & \longrightarrow & C_{n-1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_n)^{G_{n/n-1}} & \longrightarrow & \mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n}[1/S_n], E[p^\infty])^{G_{n/n-1}} & \longrightarrow & C_n^{G_{n/n-1}} & & \end{array}$$

and

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_{n-1} & \longrightarrow & \displaystyle\bigoplus_{v\in S_{n-1}} \frac{\mathrm{H}^1((\mathbf{Q}_{n-1})_v, E[p^\infty])}{E((\mathbf{Q}_{n-1})_v)\otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p} & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_{n-1}, T_pE)^\vee & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C_n & \longrightarrow & \displaystyle\bigoplus_{v\in S_n} \frac{\mathrm{H}^1((\mathbf{Q}_n)_v, E[p^\infty])}{E((\mathbf{Q}_n)_v)\otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p} & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_n, T_pE)^\vee & \longrightarrow & 0. \end{array}$$

From the inflation-restriction sequence, the center vertical arrow of the first diagram $\mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_{n-1}}[1/S_{n-1}], E[p^\infty]) \to \mathrm{H}^1(\mathcal{O}_{\mathbf{Q}_n}[1/S_n], E[p^\infty])^{G_{n/n-1}}$ is an isomorphism. Thus we have

$$\mathrm{Coker}(\mathrm{Sel}(E/\mathbf{Q}_{n-1}) \to \mathrm{Sel}(E/\mathbf{Q}_n)^{G_{n/n-1}}) = \mathrm{Ker}(C_{n-1} \to C_n^{G_{n/n-1}})$$

from the snake lemma. So, we consider the order of $\mathrm{Ker}(C_{n-1} \to C_n)$. We have

$$\begin{aligned}
& \mathrm{ord}_p(\sharp\mathrm{Ker}(C_{n-1} \to C_n)) \\
\geq\ & \mathrm{ord}_p(\sharp\mathrm{Ker}\Big(\bigoplus_{v\in S_{n-1}} \frac{\mathrm{H}^1((\mathbf{Q}_{n-1})_v, E[p^\infty])}{E((\mathbf{Q}_{n-1})_v)\otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p} \to \bigoplus_{v\in S_n} \frac{\mathrm{H}^1((\mathbf{Q}_n)_v, E[p^\infty])}{E((\mathbf{Q}_n)_v)\otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p}\Big)) \\
-\ & \mathrm{ord}_p(\sharp\mathrm{Ker}(\mathrm{Sel}(E/\mathbf{Q}_{n-1}, T_pE)^\vee \to \mathrm{Sel}(E/\mathbf{Q}_n, T_pE)^\vee)).
\end{aligned}$$

Since

$$\begin{aligned}
& \mathrm{ord}_p(\sharp\mathrm{Ker}\Big(\bigoplus_{v\in S_{n-1}} \frac{\mathrm{H}^1((\mathbf{Q}_{n-1})_v, E[p^\infty])}{E((\mathbf{Q}_{n-1})_v)\otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p} \to \bigoplus_{v\in S_n} \frac{\mathrm{H}^1((\mathbf{Q}_n)_v, E[p^\infty])}{E((\mathbf{Q}_n)_v)\otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p}\Big)) \\
\geq\ & \mathrm{ord}_p(\sharp\mathrm{Ker}\Big(\frac{\mathrm{H}^1(k_{n-1}, E[p^\infty])}{E(k_{n-1})\otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p} \to \frac{\mathrm{H}^1(k_n, E[p^\infty])}{E(k_n)\otimes_{\mathbf{Z}} \mathbf{Q}_p/\mathbf{Z}_p}\Big)) \\
=\ & \mathrm{ord}_p(\sharp\mathrm{Coker}(N_{k_n/k_{n-1}} : \widehat{E}(m_{k_n}) \to \widehat{E}(m_{k_{n-1}}))^\vee) \\
=\ & q_n
\end{aligned}$$

from Lemma 2.4.4 and

$$\begin{aligned}
& \sharp\mathrm{Ker}(\mathrm{Sel}(E/\mathbf{Q}_{n-1}, T_pE)^\vee \to \mathrm{Sel}(E/\mathbf{Q}_n, T_pE)^\vee) \\
=\ & \sharp\mathrm{Coker}(\mathrm{Sel}(E/\mathbf{Q}_n, T_pE) \to \mathrm{Sel}(E/\mathbf{Q}_{n-1}, T_pE)) \\
\cong\ & \sharp(\mathbf{Z}/p\mathbf{Z})^{q_1}
\end{aligned}$$

from Lemma 2.4.29, we have

$$\mathrm{ord}_p(\sharp\mathrm{Coker}(\mathrm{Sel}(E/\mathbf{Q}_{n-1}) \to \mathrm{Sel}(E/\mathbf{Q}_n)^{G_{n/n-1}})) \geq q_n - q_1.$$

We have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (\mathrm{Sel}(E/\mathbf{Q}_n)^\vee)_{\mathrm{tors}} & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_n)^\vee & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_1)^\vee & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \| & & \\
0 & \longrightarrow & (\mathrm{Sel}(E/\mathbf{Q}_{n-1})^\vee)_{\mathrm{tors}} & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_{n-1})^\vee & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_1)^\vee & \longrightarrow & 0.
\end{array}$$

Here, h_2 is surjective. So h_1 is also surjective and we have

$$\mathrm{Ker}h_1 = \mathrm{Ker}h_2.$$

Thus we have

$$\begin{aligned}
& \mathrm{ord}_p(\sharp(\mathrm{Sel}(E/\mathbf{Q}_n)^\vee)_{\mathrm{tors}}) \\
= \; & \mathrm{ord}_p(\sharp(\mathrm{Sel}(E/\mathbf{Q}_{n-1})^\vee)_{\mathrm{tors}}) + \mathrm{ord}_p(\sharp\mathrm{Ker}h_1) \\
= \; & r_{n-1} + \mathrm{ord}_p(\sharp\mathrm{Ker}h_2) \\
= \; & r_{n-1} + \mathrm{ord}_p\sharp\mathrm{Coker}(\mathrm{Sel}(E/\mathbf{Q}_{n-1}) \to \mathrm{Sel}(E/\mathbf{Q}_n)) \\
\geq \; & r_{n-1} + \mathrm{ord}_p\sharp\mathrm{Coker}(\mathrm{Sel}(E/\mathbf{Q}_{n-1}) \to \mathrm{Sel}(E/\mathbf{Q}_n)^{G_{n/n-1}}) \\
\geq \; & r_{n-1} + q_n - q_1 \\
= \; & r_n.
\end{aligned}$$

Thus, we have proved the lemma.

Chapter 3

A homomorphism concerning the zeta elements and the modular elements

3.1 Theorems

We give a homomorphism which concerns about Euler systems for an elliptic curve. We will construct a 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 each $N \geq 1$ and a good prime p. We will prove the theorems below.

Theorem 3.1.1 (Theorem 3.4.1)**.** *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 3.1.2 (Theorem 3.4.3)**.** *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 3.1.3 (Theorem 3.5.1)**.** *If* p *divides* N*,* $\widetilde{E}(\mathbf{F}_p(\mu_N))[p] = 0$ *and an Euler system* $(w_M)_M$ *is integral, namely*

$$(w_M)_M \in \prod_{M|N} \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathbf{Q}(\mu_M), T_pE),$$

then the admissible system $(\mathcal{P}_M(w_M))_M$ *is integral, 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.

3.2 Group rings

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 ξ_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 υ_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 $L \mid L'$ 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 3.2.1. *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 ρ be an eigenvalue of $\widehat{\sigma}_l$, then we have $\rho^n = \rho^{n+r}$, which implies that if $\rho \neq 0$, then ρ is an r-th root of unity. □

Definition 3.2.2. *For a prime number l, we define the number ϵ_l by*

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

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

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

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 3.2.3. *The inverse $F_l(\widehat{\sigma}_l)^{-1}$ exists in $\mathrm{End}_{\mathbf{Q}}(\mathbf{Q}[C_N])$. If $l \nmid N$, 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 $M \mid N$, the map $\mathrm{Nr}_{\mathbf{Q}(\mu_N)/\mathbf{Q}(\mu_M)}$ is simply denoted by $\mathrm{Nr}_{N/M}$.

3.3 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 Φ 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 [2]. The definition below is different from that in [2] 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

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

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

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

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

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

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

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

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 $[\,,\,]_N$. For an abelian field F, we define $\mathcal{G}_F := \mathrm{Gal}(F/\mathbf{Q})$ and for $N \geq 1$, $\mathcal{G}_N := \mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q}) \cong (\mathbf{Z}/N\mathbf{Z})^\times$.

Definition 3.3.1. *For each $x \in D/D^0 \otimes_{\mathbf{Q}} F$ and $z \in \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, V_pE)$, we define*

$$\begin{array}{rcl} P_F(x,z) & := & \sum_{\sigma \in \mathcal{G}_F} \mathrm{tr}_{F/\mathbf{Q}}[\sigma(x), \exp_F^*(z)]\sigma \\ & = & \sum_{\sigma,\tau \in \mathcal{G}_F}[\sigma(x), \tau(\exp_F^*(z))]\sigma\tau^{-1} \in \mathbf{Q}_p[\mathcal{G}_F]. \end{array}$$

For $N \geq 1$, we denote $P_{\mathbf{Q}_(\mu_N)}(x,z)$ by $P_N(x,z)$.

Remark 3.3.2. $P_N(x,z)$ is an analogue of the pairing $P_n(x,z)$ in Kurihara [10] §3.

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

Lemma 3.3.3. *For an element $A \in \mathbf{Q}_p[\mathcal{G}_F]$, we have*

$$\begin{array}{rcl} P_F(Ax,z) & = & A^* P_F(x,z) \\ P_F(x,Az) & = & A P_F(x,z). \end{array}$$

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

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

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

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

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

Definition 3.3.4. *Let F be an abelian field of conductor N. We define x'_N and x_N by*

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

and define $x_F \in D/D^0 \otimes_{\mathbf{Q}} F$ by

$$x_F := \mathrm{tr}_{\mathbf{Q}(\mu_N)/F}(x_N).$$

We define the homomorphism

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

by $\mathcal{P}_F(z) := P_F(x_F, z)$. Here, $F_l(T)$ is the polynomial in Definition 3.2.2. We denote $\mathcal{P}_{\mathbf{Q}(\mu_N)}(z)$ by $\mathcal{P}_N(z)$.

Proposition 3.3.5. *Assume q is a prime number and $N \geq 1$ is an integer. Then, we have*

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

Before proving the proposition, we prove a lemma.

Lemma 3.3.6. *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 $n \geq 1$,*

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

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

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

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

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

Remark 3.3.7. The sequence $(c_n^{(l)})_{n\geq 0}$ is a generalization of the sequence (c_n) in section 2.2.1 in Kurihara [10].

Proof. It is enough to show that

$$\sum_{i=0}^{n-1} c_{i+1}^{(l)} F_l(\widehat{\sigma}_l) \widehat{\sigma}_l^i + \widetilde{F}_l^{(n)}(\widehat{\sigma}_l) \widehat{\sigma}_l^n = 1. \tag{3.1}$$

We will prove the equation (3.1) 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

$$\widetilde{F}_l^{(n)}(\widehat{\sigma}_l) \widehat{\sigma}_l^n = c_{n+1}^{(l)} F_l(\widehat{\sigma}_l) \widehat{\sigma}_l^n + \widetilde{F}_l^{(n+1)}(\widehat{\sigma}_l) \widehat{\sigma}_l^{n+1} \tag{3.2}$$

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

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

Multiplying $\widehat{\sigma}_l^n$, we have proved the equation (3.2). Thus, we have proved the lemma. □

Proof of Proposition 3.3.5. We will prove the same formula for x'_N. Put $N = q^n M$ with $(q, M) = 1$.

Since we have $F_l(\widehat{\sigma}_l)^{-1} = 1 + (\frac{a_l}{l} - \frac{\epsilon_l}{l}\widehat{\sigma}_l)F_l(\widehat{\sigma}_l)^{-1}\widehat{\sigma}_l$ from Lemma 3.3.6 and $\widehat{\sigma}_q(\xi_{qN}) = \xi_N$, we have

$$\begin{aligned}
& \mathrm{tr}_{qN/N}(x'_{qN}) \\
= \; & \mathrm{tr}_{qN/N}(\upsilon_{qN}((\prod_{l|qN} F_l(\widehat{\sigma}_l)^{-1})\xi_{qN})) \\
= \; & \mathrm{tr}_{qN/N}(\upsilon_{qN}(F_q(\widehat{\sigma}_q)^{-1}(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1})\xi_{qN})) \\
= \; & \mathrm{tr}_{qN/N}(\upsilon_{qN}((1 + (\frac{a_q}{q} - \frac{\epsilon_q}{q}\widehat{\sigma}_q)F_q(\widehat{\sigma}_q)^{-1}\widehat{\sigma}_q)(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1})\xi_{qN})) \\
= \; & \mathrm{tr}_{qN/N}(\upsilon_{qN}((\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1})\xi_{qN})) \\
& + \frac{a_q}{q}\mathrm{tr}_{qN/N}(\upsilon_N(F_q(\widehat{\sigma}_q)^{-1}(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1})\xi_N)) \\
& - \frac{\epsilon_q}{q}\mathrm{tr}_{qN/N}(\upsilon_N(F_q(\widehat{\sigma}_q)^{-1}(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1})\widehat{\sigma}_q(\xi_N))). \qquad (3.3)
\end{aligned}$$

First, we treat the first term of the right hand side of the equation (3.3). As we have seen in §1, we have

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

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

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

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

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

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

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

Thus we have

$$\begin{aligned}
& \mathrm{tr}_{qN/N}(\upsilon_{qN}((\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1})\xi_{qN})) \\
= \ & \begin{cases} 0 & (n \geq 1) \\ -(\sigma_q^{-1} - \frac{a_q}{q} + \frac{\epsilon_q}{q}\sigma_q)F_q(\sigma_q)^{-1}x'_N & (n = 0) \end{cases} .
\end{aligned} \tag{3.4}$$

Next, we treat the second term of the equation (3.3). 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 $q \mid N$ and multiplication by $q-1$ if $q \nmid N$. We also have

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

if $q \mid N$. Thus we obtain

$$\begin{aligned} & \frac{a_q}{q}\mathrm{tr}_{qN/N}(\upsilon_N(F_q(\widehat{\sigma}_q)^{-1}(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1})\xi_N)) \\ = & \begin{cases} a_q x'_N & (n \geq 1) \\ \frac{(q-1)a_q}{q} F_q(\sigma_q)^{-1} x'_N & (n = 0). \end{cases} \end{aligned} \tag{3.5}$$

We then treat the third term of the equation (3.3). Since we have $\widehat{\sigma}_q(\xi_N) = \xi_{\frac{N}{q}}$ if $q \mid N$ 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 $q^2 \mid N$, we have

$$\begin{aligned} & \frac{\epsilon_q}{q}\mathrm{tr}_{qN/N}(\upsilon_N(F_q(\widehat{\sigma}_q)^{-1}(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1})\widehat{\sigma}_q(\xi_N))) \\ = & \begin{cases} \epsilon_q x'_{\frac{N}{q}} & (n \geq 2) \\ \epsilon_q F_q(\sigma_q)^{-1} x'_{\frac{N}{q}} & (n = 1) \\ \frac{\epsilon_q}{q}(q-1)\sigma_q F_q(\sigma_q)^{-1} x'_N & (n = 0). \end{cases} \end{aligned} \tag{3.6}$$

Combining the equations (3.4), (3.5) and (3.6), if $q^2 \mid N$, we have

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

If $q \,||\, N$, we have

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

If $q \nmid N$, we have

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

Thus, we have proved the proposition. □

3.4 Euler systems and admissible systems

In the introduction, we introduced two system, namely Euler systems and admissible system. We will prove the theorem below.

Theorem 3.4.1. *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 3.4.2. *Let K/F be an extension of abelian fields. For $x \in D \otimes_{\mathbf{Q}} K$ and $z \in \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} K, V_pE)$, we have*

$$\pi_{K/F}(P_K(x,z)) = P_F(\mathrm{tr}_{K/F}(x), \mathrm{Nr}_{K/F}(z)).$$

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

$$P_K(x,z) = \nu_{K/F}(P_F(x, \mathrm{Nr}_{K/F}(z))).$$

Proof. For $x \in D \otimes_{\mathbf{Q}} K$ and $z \in \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} K, V_pE)$, an easy calculation

shows that

$$\begin{aligned}
& \pi_{K/F}(P_K(x,z)) \\
= \ & \pi_{K/F}(\sum_{s,t\in\mathcal{G}_K}[s(x),\exp_K^*(t(z))]st^{-1}) \\
= \ & \sum_{s,t\in\mathcal{G}_K}[s(x),\exp_K^*(t(z))]\pi_{K/F}(st^{-1}) \\
= \ & \sum_{\sigma,\tau\in\mathcal{G}_F}(\sum_{s,t\in\mathcal{G}_K,\pi_{K/F}(s)=\sigma,\pi_{K/F}(t)=\tau}[s(x),t(\exp_K^*(z))])\sigma\tau^{-1} \\
= \ & \sum_{\sigma,\tau\in\mathcal{G}_F}[\sum_{s\in\mathcal{G}_K,\pi_{K/F}(s)=\sigma}s(x),\sum_{t\in\mathcal{G}_K,\pi_{K/F}(t)=\tau}t(\exp_K^*(z))]\sigma\tau^{-1} \\
= \ & \sum_{\sigma,\tau\in\mathcal{G}_F}[\sigma(\mathrm{tr}_{K/F}(x)),\tau(\mathrm{tr}_{K/F}(\exp_K^*(z)))]\sigma\tau^{-1} \\
= \ & \sum_{\sigma,\tau\in\mathcal{G}_F}[\sigma(\mathrm{tr}_{K/F}(x)),\exp_F^*(\tau(\mathrm{Nr}_{K/F}(z)))]\sigma\tau^{-1} \\
= \ & P_F(\mathrm{tr}_{K/F}(x),\mathrm{Nr}_{K/F}(z)).
\end{aligned}$$

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

Similarly, for $x\in D\otimes_{\mathbf{Q}}F$ and $z\in\mathrm{H}^1(\mathbf{Q}_p\otimes_{\mathbf{Q}}K,V_pE)$, we have

$$\begin{aligned}
& \nu_{K/F}(P_F(x,\mathrm{Nr}_{K/F}(z))) \\
= \ & \nu_{K/F}(\sum_{\sigma,\tau\in\mathcal{G}_F}[\sigma(x),\exp_F^*(\tau(\mathrm{Nr}_{K/F}(z)))]\sigma\tau^{-1}) \\
= \ & \sum_{\rho\in\mathcal{G}_K}(\sum_{\sigma,\tau\in\mathcal{G}_F,\pi_{K/F}(\rho)=\sigma\tau^{-1}}[\sigma(x),\exp_F^*(\tau(\mathrm{Nr}_{K/F}(z)))])\rho \\
= \ & \sum_{\rho\in\mathcal{G}_K}(\sum_{\sigma,\tau\in\mathcal{G}_F,\pi_{K/F}(\rho)=\sigma\tau^{-1}}[\sigma(x),\tau(\mathrm{tr}_{K/F}(\exp_K^*(z)))])\rho \\
= \ & \sum_{\rho\in\mathcal{G}_K}(\sum_{\sigma,\tau\in\mathcal{G}_F,\pi_{K/F}(\rho)=\sigma\tau^{-1}}[\sigma(x),\sum_{t\in\mathcal{G}_K,\pi_{K/F}(t)=\tau}t(\exp_K^*(z))])\rho \\
= \ & \sum_{\rho,t\in\mathcal{G}_K,\sigma,\tau\in\mathcal{G}_F,\pi_{K/F}(\rho)=\sigma\tau^{-1},\pi_{K/F}(t)=\tau}[\sigma(x),t(\exp_K^*(z))]\rho.
\end{aligned}$$

The condition $\pi_{K/F}(\rho)=\sigma\tau^{-1}$ and $\pi_{K/F}(t)=\tau$ is equivalent that $\pi_{K/F}(\rho t)=$

σ and $\pi_{K/F}(t) = \tau$. Putting $s = \rho t \in \mathcal{G}_K$, we obtain

$$\begin{aligned}
& \sum_{\rho,t\in\mathcal{G}_K,\sigma,\tau\in\mathcal{G}_F,\pi_{K/F}(\rho)=\sigma\tau^{-1},\pi_{K/F}(t)=\tau} [\sigma(x), t(\exp_K^*(z))]\rho \\
= & \sum_{s,t\in\mathcal{G}_K,\sigma,\tau\in\mathcal{G}_F,\pi_{K/F}(s)=\sigma,\pi_{K/F}(t)=\tau} [\sigma(x), t(\exp_K^*(z))]st^{-1} \\
= & \sum_{s,t\in\mathcal{G}_K} [s(x), \exp_K^*(t(z))]st^{-1} \\
= & P_K(x,z)
\end{aligned}$$

Thus, we have proved the lemma. □

Proof of Theorem 3.4.1. From Definition 3.3.4 and Lemma 3.4.2, we have

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

If $q^2 \mid M$, from Proposition 3.3.5, we have

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

Applying Lemma 3.4.2 by $L = \frac{M}{q}$, we have

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

Thus, we have proved that

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

If $q \mid\mid M$, then we have

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

Here, we used Lemma 3.3.3.

If $q \nmid M$, then we have

$$\begin{aligned}
& P_M(\mathrm{tr}_{qM/M}(x_{qM}), \mathrm{Nr}_{qM/M}(w_{qM})) \\
= \; & P_M((a_q - \epsilon_q \sigma_q - \sigma_q^{-1}) F_q(\sigma_q)^{-1} x_M, F_q(\sigma_q^{-1}) w_M) \\
= \; & (a_q - \sigma_q - \epsilon_q \sigma_q^{-1}) \mathcal{P}_M(w_M)\,.
\end{aligned}$$

Thus, we have proved the theorem. □

Theorem 3.4.3. *For the notations as above, we have* $\mathcal{P}_N(z_N) = \theta_N$.

To prove this theorem, we need some lemmas.

Lemma 3.4.4. *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* χ *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 χ of $\mathcal{G}_M$. From the assumption, $\chi(\eta_M) = \chi(\kappa_M)$ for each character χ of conductor M. If the conductor of χ is not equal to M, then we can regard χ 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 $\pi_{M/\frac{M}{q}}(\eta_M) = a_q \eta_{\frac{M}{q}} - \epsilon_q \nu_{\frac{M}{q}/\frac{M}{q^2}}(\eta_{\frac{M}{q^2}})$ and $\pi_{M/\frac{M}{q}}(\kappa_M) = a_q \kappa_{\frac{M}{q}} - \epsilon_q \nu_{\frac{M}{q}/\frac{M}{q^2}}(\kappa_{\frac{M}{q^2}})$. 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 $q \mid\mid M$, then we have

$$\pi_{M/\frac{M}{q}}(\eta_M) = (a_q - \sigma_q - \epsilon_q \sigma_q^{-1})\eta_{\frac{M}{q}} = (a_q - \sigma_q - \epsilon_q \sigma_q^{-1})\kappa_{\frac{M}{q}} = \pi_{M/\frac{M}{q}}(\kappa_M).$$

Thus we have proved the lemma. □

Lemma 3.4.5. *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 χ 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 χ^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 χ 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 3.4.4, we have $\eta_M = \kappa_M$. Thus we have proved the lemma. □

Proof of Theorem 3.4.3. From Lemma 3.4.5, it is enough to show that for a character χ of conductor N, the χ part of the both hands are equal.

A direct calculation shows that

$$\begin{aligned} & \chi(\mathcal{P}_N(z_N)) \\ = & \sum_{\sigma,\tau \in \mathcal{G}_N} [\sigma(x_N), \tau(\exp_N^*(z_N))]\chi(\sigma)\chi(\tau^{-1}) \\ = & \left[\sum_{\sigma \in \mathcal{G}_N} \sigma(x_N)\chi(\sigma), \sum_{\tau \in \mathcal{G}_N} \tau(\exp_N^*(z_N))\chi^{-1}(\tau)\right]. \end{aligned} \tag{3.7}$$

We first treat the right half of the pairing of the equation (3.7). 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

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

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

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

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 (3.7) that

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

Thus, we have proved the equality. □

3.5 Integrality of the map

In this section, we will prove the following theorem.

Theorem 3.5.1. *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 $S(N) := \{l : \text{prime number} | \, e_l > 0\}$, 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 3.3.6, we have

$$\begin{aligned}
x_N &= \upsilon_N((\prod_{l|N} F_l(\widehat{\sigma}_l)^{-1})\xi_N)\omega^* \\
&= \upsilon_N(F_p(\widehat{\sigma}_p)^{-1}(\prod_{l|M} F_l(\widehat{\sigma}_l)^{-1})\xi_N)\omega^* \\
&= \upsilon_N(F_p(\widehat{\sigma}_p)^{-1}(\prod_{l|M}(\sum_{i=0}^{e_l-1} c_i^{(l)}\widehat{\sigma}_l^i + \widetilde{F}_l^{(e_l)}(\widehat{\sigma}_l)F_l(\widehat{\sigma}_l)^{-1}\widehat{\sigma}_l^{e_l}))\xi_N)\omega^* \\
&= \upsilon_N(F_p(\widehat{\sigma}_p)^{-1}\sum_{S\subset S(M)}(\prod_{l'\notin S}\sum_{i=0}^{e_{l'}-1} c_i^{(l')}\widehat{\sigma}_{l'}^i)(\prod_{l\in S}\widetilde{F}_l^{(e_l)}(\widehat{\sigma}_l)F_l(\widehat{\sigma}_l)^{-1}\widehat{\sigma}_l^{e_l})\xi_N)\omega^* \\
&= \sum_{S\subset S(M)}\upsilon_N(F_p(\widehat{\sigma}_p)^{-1}(\prod_{l'\notin S}\sum_{i=0}^{e_{l'}-1} c_i^{(l')}\widehat{\sigma}_{l'}^i)(\prod_{l\in S}\widetilde{F}_l^{(e_l)}(\widehat{\sigma}_l)F_l(\widehat{\sigma}_l)^{-1})\xi_{N_S})\omega^*.
\end{aligned}$$

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

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

Here, the coefficients of γ_S are in $\mathbf{Z}_{(p)} = \{\frac{a}{b} \in \mathbf{Q} | a, b \in \mathbf{Z}, p \nmid b\}$ 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, $\log_{\widehat{E}}$ is the formal logarithm of the formal group $\widehat{E}$ and for an abelian field F, we put $\log_{\widehat{E}}(\widehat{E}(m_F)) := \prod_{v|p}\log_{\widehat{E}}(\widehat{E}(m_{F_v}))$, and we put $\log(\widehat{E}(m_F)) := \log_{\widehat{E}}(\widehat{E}(m_F))\omega^* \subset D/D^0 \otimes_{\mathbf{Q}} F$.

Lemma 3.5.2. *Let $\alpha \in \log(\widehat{E}(m_F))$ and $w \in \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, T_pE)$. Then we have*

$$P_F(\alpha, w) \in \mathbf{Z}_p[\mathcal{G}_F].$$

Proof. From the definition, we have

$$\begin{aligned}
& P_F(\alpha, w) \\
= & \sum_{\sigma\in\mathcal{G}_F} \mathrm{tr}_{F/\mathbf{Q}}[\sigma(\alpha), w]\sigma.
\end{aligned}$$

So what we have to prove is that $\mathrm{tr}_{F/\mathbf{Q}}[\sigma(\alpha), \exp_F^*(w)] \in \mathbf{Z}_p$. But this follows from the fact that $\sigma(\alpha)$ is in the image of log because the formal logarithm map is Galois compatible, and the commutativity of the following diagram

$$\begin{array}{ccccc} \widehat{E}(m_F) & \times & \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, T_pE) & \to & \mathbf{Z}_p \\ \downarrow \log & & \downarrow \exp_F^* & & \downarrow \\ D/D_0 \otimes_{\mathbf{Q}_p} (\mathbf{Q}_p \otimes_{\mathbf{Q}} F) & \times & D_0 \otimes_{\mathbf{Q}_p} (\mathbf{Q}_p \otimes_{\mathbf{Q}} F) & \to & \mathbf{Q}_p \end{array} ,$$

where the pairing in the upper row is the composite of the Kummer map $\widehat{E}(m_F) \to \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, T_pE)$ and

$$[,]_F : \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, T_pE) \times \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, T_pE) \to \mathbf{Z}_p,$$

and the pairing in the lower row is $\mathrm{tr}_{F/\mathbf{Q}}[,]$.

□

Lemma 3.5.3. *If $\alpha_S \in \log(m_{\mathbf{Q}(\mu_{N_S})})$ 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

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

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

Proof of Lemma 3.5.3. From the definition, we get

$$\begin{aligned} & P_F(y, w_F) \\ = \; & P_F(\sum_{S \subset S(M)} (\prod_{l \in S} F_l(\sigma_l)^{-1})\alpha_S, w_F) \\ = \; & \sum_{S \subset S(M)} P_F((\prod_{l \in S} F_l(\sigma_l)^{-1})\alpha_S, w_F) \\ = \; & \sum_{S \subset S(M)} \nu_{F/F_S}(P_{F_S}((\prod_{l \in S} F_l(\sigma_l)^{-1})\alpha_S, \mathrm{Nr}_{F/F_S}(w_F))). \end{aligned}$$

We have

$$\begin{aligned} & \nu_{F/F_S}(P_{F_S}((\prod_{l\in S} F_l(\sigma_l)^{-1})\alpha_S, \mathrm{Nr}_{F/F_S}(w_F))) \\ = \; & \nu_{F/F_S}(P_{F_S}((\prod_{l\in S} F_l(\sigma_l)^{-1})\alpha_S, (\prod_{l\in S} F_l(\sigma_l^{-1}))w_S)) \\ = \; & \nu_{F/F_S}(P_{F_S}(\alpha_S, w_S)). \end{aligned}$$

From the previous lemma, we have

$$P_{F_S}(\alpha_S, w_S) \in \mathbf{Z}_p[\mathcal{G}_{F_S}].$$

Thus we have proved the lemma. □

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 σ_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

$$\mathcal{C}_K := \{f(T) \in K[[T]] \mid f(x) \text{ converges for any } x \in \overline{\mathbf{Q}_p} \text{ such that } |x|_p < 1\},$$

i.e. the ring of power series whose radius of convergence is ≥ 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 ϕ.

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

$$\begin{array}{rcl} \alpha & \mapsto & \sigma(\alpha) \\ \xi_{p^n} & \mapsto & \xi_{p^n}^p \end{array}$$

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 3.5.4. *There is an isomorphism*

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

and the diagrams

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

and

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

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 ϕ 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 ς_n and υ_{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 [4].

Proposition 3.5.5. *We have*

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

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 [6] 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 3.5.6. *Assume that $\widetilde{E}(k)[p] = 0$. Then we have*

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

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

$$\begin{aligned} & (1 - \frac{a_p}{p}\phi + \frac{1}{p}\phi^2) \log_{\hat{E}}(\alpha T^i) \\ =\ & (\alpha - a_p p^{i-1}\alpha^{\sigma} + p^{2i-1}\alpha^{\sigma^2})T^i + r(T) \end{aligned}$$

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

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

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

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

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 α_p, β_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 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

$$\begin{aligned} & (1 - \frac{a_p}{p}\phi + \frac{1}{p}\phi^2) \log_{\hat{E}}(p^j u) \\ \equiv \quad & -a_p p^{j-1} u^{\sigma} + p^{j-1} u^{\sigma^2} \pmod{p^j}. \end{aligned}$$

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 a power series satisfying

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

Then, from the arguments above,

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

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

3.6 Kernel of the map

In this section we prove the next proposition. This was used in the proof of Proposition 2.4.20.

Proposition 3.6.1. *Let p be a supersingular prime. Let $\mathbf{Q}_\infty/\mathbf{Q}$ be the cyclotomic $\mathbf{Z}_p$-extension and $\mathbf{Q}_n$ its n-th layer. Let k_n be the p-adic completion of $\mathbf{Q}_n$. Then the kernel of the map*

$$\begin{aligned} \widehat{P}_n : \mathrm{H}^1(k_n, T_pE) & \to \mathbf{Z}_p[\mathcal{G}_{\mathbf{Q}_n}]^2 \\ w & \mapsto (\mathcal{P}_{\mathbf{Q}_n}(w), \nu_n \circ \mathcal{P}_{\mathbf{Q}_{n-1}} \circ \mathrm{Nr}_{\mathbf{Q}_n/\mathbf{Q}_{n-1}}(w)) \end{aligned}$$

is $E(k_n)\widehat{\otimes}\mathbf{Z}_p$.

Proposition 3.6.2. *Let F be an abelian field. Let $\alpha \in \widehat{E}(m_F)$. Then the kernel of the map*

$$P_F(\log(\alpha), \cdot\,) : \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, T_pE) \to \mathbf{Z}_p[\mathcal{G}_F]$$

is $(\langle\alpha\rangle_{\mathbf{Z}_p[\mathcal{G}_F]})^\perp$. Here $(\cdot)^\perp$ is the exact annihilator with respect to the cup product

$$\mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, T_pE) \times \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, T_pE) \to \mathbf{Z}_p.$$

Proof. This follows immediately from the definition. □

Corollary 3.6.3. Let F be an abelian field. Let $\alpha, \beta \in \widehat{E}(m_F)$. Then the kernel of the map

$$\begin{aligned} P : \mathrm{H}^1(\mathbf{Q}_p \otimes_{\mathbf{Q}} F, T_pE) &\to \mathbf{Z}_p[\mathcal{G}_F]^2 \\ w &\mapsto (P_F(\log(\alpha), w), P_F(\log(\beta), w)) \end{aligned}$$

is $(\langle\alpha, \beta\rangle_{\mathbf{Z}_p[\mathcal{G}_F]})^\perp$.

As we have seen in the previous section, there exists $\alpha_{qp^n} \in \widehat{E}(m_{\mathbf{Q}(\mu_{qp^n})})$ such that $\log(\alpha_{qp^n}) = x_{qp^n}$.

Lemma 3.6.4. *We have*

$$\widehat{E}(m_{\mathbf{Q}(\mu_q)}) = \langle\alpha_q\rangle_{\mathbf{Z}_p[\mathcal{G}_q]},$$

and

$$\widehat{E}(m_{\mathbf{Q}(\mu_{qp^n})}) = \langle\alpha_{qp^n}, \alpha_{qp^{n-1}}\rangle_{\mathbf{Z}_p[\mathcal{G}_{qp^n}]}$$

for $n \geq 1$.

Proof. Since p is supersingular,

$$\log_{\hat{E}} : \widehat{E}(m_{\mathbf{Q}(\mu_q)}) \to m_{\mathbf{Q}(\mu_q)}$$

is an isomorphism. We have to show x'_q generates $m_{\mathbf{Q}(\mu_q)}$. First, we assume that p is an odd prime. An easy calculation shows that

$$\begin{aligned} & x'_p \\ = \;& \zeta_p + (\frac{a_p}{p} - \frac{1}{p})F_p(1)^{-1} \\ = \;& \zeta_p - 1 + \frac{p}{p - a_p + 1} \end{aligned}$$

Since $\zeta_p - 1$ generates $m_{\mathbf{Q}(\mu_q)}$ as a $\mathbf{Z}_p[\mathcal{G}_q]$-module, x'_q generates $m_{\mathbf{Q}(\mu_q)}/pm_{\mathbf{Q}(\mu_q)}$. From Nakayama's lemma, x'_q generates $m_{\mathbf{Q}(\mu_q)}$.

If $p = 2$, then we have

$$\begin{aligned} & x'_4 \\ = \ & \zeta_4 - c_2^{(2)} + F_2^{(2)}(1)F_2(1)^{-1} \\ = \ & \zeta_4 - 1 + \frac{2 - a_2 - 2(2 - a_2)c_2}{2 - a_2 + 1} \end{aligned}$$

By the similar arguments above, x'_4 generates $m_{\mathbf{Q}(\mu_4)}$. Thus we have proved the first half of the lemma.

We will prove the latter half by induction. We will prove that $\alpha_{qp^{n+1}}$ generates $\widehat{E}(m_{\mathbf{Q}(\mu_{qp^{n+1}})})/\widehat{E}(m_{\mathbf{Q}(\mu_{qp^n})})$. The formal logarithm map induces an injection

$$\begin{aligned} \log_{\hat{E}} : \widehat{E}(m_{\mathbf{Q}(\mu_{qp^{n+1}})})/\widehat{E}(m_{\mathbf{Q}(\mu_{qp^n})}) \ & \to \ (m_{\mathbf{Q}(\mu_{qp^{n+1}})} + \mathbf{Q}_p(\mu_{qp^n}))/\mathbf{Q}_p(\mu_{qp^n}) \\ & \cong \ m_{\mathbf{Q}(\mu_{qp^{n+1}})}/m_{\mathbf{Q}(\mu_{qp^n})}. \end{aligned}$$

The element $\alpha_{qp^{n+1}}$ corresponds to $x_{qp^{n+1}} \cong \zeta_{qp^{n+1}} - 1 \pmod{\mathbf{Q}_p(\mu_{qp^n})}$. Since $\zeta_{qp^{n+1}} - 1$ generates $m_{\mathbf{Q}(\mu_{qp^{n+1}})}/m_{\mathbf{Q}(\mu_{qp^n})}$, $\alpha_{qp^{n+1}}$ generates

$$\widehat{E}(m_{\mathbf{Q}(\mu_{qp^{n+1}})})/\widehat{E}(m_{\mathbf{Q}(\mu_{qp^n})}).$$

Since $\mathrm{tr}_{qp^{n+1}/qp^n} x_{qp^{n+1}} = a_p x_{qp^n} - x_{qp^{n-1}}$, we have

$$N_{qp^{n+1}/qp^n} \alpha_{qp^{n+1}} = a_p \alpha_{qp^n} - \alpha_{qp^{n-1}}.$$

Thus $\alpha_{qp^{n+1}}$ and α_{qp^n} generates $\widehat{E}(m_{\mathbf{Q}(\mu_{qp^{n+1}})})$. □

Put $\alpha_{\mathbf{Q}_n} := N_{\mathbf{Q}(\mu_{qp^n})/\mathbf{Q}_n}(\alpha_{qp^n})$. Then, we have the following lemma.

Lemma 3.6.5. *Let* $\alpha_{\mathbf{Q}_n}, \alpha_{\mathbf{Q}_{n-1}} \in \widehat{E}(m_{\mathbf{Q}_n})$ *be elements such that* $\log(\alpha_{\mathbf{Q}_n}) = x_{\mathbf{Q}_n}$ *and* $\log(\alpha_{\mathbf{Q}_{n-1}}) = x_{\mathbf{Q}_{n-1}}$. *Then we have*

$$\widehat{E}(m_{\mathbf{Q}_n}) = \langle \alpha_{\mathbf{Q}_n}, \alpha_{\mathbf{Q}_{n-1}} \rangle_{\mathbf{Z}_p[\mathcal{G}_{\mathbf{Q}_n}]}.$$

Proof. We only have to show that $N_{\mathbf{Q}_p(\mu_{qp^n})/k_n}$ is surjective. Let e and f be the ramification index and the order of the different of the extension $\mathbf{Q}(\mu_{qp^n})/k_n$ respectively. If $p = 2$, we have $e = f = 2$. If $p \geq 3$, we have $e = f = p - 1$. In both cases, $f \leq 2e - 2$. From Lemma 2.4.3, the norm map is surjective. □

Proof of Proposition 3.6.1. Since we have

$$\mathcal{P}_{\mathbf{Q}_n}(w) = P_{\mathbf{Q}(\mu_n)}(x_{\mathbf{Q}_n}, w)\nu_n \circ \mathcal{P}_{\mathbf{Q}_{n-1}} \circ \mathrm{Nr}_{\mathbf{Q}_n/\mathbf{Q}n-1}(w) = P_{\mathbf{Q}(\mu_n)}(x_{Q_{n-1}}, w),$$

the kernel of the map $\widehat{P}_n$ is $\langle \alpha_{\mathbf{Q}_n}, \alpha_{\mathbf{Q}_{n-1}} \rangle^{\perp}_{\mathbf{Z}_p[\mathcal{G}_{\mathbf{Q}_n}]} = \widehat{E}(m_{\mathbf{Q}_n})^{\perp} = (E(k_n)\widehat{\otimes}\mathbf{Z}_p)^{\perp}$. Since the exact annihilator of $E(k_n)\widehat{\otimes}\mathbf{Z}_p$ is $E(k_n)\widehat{\otimes}\mathbf{Z}_p$ itself, we have proved the proposition. □

Lemma 3.6.6. *Let $(\eta_{p^n})_n$ and $(\kappa_{p^n})_n$ be two admissible systems. Then*

$$\nu_{p^{n+1}/p^n}(\eta_{p^n})\kappa_{p^{n+1}} = \eta_{p^{n+1}}\nu_{p^{n+1}/p^n}(\kappa_{p^n}).$$

Proof. Since both of the right and left hand side of the equation is in $\nu_{p^{n+1}/p^n}(\mathbf{Q}_p[\mathcal{G}_{p^n}])$, it suffices to show the equality

$$\pi_{p^{n+1}/p^n}(\nu_{p^{n+1}/p^n}(\eta_{p^n})\kappa_{p^{n+1}}) = \pi_{p^{n+1}/p^n}(\eta_{p^{n+1}}\nu_{p^{n+1}/p^n}(\kappa_{p^n})).$$

First we assume that $n = 0$. Then we have

$$\begin{aligned} & \pi_{p/1}(\nu_{p/1}(\eta_1)\kappa_p) \\ = \ & (p-1)\eta_1\pi_{p/1}(\kappa_p) \\ = \ & (p-1)\eta_1(a_p - 1 - \epsilon_p)\kappa_1. \end{aligned}$$

We also have

$$\begin{aligned} & \pi_{p/1}(\eta_p\nu_{p/1}(\kappa_1)) \\ = \ & \pi_{p/1}(\eta_p)(p-1)\kappa_1 \\ = \ & (a_p - 1 - \epsilon_p)\eta_1(p-1)\kappa_1. \end{aligned}$$

Thus we have proved the equality in the case when $n = 0$. Next, we assume that $n \geq 1$. We will prove the equation by induction. Then the left hand side of the equation is

$$\begin{aligned} & \pi_{p^{n+1}/p^n}(\nu_{p^{n+1}/p^n}(\eta_{p^n})\kappa_{p^{n+1}}) \\ = \ & p\eta_{p^n}\pi_{p^{n+1}/p^n}(\kappa_{p^{n+1}}) \\ = \ & p\eta_{p^n}(a_p\kappa_{p^n} - \epsilon_p\nu_{p^n/p^{n-1}}(\kappa_{p^{n-1}})). \end{aligned}$$

The right hand is

$$\begin{aligned} & \pi_{p^{n+1}/p^n}(\eta_{p^{n+1}}\nu_{p^{n+1}/p^n}(\kappa_{p^n})) \\ = \ & \pi_{p^{n+1}/p^n}(\eta_{p^{n+1}})p\kappa_{p^n} \\ = \ & (a_p\eta_{p^n} - \epsilon_p\nu_{p^n/p^{n-1}}(\eta_{p^{n-1}}))p\kappa_{p^n}. \end{aligned}$$

From the assumption of the induction, we have

$$\eta_{p^n}\nu_{p^n/p^{n-1}}(\kappa_{p^{n-1}}) = \nu_{p^n/p^{n-1}}(\eta_{p^{n-1}})\kappa_{p^n}\,.$$

Thus, we have proved the lemma. □

Bibliography

[1] Breuil, C., Conrad, B., Diamond, F., Taylor, R.: *On the modularity of elliptic curves over* $\mathbf{Q}$*, or* 3*-adic exercises*, J. Amer. Math. Soc. **14**, (2001), 849-939.

[2] Bloch, S., Kato, K.: *L-functions and Tamagawa number of motives*, in: Grothendieck Festschrift (Vol. I), Prog. in Math. **86** (1990), 333-400.

[3] Coates, J., Sujatha, R.: *Galois cohomology of elliptic curves*, Tata Institute of Fundamental Research Lectures on Math. **88**, Narosa Publishing House, New Delhi (2000).

[4] Coleman, R.: *Division values in local fields*, Invent. Math. **53** (1979), 91-116.

[5] Greenberg, R.: *Iwasawa theory for elliptic curves*, in: Arithmetic theory for elliptic curves, Cetraro, Italy 1997, Springer Lecture Notes in Math. **1716** (1999), 51-144.

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

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

[8] Kobayashi, S.: *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), 1-36.

[9] Kolyvagin, V. A., *Euler systems*, The Grothendieck Festschrift, vol. 2, Birkhauser, (1990), 435-483.

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

[11] Kurihara, M., 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.

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

[13] Mazur, B., Tate, J., Teitelbaum, J.: *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1-48.

[14] Perrin-Riou, B.: *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier **43**, 4 (1993), 945-995.

[15] Pollack, R.: *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** No. 3 (2003), 523-558.

[16] Rubin, K., *The main conjecture*, Appendix to Lang, S., Cyclotomic Fields I and II, Grad. Texts in Math., 121, Springer, (1990), 397-420.

[17] Rubin, K., *The"main conjecture" of Iwasawa theory for imaginary quadratic fields*, Invent. Math., **103** (1991), 25-68.

[18] Serre, J. -P.: *Corps Locaux*, Hermann, Paris, (1968).

[19] Silverman, J.H.: *The arithmetic of elliptic curves*, GTM **106**, Springer-Verlag (1986).