Some analytic quantities yielding arithmetic information about elliptic curves

Masato Kurihara

Abstract

For an elliptic curve E over $\mathbb{Q}$, and a positive integer n satisfying some properties, we introduce analytic quantities δ_n using modular symbols, and give conjectures that these quantities control the maps of reduction modulo primes dividing n on $E(\mathbb{Q})$. These conjectures also describe the structure of Selmer groups and the Tate-Shafarevich group of E. One of the aims of this paper is to provide an exposition on the theory of these analytic quantities. In the direction of the conjectures, we generalize, to all good reduction primes p, an injectivity theorem which was proven only for good ordinary primes in our earlier paper [15].

0 Introduction

The aim of this paper is to introduce a theory on some analytic quantities δ_n and to describe its role in the arithmetic of elliptic curves. This introduction is an exposition of this theory for non-specialists, and we explain here and in the next §1 some fundamental and typical phenomena of this theory.

In general, for an algebraic variety defined over the field of rational numbers $\mathbb{Q}$, the maps given by reduction modulo primes ℓ provide perhaps the first elementary attempt to understand rational points of the variety. In particular, for an elliptic curve E over $\mathbb{Q}$, and for any prime ℓ we write $r_\ell : E(\mathbb{Q}) \to E(\mathbb{F}_\ell)$ for the reduction modulo ℓ map. Let $E(\mathbb{Q})_{\mathrm{tors}}$ denote the torsion subgroup of E. Then we know (using Nagell-Lutz's theorem) that, for any odd prime ℓ at which E has good reduction, r_ℓ induces an injective homomorphism

$$E(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow E(\mathbb{F}_\ell).$$

These maps for several ℓ's give enough information on the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$. In the present paper, we go further, and study the whole Mordell-Weil group $E(\mathbb{Q})$ using the maps r_ℓ's for various good reduction primes ℓ.

For distinct good reduction primes ℓ_1,...,ℓ_r, put $n = \ell_1 \cdot ... \cdot \ell_r$, and denote by r_n the map

$$r_n : E(\mathbb{Q}) \longrightarrow \bigoplus_{\ell | n} E(\mathbb{F}_\ell),$$

whose each ℓ-component is r_ℓ. For a prime number p, we write

$$r_{n,p} : E(\mathbb{Q}) \otimes \mathbb{Z}/p \longrightarrow \bigoplus_{\ell | n} E(\mathbb{F}_\ell) \otimes \mathbb{Z}/p$$

for r_n modulo p, which is a homomorphism of finite dimensional $\mathbb{F}_p$-vector spaces. In the following, we always work with prime numbers ℓ such that $E(\mathbb{F}_\ell) \otimes \mathbb{Z}/p \simeq \mathbb{Z}/p$ and their squarefree products n (for the precise setting, see §1.1).

We fix an odd prime number p at which E has good reduction. In §1.2 we introduce an analytic quantity $\delta_n \in \mathbb{F}_p$, which is defined explicitly using modular symbols (see (3) in §1.2), and which is numerically computable. The first aim of this paper is to formulate conjectures asserting that $\delta_n \in \mathbb{F}_p$ *controls* the homomorphism $r_{n,p}$, and to provide an exposition of these conjectures, with many numerical examples. We also prove Theorem 2.1 which asserts that $\delta_n \neq 0$ implies that $r_{n,p}$ is injective, under some minor conditions (concerning the conditions, see the beginning of §2.2).

For simplicity, we assume only for the rest of this Introduction that both $E(\mathbb{Q})$ and the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ have no element of order p (see §1.4 for more general case). Note that if p is big enough, this condition is satisfied if we admit the conjecture that $Ш(E/\mathbb{Q})$ is finite. We define $\nu(n)$ to be the number of primes dividing n. Following the terminology of our previous paper [15], we say that n is δ-minimal for p if $\delta_n \neq 0$ and $\delta_d = 0$ for every proper divisor d of n. We conjecture that such δ-minimal n always exist. We can always find such n in numerical examples.

Conjecture 0.1. *Assume that n is δ-minimal for p. Then $r_{n,p}$ is bijective, so that*

$$\operatorname{rank} E(\mathbb{Q}) = \nu(n).$$

Conjecture 0.1 predicts a connection of the rank $E(\mathbb{Q})$ with these analytic quantities δ_n, in a form very different from the conjecture of Birch and Swinnerton-Dyer. An important aspect of our conjecture is that a *single* n gives the rank of $E(\mathbb{Q})$. For a more general form of this conjecture on the Selmer group, see Conjecture 1.7 in §1.4.

Next we take general n which is not necessarily δ-minimal and which satisfies $\nu(n) = \operatorname{rank} E(\mathbb{Q})$, and consider a question whether $r_{n,p}$ is bijective or not. We note that the answer to this question gives information on the rational points on E.

Conjecture 0.2. *Let n be such that $\nu(n) = \operatorname{rank} E(\mathbb{Q})$. Then $r_{n,p}$ is bijective if and only if $\delta_n \neq 0$.*

We urge the reader to look at the numerical examples in §1 to understand the phenomenon on the bijectivity of $r_{n,p}$. We prove in this paper the "if" part of this conjecture. Actually, it follows from the injectivity theorem (Theorem 2.1) because the source and the target of $r_{n,p}$ have the same dimension. A remarkable point of this conjecture is the observation that *the converse should also hold*. Thus Conjecture 0.2 asserts that δ_n *completely controls* the bijectivity of $r_{n,p}$.

Concerning the converse, we remark here the following. We can also formulate in §3 some analogous statement for ideal class groups, and prove the "if" part (Theorem 3.1). However, the converse (the "only if" part) does not hold in this case. Also the analogous statement to Conjecture 0.1 does not hold in the class group setting.

We extend $r_{n,p}$ to the classical Selmer group $\mathrm{Sel}(\mathbb{Q}, E[p])$ and a certain Selmer group $\mathrm{Sel}_{\mathcal{F}^n}(\mathbb{Q}, E[p])$ to get maps $r_{n,p}^{\mathrm{Sel}}$ and $r_{n,p}^{\mathcal{F}^n}$. We study these maps and make conjectures in §1.3.

We conjecture that the system $(\delta_n)_n$ should determine not only the Mordell-Weil rank, but also the structure of Selmer groups. A conjecture on the structure of $Ш(E/\mathbb{Q})$ is given in Conjecture 2.3 in §2. When p is a good ordinary prime, this conjecture was studied in our previous papers [15], [14], and proved in [14] Theorem B under several assumptions.

Our injectivity theorem (Theorem 2.1) gives information on the structure of $Ш(E/\mathbb{Q})$. We will give some numerical examples in §2.3 for which we can determine the structures of their Tate-Shafarevich groups.

In this way this theory gives a relationship between the algebraic (arithmetic) objects and the L-values of elliptic cuvres in a different style from the Birch and Swinnerton-Dyer conjecture. We note that the BSD conjecture gives the information on the order of $Ш(E/\mathbb{Q})$, but not on the structure of it (see Examples 3, 4 in §2.3 to understand the difference between our theory and the BSD conjecture). We do not know currently the direct connection of this theory with the BSD conjecture.

We state several conjectures in §1. The numerical examples in §1 would be helpful to understand the subject of this paper. We restrict ourselves to $\mathbb{F}_p$-vector spaces in §1, but we develop in §2 a theory for $\mathbb{Z}/p^m$-modules. We study in §3 the class groups for CM-fields in order to compare them with the theory in §1. In §4 we give proofs of theorems stated in §2.2, especially Theorem 2.1. The key tool of the proof is the Euler systems of Gauss sum type. To construct the Euler systems, we study Iwasawa theory for elliptic curves with supersingular reduction at p. We work on the equivariant Iwasawa theory (see Theorem 4.3), and get a result on the annihilation of Selmer groups (see Theorem 4.7). We give an explicit construction of an equivariant p-adic L-function from modular symbols in §4.2. The strategy of the proof of Theorem 2.1 is the same as that in our previous paper [15]. In this sense this paper is a sequel of [15].

The author would like to thank late John Coates for his hospitality when the author stayed in Cambridge where the author developed the subject in this paper and gave talks on this subject in 2012 and 2019. The author thanks very much John for his interest in the theory of this paper, and for his careful reading of this manuscript and giving the author many comments. The author thanks the organizers, N. Fakhruddin, E. Ghate, A. Nair, C.S Rajan and S. Varma of the International Colloquium on Arithmetic Geometry held in 2020 at Tata Institute for inviting him and for organizing a very pleasant conference. The author also thanks D. Prasad who gave the author his preprint [23] with S. Shekhar during the conference. We determine the structure of the Tate-Shafarevich group in Example 4 in §2.3 of a curve treated in their paper [23].

After the first version of this manuscript was written in 2020, much progress on this theory was made, especially by Ryotaro Sakamoto and Chan-Ho Kim. See Remark 1.8 for the new progress.

1 Reduction maps and Conjectures

1.1 Setting and a problem

We suppose that E is an elliptic curve over $\mathbb{Q}$ with no complex multiplication (for simplicity). We denote by N the conductor of E.

In the following, we *fix* an odd prime number p such that p is a good reduction prime ($p \nmid N$), and the action of the Galois group on the group $E[p]$ of p-torsion points $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\, E[p]$ is surjective. Consider the

set

$$\mathcal{P} = \{\ell : \text{prime} \mid \ell \equiv 1 \pmod{p},\ \ell \nmid N,\ \text{and } E(\mathbb{F}_{\ell_i}) \otimes \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z}\}.$$

We know that $\mathcal{P}$ is an infinite set using Chebotarev density theorem (see [14] §5.8).

We denote by $\mathcal{N}$ the set of squarefree products of primes in $\mathcal{P}$. We suppose that 1 is also in $\mathcal{N}$. For $n \in \mathcal{P}$ we write $\nu(n)$ for the number of primes dividing n.

Let r_ℓ and $r_n = \oplus_{\ell|n} r_\ell : E(\mathbb{Q}) \to \bigoplus_{\ell|n} E(\mathbb{F}_\ell)$ be as in Introduction for $n \in \mathcal{N}$. We consider $r_{n,p}$ which is r_n mod p, and since we fixed p, we write simply r_n for it;

$$r_n : E(\mathbb{Q}) \otimes \mathbb{Z}/p\mathbb{Z} \longrightarrow \bigoplus_{\ell|n} E(\mathbb{F}_\ell) \otimes \mathbb{Z}/p\mathbb{Z} \simeq (\mathbb{Z}/p\mathbb{Z})^{\nu(n)}\ . \tag{1}$$

In this paper we show that this fundamental map is controlled by some analytic quantities δ_n which we introduce in the next subsection.

Before we proceed, we give some numerical examples. We take $n \in \mathcal{N}$ such that $\operatorname{rank} E(\mathbb{Q}) = \nu(n)$. Then our assumption implies $E(\mathbb{Q})[p] = 0$, so r_n in (1) is the map between two $\mathbb{F}_p$-vector spaces with the same dimension $\nu(n)$. In this situation we ask whether r_n is bijective or not.

Example 1. Let E be a curve $y^2 + y = x^3 + x$ which is of conductor 91. Take $p = 3$. Then

$$\mathcal{P} = \{19, 37, 43, 61, 73, 103, 127, 163, 181, 229, 271, 337, 349, 367, 397, 409, 439, 499, ...\}.$$

For this curve we know that $E(\mathbb{Q})$ is free of rank 1 and is generated by the point $P = (0, 0)$.

Take several $\ell \in \mathcal{P}$. Since the order of $P = (0, 0)$ in $E(\mathbb{F}_\ell)$ can be easily computed, it is easy to check whether r_ℓ is bijective or zero by checking whether $r_\ell(P)$ generates $E(\mathbb{F}_\ell)/p$. Here is a table

ℓ	19	37	43	61	73	103	127	163	181	229	271	337
r_ℓ	bij	bij	bij	bij	bij	bij	bij	zero	bij	bij	bij	bij

ℓ	349	367	397	409	439	499
r_ℓ	bij	bij	zero	bij	zero	zero

Example 2. We consider $E : y^2 + xy + y = x^3 + x^2 - 15x + 16$. In this case the Mordell-Weil group $E(\mathbb{Q})$ is free of rank 2 and is generated by two

points $P = (2, -2)$ and $Q = (-4, 7)$. Take $p = 3$. Then $\mathcal{P}$ can be computed as

$$\mathcal{P} = \{13, 61, 103, 109, 127, 139, 163, 211, 229, 271, 283, 313, 349, 367, 433, ...\}.$$

We consider

$$r_n : E(\mathbb{Q})/p \longrightarrow E(\mathbb{F}_{\ell_1})/p \oplus E(\mathbb{F}_{\ell_2})/p$$

for $n = \ell_1 \cdot \ell_2 \in \mathcal{N}$.

ℓ	61	103	109	127	139	163	211	229	271	283	313	349
$r_{13\times\ell}$	bij	not bij	bij	bij	not bij	bij	bij	not bij	bij	bij	bij	not bij

ℓ	103	109	127	139	163	211	229	271	283	313	349	367
$r_{61\times\ell}$	bij	not bij	bij	bij	bij	bij	not bij	not bij	bij	not bij	bij	bij

We will see later that, surprisingly, just one analytic quantity δ_n which will be defined in the next subsection determines completely whether r_n is bijective or not.

1.2 Analytic quantities δ_n

Let $f_E(z)$ be the cusp form of weight 2 corresponding to the elliptic curve E. We consider the modular symbol

$$\left[\frac{a}{n}\right] = \mathrm{Re}\left(2\pi i \int_\infty^{a/n} f_E(z)dz\right)/\Omega_E^+ \in \mathbb{Q}$$

for $a, n \in \mathbb{Z}$ where $\Omega_E^+ = \int_{E(\mathbb{R})} \omega_E$ is the Néron period (if the Néron lattice is nonrectangular, it is the minimal positive real number in the Néron lattice, and if the lattice is rectangular, it is twice of the minimal positive real number in the Néron lattice, cf. [19] (1.1)). For $n \in \mathcal{N}$ and $a \in \mathbb{Z}$, since we assumed that the Galois representation $E[p]$ is irreducible, we have $[a/n] \in \mathbb{Z}_p$, namely its denominator is prime to p (see Stevens [30] §3). Therefore one can consider $[\frac{a}{n}] \bmod p \in \mathbb{F}_p$.

Let ℓ be a prime in $\mathcal{P}$. Fixing a generator g_ℓ of $\mathbb{F}_\ell^\times$, we define $\log_{\mathbb{F}_\ell}$ by

$$\log_{\mathbb{F}_\ell} : \mathbb{F}_\ell^\times \simeq \mathbb{Z}/(\ell - 1)\mathbb{Z} \longrightarrow \mathbb{F}_p \tag{2}$$

where the first map is defined by fixing the generator g_ℓ and the second map is the natural homomorphism $\mathbb{Z}/(\ell - 1)\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Writing $\overline{\left[\frac{a}{n}\right]}$ for $\left[\frac{a}{n}\right] \bmod p$, we define

$$\delta_n = \sum_{\substack{a=1 \\ (a,n)=1}}^{n} \overline{\left[\frac{a}{n}\right]} \left(\prod_{\ell \mid n} \log_{\mathbb{F}_\ell}(a) \right) \in \mathbb{F}_p \,. \tag{3}$$

This appears as a coefficient of the modular element $\theta_{\mathbb{Q}(\mu_n)^+} \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_n)^+ / \mathbb{Q})]$ of Mazur and Tate [19] (see §4.5). We stress here that δ_n can be easily computed *numerically* when E and n are given.

We give here a fundamental conjecture (cf. Conjecture 1 on page 320 in [15]). We denote the Tamagawa factor of E by $\mathrm{Tam}(E) = \Pi_{\ell:\mathrm{bad}}(E(\mathbb{Q}_\ell) : E^0(\mathbb{Q}_\ell))$.

Conjecture 1.1. *Assume that p is prime to $\mathrm{Tam}(E)$. Then there exists $n \in \mathcal{N}$ such that $\delta_n \neq 0$ in $\mathbb{F}_p$.*

As we mentioned, the numerical computation of δ_n is easy. For two examples in the previous subsection, the values of δ_n are as follows.

Example 1. For $y^2 + y = x^3 + x$, taking $p = 3$, we have

ℓ	19	37	43	61	73	103	127	163	181	229	271	337
δ_ℓ	2	1	1	2	1	1	2	0	2	2	1	1

ℓ	349	367	397	409	439	499
δ_ℓ	2	1	0	2	0	0

Example 2. For $y^2 + xy + y = x^3 + x^2 - 15x + 16$, taking $p = 3$, we have

ℓ	61	103	109	127	139	163	211	229	271	283	313	349
$\delta_{13\times\ell}$	1	0	1	1	0	2	1	0	2	2	2	0

ℓ	103	109	127	139	163	211	229	271	283	313	349	367
$\delta_{61\times\ell}$	1	0	1	1	2	1	0	0	2	0	1	1

1.3 Conjectures on r_n and δ_n

Comparing the tables in Subsections 1.1 and 1.2, we are led to the following conjecture.

Conjecture 1.2. *Suppose that p does not divide $\#Ш(E/\mathbb{Q})\,\mathrm{Tam}(E)$ where $Ш(E/\mathbb{Q})$ is the Tate-Shafarevich group. For any $n \in \mathcal{N}$ such that $\mathrm{rank}\, E(\mathbb{Q}) = \nu(n)$,*

$$r_n : E(\mathbb{Q})/p \longrightarrow \bigoplus_{\ell|n} E(\mathbb{F}_\ell) \otimes \mathbb{Z}/p\mathbb{Z} \text{ is bijective } \iff \delta_n \neq 0$$

holds.

Let $\mathrm{Sel}(\mathbb{Q}, E[p])$ be the Selmer group over $\mathbb{Q}$ with respect to $E[p]$. So we have an exact sequence

$$0 \longrightarrow E(\mathbb{Q})/pE(\mathbb{Q}) \longrightarrow \mathrm{Sel}(\mathbb{Q}, E[p]) \longrightarrow Ш(E/\mathbb{Q})[p] \longrightarrow 0$$

where $Ш(E/\mathbb{Q})[p]$ is the subgroup of $Ш(E/\mathbb{Q})$ consisting of elements that are annihilated by p. For a prime $\ell \in \mathcal{P}$ and $x \in \mathrm{Sel}(\mathbb{Q}, E[p])$, the image of x in $H^1(\mathbb{Q}_\ell, E[p])$ is by definition in $E(\mathbb{Q}_\ell)/pE(\mathbb{Q}_\ell)$ which is naturally isomorphic to $E(\mathbb{F}_\ell)/pE(\mathbb{F}_\ell)$ since ℓ is a good reduction prime and is prime to p. Thus r_n can be naturally extended to

$$r_n^{\mathrm{Sel}} : \mathrm{Sel}(\mathbb{Q}, E[p]) \longrightarrow \bigoplus_{\ell|n} E(\mathbb{F}_\ell) \otimes \mathbb{Z}/p\mathbb{Z} \simeq (\mathbb{Z}/p\mathbb{Z})^{\nu(n)} \ . \tag{4}$$

for each $n \in \mathcal{N}$.

Conjecture 1.2 is a special case of the following conjecture.

Conjecture 1.3. *Suppose that p does not divide $\mathrm{Tam}(E)$. For any $n \in \mathcal{N}$ such that $\dim_{\mathbb{F}_p} \mathrm{Sel}(\mathbb{Q}, E[p]) = \nu(n)$,*

$$r_n^{\mathrm{Sel}} : \mathrm{Sel}(\mathbb{Q}, E[p]) \longrightarrow \bigoplus_{\ell|n} E(\mathbb{F}_\ell) \otimes \mathbb{Z}/p\mathbb{Z} \text{ is bijective } \iff \delta_n \neq 0$$

holds.

If p does not divide the order of $Ш(E/\mathbb{Q})$, the natural map $E(\mathbb{Q})/p \simeq \mathrm{Sel}(\mathbb{Q}, E[p])$ is bijective, so Conjecture 1.3 clearly implies Conjecture 1.2.

We will prove in Theorem 2.1 that the right hand side implies the left hand side in Conjecture 1.3 (under some mild assumptions in the beginning of §2.2).

Remark 1.4. We can make an analogous statement for ideal class groups. But this statement does not hold in general. We will see in §3 that the analogous claim (11) for class groups does not hold with numerical examples. This phenomenon will be explained in §3.

Remark 1.5. Here, we explain a little recent argument of Sakamoto on his Kolyvagin systems of rank 0. One can extend the homomorphism r_n^{Sel} to a certain subgroup $\mathrm{Sel}_{\mathcal{F}^n}(\mathbb{Q}, E[p])$ of $H^1(\mathbb{Q}, E[p])$.

We use the terminology of Mazur and Rubin in their theory of Kolyvagin systems [18]. For any prime ℓ, we regard $E(\mathbb{Q}_\ell)/p$ as a subgroup of $H^1(\mathbb{Q}_\ell, E[p])$ by the Kummer map. We define $H^1_{tr}(\mathbb{Q}_\ell, E[p])$ to be the kernel of the natural map $H^1(\mathbb{Q}_\ell, E[p]) \to H^1(\mathbb{Q}_\ell(\mu_\ell), E[p])$ where $\mathbb{Q}_\ell(\mu_\ell)$ is the cyclotomic field of ℓ-th roots of unity over $\mathbb{Q}_\ell$.

For any $n \in \mathcal{N}$, we define $\mathrm{Sel}_{\mathcal{F}^n}(\mathbb{Q}, E[p])$ to be the subgroup of $H^1(\mathbb{Q}, E[p])$ consisting of elements whose image in $H^1(\mathbb{Q}_\ell, E[p])$ is in $E(\mathbb{Q}_\ell)/p$ for any prime ℓ that does not divide n. We consider a natural map

$$r_n^{\mathcal{F}^n} : \mathrm{Sel}_{\mathcal{F}^n}(\mathbb{Q}, E[p]) \longrightarrow \bigoplus_{\ell|n} H^1(\mathbb{Q}_\ell, E[p])/H^1_{tr}(\mathbb{Q}_\ell, E[p]) \simeq \bigoplus_{\ell|n} E(\mathbb{F}_\ell)/p.$$

Since the diagram

$$\begin{array}{ccc} \mathrm{Sel}(\mathbb{Q}, E[p]) & \xrightarrow{r_n^{\mathrm{Sel}}} & \bigoplus_{\ell|n} E(\mathbb{F}_\ell)/p \\ \downarrow & & \downarrow \simeq \\ \mathrm{Sel}_{\mathcal{F}^n}(\mathbb{Q}, E[p]) & \xrightarrow{r_n^{\mathcal{F}^n}} & \bigoplus_{\ell|n} H^1(\mathbb{Q}_\ell, E[p^m])/H^1_{tr}(\mathbb{Q}_\ell, E[p]) \end{array}$$

is commutative, $r_n^{\mathcal{F}^n}$ is an extension of r_n^{Sel}. We denote the kernel of $r_n^{\mathcal{F}^n}$ by $\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, E[p^m])$, which is a finite dimensional $\mathbb{F}_p$-vector space.

Sakamoto constructed in [27] a theory of Kolyvagin systems of rank 0. The space of Kolyvagin systems of rank 0 has rank 1, and using a basis κ of the space one can define $\delta_n(\kappa)$ by the method in [27]. Sakamoto proved in [27] Theorem 5.8 that

$$\mathrm{Fitt}_{\mathbb{F}_p}(\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, E[p])) = (\delta_n(\kappa)).$$

We note that $\delta_n(\kappa)$ in [27] is defined algebraically and has no relation with elements with analytic origin. However, we can expect the equality $(\delta_n(\kappa)) = (\delta_n)$ of ideals (see Remark 1.8). Therefore we can conjecture that

$$\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, E[p]) = 0 \iff \delta_n \neq 0\ . \tag{5}$$

Then this conjecture (5) and the next proposition imply that the left hand side of Conjecture 1.3 implies the right hand side of Conjecture 1.3.

Proposition 1.6. *Suppose that* $r_n^{\mathrm{Sel}} : \mathrm{Sel}(\mathbb{Q}, E[p]) \longrightarrow \bigoplus_{\ell|n} E(\mathbb{F}_\ell) \otimes \mathbb{Z}/p\mathbb{Z}$ *is bijective. Then we have* $\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, E[p]) = 0$.

This proposition will be proved in §4.1.

1.4 Conjectures on the Selmer group $\mathrm{Sel}(\mathbb{Q}, E[p])$

In the previous subsection we proposed conjectures on the map r_n. In this subsection we propose a conjecture on the structure of the classical Selmer group $\mathrm{Sel}(\mathbb{Q}, E[p])$.

For general $n \in \mathcal{N}$ which may not satisfy $\dim_{\mathbb{F}_p} \mathrm{Sel}(\mathbb{Q}, E[p]) = \nu(n)$, we prove in Theorem 2.1 that if $\delta_n \neq 0$ in $\mathbb{F}_p$, then r_n is injective (under some mild assumptions in the beginning of §2.2). Therefore, if $\delta_n \neq 0$, we have

$$\dim_{\mathbb{F}_p} \mathrm{Sel}(\mathbb{Q}, E[p]) \leq \nu(n).$$

Suppose that $n \in \mathcal{N}$. As we mentioned in §0, we say that n is *δ-minimal* if $\delta_d = 0$ for all divisors d of n such that $1 \leq d < n$ and $\delta_n \neq 0$. We propose the following conjecture (see also Conjecture 2 on page 322 in [15]).

Conjecture 1.7. *Suppose that p does not divide* $\mathrm{Tam}(E)$. *If $n \in \mathcal{N}$ is δ-minimal, then r_n^{Sel} is bijective. In particular,*

$$\mathrm{Sel}(\mathbb{Q}, E[p]) \simeq (\mathbb{Z}/p\mathbb{Z})^{\nu(n)}.$$

Suppose that both n and n' are δ-minimal. Then Conjecture 1.7 also asserts that $\nu(n) = \nu(n')$. This conjecture asserts that a *single* n which is δ-minimal determines the Selmer rank.

One can always find δ-minimal n conjecturally. In fact, suppose that there is $m \in \mathcal{N}$ such that $\delta_m \neq 0$ (the existence of such m is conjectured in Conjecture 1.1). Then, r_m^{Sel} is injective by Theorem 2.1. Therefore, there exists a divisor n of m such that r_n^{Sel} is bijective. Then for any proper divisor d of n, r_d^{Sel} is not injective since $\nu(d) < \dim_{\mathbb{F}_p} \mathrm{Sel}(\mathbb{Q}, E[p])$. This implies that $\mathrm{Sel}_{\mathcal{F}(d)}(\mathbb{Q}, E[p]) \neq 0$. By conjecture (5) in the previous subsection, we must have $\delta_d = 0$. This shows that n is δ-minimal. In this way, one can expect to find δ-minimal $n \in \mathcal{N}$ among divisors of m.

Remark 1.8. After the first version of this paper was written, so much progress on these conjectures was made. First of all, when p is a good ordinary prime, Sakamoto in [28] proved Conjecture 1.7. He also showed in the ordinary case that the conjecture (5) in the previous section is equivalent to the Iwasawa main conjecture for the cyclotomic $\mathbb{Z}_p$-extension. More general theory which can be applied to any non-ordinary p is developed in [17]. Chan-Ho Kim also has obtained a general theory on the structure of Selmer groups in his recent new work [8]. Especially he has also proved Conjecture 1.7 in it.

2 Main theorem

2.1 Setting and notation for $\mathbb{Z}/p^m\mathbb{Z}$-modules

In the previous section we considered only $\mathbb{F}_p$-vector spaces. In this section we study more general theory for $\mathbb{Z}/p^m$-modules with $m \in \mathbb{Z}_{>0}$.

We assume that the action $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\, E[p^\infty] \simeq GL_2(\mathbb{Z}_p)$ on p-power torsion points $E[p^\infty]$ is surjective. We fix a positive integer $m > 0$. We define

$$\mathcal{P}^{(m)} = \{\ell \mid \ell \equiv 1 \pmod{p^m},\ \ell \nmid N,\ \text{and } E(\mathbb{F}_\ell) \otimes \mathbb{Z}/p^m\mathbb{Z} \simeq \mathbb{Z}/p^m\mathbb{Z}\}.$$

Thus $\mathcal{P}^{(1)}$ coincides with $\mathcal{P}$ in the previous section, and

$$\mathcal{P} = \mathcal{P}^{(1)} \supset \mathcal{P}^{(2)} \supset \mathcal{P}^{(3)} \supset \dots .$$

The set $\mathcal{P}^{(m)}$ is an infinite set, which can be checked by using Chebotarev density theorem (see [14] §5.8).

We define $\mathcal{N}^{(m)}$ to be the set of squarefree products of primes in $\mathcal{P}^{(m)}$. Again, we suppose $1 \in \mathcal{N}^{(m)}$.

Next we define several subgroups of $H^1(F, E[p^m])$ for a number field F. For a positive integer n, we define

$$\mathrm{Sel}_{\mathcal{F}^n}(F, E[p^m]) = \mathrm{Ker}(H^1(F, E[p^m]) \longrightarrow \bigoplus_{v \nmid n} H^1(F_v, E[p^m])/(E(F_v) \otimes \mathbb{Z}/p^m))$$

where we regard $E(F_v) \otimes \mathbb{Z}/p^m$ as a subgroup of $H^1(F_v, E[p^m])$ by the Kummer map as usual. If $n = 1$, we just write $\mathrm{Sel}(F, E[p^m])$ for $\mathrm{Sel}_{\mathcal{F}^1}(F, E[p^m])$, which is the classical Selmer group. *If p divides n*, we also use the notation $H^1_{\mathcal{F}^n}(F, E[p^m])$ for $\mathrm{Sel}_{\mathcal{F}^n}(F, E[p^m])$. We note that $H^1_{\mathcal{F}^{npN}}(F, E[p^m])$ coincides with the étale cohomology group $H^1_{et}(\mathrm{Spec}\ \mathcal{O}_F[1/npN], E[p^m])$ where N is the conductor of E.

We define $\mathrm{Sel}_{\mathcal{F}^n}(F, E[p^\infty])$, $\mathrm{Sel}_{\mathcal{F}^n}(F, T_p(E))$ similarly, using the local conditions $E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ and $E(F_v) \otimes \mathbb{Z}_p$, respectively. For $n = 1$, we also write $\mathrm{Sel}(F, E[p^\infty])$ for $\mathrm{Sel}_{\mathcal{F}^1}(F, E[p^\infty])$, and sometimes denote it by $\mathrm{Sel}(E/F)$. If p divides n, $H^1_{\mathcal{F}^n}(F, T_p(E))$ means $\mathrm{Sel}_{\mathcal{F}^n}(F, T_p(E))$.

For $F = \mathbb{Q}$, as in the case $m = 1$, following Mazur and Rubin [18], we define $H^1_{tr}(\mathbb{Q}_\ell, E[p^m])$ to be the kernel of the natural map $H^1(\mathbb{Q}_\ell, E[p^m]) \to H^1(\mathbb{Q}_\ell(\mu_\ell), E[p^m])$ where $\mathbb{Q}_\ell(\mu_\ell)$ is the cyclotomic field of ℓ-th roots of unity over $\mathbb{Q}_\ell$. For positive integers n, k such that n is prime to p and k is prime to np, we define $\mathrm{Sel}_{\mathcal{F}(n)^k}(\mathbb{Q}, E[p^m])$ by

$$\mathrm{Sel}_{\mathcal{F}(n)^k}(\mathbb{Q}, E[p^m]) = \mathrm{Ker}(\mathrm{Sel}_{\mathcal{F}^{nk}}(\mathbb{Q}, E[p^m]) \longrightarrow \bigoplus_{\ell \mid n} H^1(\mathbb{Q}_\ell, E[p^m])/H^1_{tr}(\mathbb{Q}_\ell, E[p^m])).$$

If $k = 1$, we just write $\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, E[p^m])$ for $\mathrm{Sel}_{\mathcal{F}(n)^1}(F, E[p^m])$.

For any prime $\ell \in \mathcal{P}^{(m)}$, we have $E(\mathbb{Q}_\ell)/p^m \simeq E(\mathbb{F}_\ell)/p^m \simeq \mathbb{Z}/p^m$. The local cohomology group $H^1(\mathbb{Q}_\ell, E[p^m])$ is free of rank 2 and decomposes into

$$H^1(\mathbb{Q}_\ell, E[p^m]) = E(\mathbb{F}_\ell)/p^m \oplus H^1_{tr}(\mathbb{Q}_\ell, E[p^m]),$$

so we have

$$H^1(\mathbb{Q}_\ell, E[p^m])/H^1_{tr}(\mathbb{Q}_\ell, E[p^m]) \simeq E(\mathbb{F}_\ell)/p^m.$$

For $n \in \mathcal{N}^{(m)}$, as in the previous section, we have a natural homomorphism

$$r_n^{\mathrm{Sel}} : \mathrm{Sel}(\mathbb{Q}, E[p^m]) \longrightarrow \bigoplus_{\ell|n} E(\mathbb{F}_\ell) \otimes \mathbb{Z}/p^m\mathbb{Z} \simeq (\mathbb{Z}/p^m\mathbb{Z})^{\nu(n)},$$

which can be extended to

$$r_n^{\mathcal{F}^n} : \mathrm{Sel}_{\mathcal{F}^n}(\mathbb{Q}, E[p^m]) \longrightarrow \bigoplus_{\ell|n} H^1(\mathbb{Q}_\ell, E[p^m])/H^1_{tr}(\mathbb{Q}_\ell, E[p^m]) \simeq \bigoplus_{\ell|n} E(\mathbb{F}_\ell)/p^m. \tag{6}$$

2.2 Injectivity theorems

Put $a_p = p + 1 - \#E(\mathbb{F}_p)$ as usual. From this subsection throughout this paper, we assume that if E has good ordinary reduction at p, then $a_p \not\equiv 1 \pmod{p}$ (not anomalous), and that if E has supersingular reduction at p, then $a_p = 0$. The latter is always satisfied if $p \geq 5$. Also, we assume that the μ-invariant for the cyclotomic $\mathbb{Z}_p$-extension vanishes if p is ordinary, and that $\mu^+ = 0$, or $\mu^- = 0$ if p is supersingular (for the precise definition of the latter, see the definition just before Lemma 4.1 below). The conditions on the μ-invariants are conjectured by Greenberg to hold true always. We assume the conditions on the μ-invariants though there is a possibility to remove them by using a recent result of Kataoka [5].

For $n \in \mathcal{N}^{(m)}$, we can define $\delta_n \in \mathbb{F}_p$ since n is in $\mathcal{N}$.

Theorem 2.1. *Suppose that m is a positive integer, and $n \in \mathcal{N}^{(m)}$ satisfies $\delta_n \neq 0$ in $\mathbb{F}_p$. Then the natural map*

$$r_n^{\mathrm{Sel}} : \mathrm{Sel}(\mathbb{Q}, E[p^m]) \longrightarrow \bigoplus_{\ell|n} E(\mathbb{F}_\ell)/p^m \simeq (\mathbb{Z}/p^m\mathbb{Z})^{\nu(n)}$$

is injective. In particular, we have

$$\mathrm{rank}\, E(\mathbb{Q}) + \dim_{\mathbb{F}_p} Ш(E/\mathbb{Q})[p] \leq \nu(n)$$

where $Ш(E/\mathbb{Q})[p]$ *is the subgroup of* $Ш(E/\mathbb{Q})$ *consisting of elements that are annihilated by* p*.*

Remark 2.2. This theorem was proved in our previous paper (see §4.1 in [15]) in the ordinary case, so in this paper we prove this theorem in the supersingular case.

2.3 Structure of Tate-Shafarevich groups and some numerical examples

Theorem 2.1 is useful to determine the structure of the Tate-Shafarevich group of E. We denote by $Ш(E/\mathbb{Q})[p^\infty]$ the p-primary component of the Tate-Shafarevich group $Ш(E/\mathbb{Q})$.

Example 3. We take E to be

$$y^2 + xy = x^3 - x^2 - 22959594440x - 1339036978455744$$

with conductor $N = 152330$ (Cremona label $152330l1$). We know $E(\mathbb{Q}) = 0$ and $\mathrm{Tam}(E/\mathbb{Q}) = 2$. Take $p = 3$. Then $a_3 = 0$ (so 3 is a supersingular prime), the Galois action on $E[3^\infty]$ is surjective and both the cyclotomic $\mu^{\pm}$-invariants vanish. Therefore, all the conditions in the beginning of §2.2 are satisfied and we can apply Theorem 2.1.

In this case since N is squarefree, we know by the main theorem of X. Wan in [31] that the Iwasawa main conjecture for $p = 3$ holds true for E. Therefore, it follows from $L(E,1)/\Omega_E = 162$ that the 3-component $Ш(E/\mathbb{Q})[3^\infty]$ of the Tate-Shafarevich group has order 81 (while the Birch and Swinnerton-Dyer conjecture asserts that the whole $Ш(E/\mathbb{Q})$ has order 81). Thus there are two possibilities for the structure of $Ш(E/\mathbb{Q})[3^\infty]$ as an abelian group, namely $(\mathbb{Z}/3\mathbb{Z})^{\oplus 4}$ and $(\mathbb{Z}/9\mathbb{Z})^{\oplus 2}$.

Taking $p = 3$ and computing $\mathcal{P}$, we have

$$\mathcal{P} = \{13, 31, 61, 127, ...\}.$$

We can easily compute $\delta_{13\times\ell}$ and $\delta_{31\times\ell}$ to get the following table.

ℓ	31	61	127
$\delta_{13\times\ell}$	1	0	2

ℓ	61	127
$\delta_{31\times\ell}$	1	0

Applying $n = 13 \times 31$ for example, we get from $\delta_{13\times 31} \neq 0$ and Theorem 2.1 that

$$\dim_{\mathbb{F}_3} Ш(E/\mathbb{Q})[3] \leq \nu(13 \times 31) = 2,$$

which implies that $\dim_{\mathbb{F}_3} Ш(E/\mathbb{Q})[3] = 2$ and

$$Ш(E/\mathbb{Q})[3^\infty] \simeq \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}.$$

Thus we also have $Ш(E/\mathbb{Q}) \simeq \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$ if we admit the Birch and Swinnerton-Dyer conjecture.

Example 4. We take E to be

$$E : y^2 + y = x^3 - 17034726259173x - 27061436852750306309.$$

This is the curve studied by Prasad and Shekhar in [23] Example 2. The conductor is $N = 423801$ (Cremona label $423801ci1$). Take $p = 5$. Then the action on $E[5^\infty]$ is surjective, 5 is good ordinary with $a_5 = 4$, and the cyclotomic μ-invariant is 0, so all the conditions in the beginning of §2.2 are satisfied and one can apply Theorem 2.1. For this curve, we know $E(\mathbb{Q}) = 0$ and $\mathrm{Tam}(E/\mathbb{Q}) = 16$.

We know $a_{11} = a_{41} = 2$ and $a_{191} = -18$ for this curve (a_ℓ is the coefficient of the modular form corresponding to E), and

$$\mathcal{P} = \{11, 41, 191, ...\}.$$

We compute $\delta_{11\times 41}$ to get $\delta_{11\times 41} = -1628692 = 3 \neq 0$ in $\mathbb{F}_p$.

In order to see that the main conjecture for (E, p) holds, we cannot apply the main theorem by Skinner and Urban in [29] because $N = 423801 = 3^2 \cdot 7^2 \cdot 31^2$ is a perfect square. Instead, we can use the main theorem in C.-H. Kim, M. Kim and H.-S. Sun in [7]. In fact, using Corollary 1.2 in [7] and $\delta_{11\times 41} \neq 0$, we know that the main conjecture for (E, p) holds true.

Since $L(E, 1)/\Omega_E = 10000$, the main conjecture implies that the 5-component of $Ш(E/\mathbb{Q})$ has order $625 = 5^4$.

It follows from Theorem 2.1 and $\delta_{11\times 41} \neq 0$ that $\dim_{\mathbb{F}_5} Ш(E/\mathbb{Q})[5] \leq 2$. This implies that

$$Ш(E/\mathbb{Q})[5^\infty] \simeq \mathbb{Z}/25\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}.$$

If we admit the Birch and Swinnerton-Dyer conjecture, $Ш(E/\mathbb{Q})$ has only 5-components and we have $Ш(E/\mathbb{Q}) \simeq \mathbb{Z}/25\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}$.

For general E over $\mathbb{Q}$, concerning the structure of the Tate-Shafarevich group $Ш(E/\mathbb{Q})$, we have the following conjecture (see Theorem B in [14]). To state the conjecture, we have to define $\delta_n^{(m)}$ that is δ_n mod p^m for any

$n \in \mathcal{N}^{(m)}$. For any $\ell \in \mathcal{P}^{(m)}$, $\log_{\mathbb{F}_\ell}^{(m)} : \mathbb{F}_\ell^\times \simeq \mathbb{Z}/(\ell-1)\mathbb{Z} \to \mathbb{Z}/p^m$ is naturally defined by using the fixed generator g_ℓ of $\mathbb{F}_\ell^\times$, and $[a/n]^{(m)}$ is defined as $[a/n]$ mod p^m. Then as in (3) we define $\delta_n^{(m)}$ by

$$\delta_n^{(m)} = \sum_{\substack{a=1 \\ (a,n)=1}}^{n} \left[\frac{a}{n}\right]^{(m)} \left(\prod_{\ell|n} \log_{\mathbb{F}_\ell}^{(m)}(a)\right) \in \mathbb{Z}/p^m\mathbb{Z}. \tag{7}$$

Let $Ш(E/\mathbb{Q})[p^m]$ be the kernel of the multiplication by p^m on $Ш(E/\mathbb{Q})$.

Conjecture 2.3. *Suppose that p does not divide* $\mathrm{Tam}(E/\mathbb{Q})$, *and* $\mathrm{rank}\, E(\mathbb{Q}) = r$. *For any integers $m > 0$ and $i \geq 0$, we define $I_{m,i}$ to be the ideal of $\mathbb{Z}/p^m\mathbb{Z}$ generated by all $\delta_n^{(m)}$ with $n \in \mathcal{N}^{(m)}$ such that $\nu(n) = r + i$. Then for any even $i \geq 0$ we have*

$$\mathrm{Fitt}_{i,\mathbb{Z}/p^m} Ш(E/\mathbb{Q})[p^m] = I_{m,i}$$

where $\mathrm{Fitt}_{i,\mathbb{Z}/p^m} Ш(E/\mathbb{Q})[p^m]$ *is the i-th higher Fitting ideal of* $Ш(E/\mathbb{Q})[p^m]$.

We have to restrict i to even numbers ≥ 0 in Conjecture 2.3. In fact, for odd i the above equality in Conjecture 2.3 does not hold. But Conjecture 2.3 is enough to determine the structure of $Ш(E/\mathbb{Q})[p^m]$. Assume that $Ш(E/\mathbb{Q})[p^\infty]$ is finite. Then, by the existence of the Cassels-Tate pairing, $Ш(E/\mathbb{Q})[p^\infty]$ is isomorphic to $A \oplus A$ for some finite abelian group A, and $Ш(E/\mathbb{Q})[p^m]$ is isomorphic to $(\mathbb{Z}/p^{k_1}\mathbb{Z})^{\oplus 2} \oplus ... \oplus (\mathbb{Z}/p^{k_s}\mathbb{Z})^{\oplus 2}$ with some k_1,...,k_s such that $m \geq k_1 \geq ... \geq k_s$. Then by the definition of the higher Fitting ideal, $\mathrm{Fitt}_{0,\mathbb{Z}/p^m} Ш(E/\mathbb{Q})[p^m]$ is generated by $p^{2(k_1+...+k_s)}$, $\mathrm{Fitt}_{2,\mathbb{Z}/p^m} Ш(E/\mathbb{Q})[p^m]$ is generated by $p^{2(k_2+...+k_s)}$, $\mathrm{Fitt}_{4,\mathbb{Z}/p^m} Ш(E/\mathbb{Q})[p^m]$ is generated by $p^{2(k_3+...+k_s)}$, etc. So taking m sufficiently large such that $Ш(E/\mathbb{Q})[p^\infty] = Ш(E/\mathbb{Q})[p^m]$ and $\mathrm{Fitt}_{i,\mathbb{Z}/p^m} Ш(E/\mathbb{Q})[p^m] \neq 0$, we can determine the structure of the Tate-Shafarevich group $Ш(E/\mathbb{Q})[p^\infty]$ from Conjecture 2.3.

We proved Conjecture 2.3 in Theorem B in [14] under several (strong) conditions including the finiteness of $Ш(E/\mathbb{Q})[p^\infty]$ and the ordinary condition on p.

3 Analogous results for ideal class groups

Concerning Conjectures 1.2, 1.3 in §1.3, "the left hand side $\Longleftarrow$ the right hand side" can be proved under some mild assumptions, as we explained in §2. So the problem is to show the converse.

In this section we first state Theorem 3.1 for ideal class groups, which corresponds to Theorem 2.1 for the Selmer group. For ideal class groups, we will show in this section that "the converse" of the analogy of the above conjectures *does not* hold.

Since the unramified cohomology $H^1_f(\mathbb{Q}_\ell, E[p])$ is $E(\mathbb{Q}_\ell)/p$ and the map r_n^{Sel} can be regarded as $r_n^{\mathrm{Sel}} : \mathrm{Sel}(\mathbb{Q}, E[p]) \to \bigoplus_{\ell|n} H^1_f(\mathbb{Q}_\ell, E[p])$, its dual is

$$\bigoplus_{\ell|n} H^1(\mathbb{Q}_\ell, E[p])/H^1_f(\mathbb{Q}_\ell, E[p]) \longrightarrow \mathrm{Hom}(\mathrm{Sel}(\mathbb{Q}, E[p]), \mathbb{Z}/p\mathbb{Z}). \tag{8}$$

Conjecture 1.3 studies the bijectivity of this map.

For a number field K and the Galois module μ_p consisting of p-th roots of unity, $H^1(K_v, \mu_p) = K_v^\times \otimes \mathbb{Z}/p\mathbb{Z}$ and $H^1_f(K_v, \mu_p) = E_{K_v} \otimes \mathbb{Z}/p\mathbb{Z}$ for a finite prime v of K where E_{K_v} is the unit group of K_v. Therefore, $H^1(K_v, \mu_p)/H^1_f(K_v, \mu_p) \simeq \mathbb{Z}/p\mathbb{Z}$ where the isomorphism is defined by the normalized additive valuation of K_v.

Let C_K be the ideal class group of K. For a squarefree product n of finite primes of K, the analogous map of (8) is

$$\bigoplus_{\mathcal{L}|n} \mathbb{Z}/p\mathbb{Z} \longrightarrow C_K/pC_K \tag{9}$$

where $\mathcal{L}$ runs over all primes of K dividing n, and $e_\mathcal{L} = (0, ..., 1, ...0)$ (the element whose $\mathcal{L}$-component is 1 and other components are zero) goes to the class of $\mathcal{L}$ in C_K/pC_K.

Let k be a totally real field and K be a CM-field such that $[K : k] = 2$. Theorem 3.1 we will prove below can be generalized to more general abelian extension K/k, but here we restrict ourselves to this simple setting $[K : k] = 2$.

We assume that p is an odd prime and that K does not contain a primitive p-th root of unity. For a finite prime ℓ of k such that $N(\ell) \equiv 1 \pmod{p}$, we define $n_\ell \in \mathbb{Z}_{>0}$ by $p^{n_\ell} \| N(\ell) - 1$. We say ℓ is *suitable* if k has a cyclic extension $k(\ell)/k$ of degree p^{n_ℓ} such that $k(\ell)/k$ is unramified outside ℓ and totally ramified at ℓ. If $k = \mathbb{Q}$, all prime numbers are suitable. We define a set $\mathcal{P}^{cl}$ of finite primes of k by

$$\mathcal{P}^{cl} = \{\ell \mid N(\ell) \equiv 1 \pmod{p},\ \ell \text{ splits in } K \text{ and } \ell \text{ is suitable}\}.$$

By Chebotarev density theorem one knows that $\mathcal{P}^{cl}$ is infinite (see §3 in [13]). We define $\mathcal{N}^{cl}$ the set of squarefree products of primes in $\mathcal{P}^{cl}$. For each ℓ we take a cyclic extension $k(\ell)/k$ of degree p^{n_ℓ} such that $k(\ell)/k$ is

unramified outside ℓ and totally ramified at ℓ, and define $k(n)$ to be the composite field of all $k(\ell)$ for ℓ dividing n.

Suppose that $n \in \mathcal{N}^{cl}$. We consider the composite field $Kk(n)$ of K and $k(n)$. For $\sigma \in \mathrm{Gal}(Kk(n)/k)$, we consider the partial zeta function

$$\zeta_k(s,\sigma) = \sum_{(\frac{Kk(n)/k}{\mathfrak{a}})=\sigma} N(\mathfrak{a})^{-s}$$

where $\mathfrak{a}$ runs over all integral ideals of k whose Artin symbol is σ. This function has a meromorphic continuation to the whole complex plane. Since μ_p is not in $Kk(n)$ by our assumption, we know that $\zeta(0,\sigma) \in \mathbb{Z}_p$ by Deligne and Ribet [2], and Pierrette Cassou-Noguès [1].

For $\ell \in \mathcal{P}^{cl}$ we define $\log_{\mathbb{F}_\ell}^{cl}$ by

$$\begin{aligned} \log_{\mathbb{F}_\ell}^{cl} : \mathrm{Gal}(Kk(n)/k) &\longrightarrow \mathrm{Gal}(k(\ell)/k) \simeq \mathbb{F}_{N(\ell)}^{\times} \otimes \mathbb{Z}_p \simeq \mathbb{Z}/p^{n_\ell}\mathbb{Z} \\ &\longrightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p, \end{aligned}$$

fixing a generator of $\mathbb{F}_{N(\ell)}^{\times}$. We denote by χ the quadratic character of $\mathrm{Gal}(Kk(n)/k)$ defined by

$$\chi : \mathrm{Gal}(Kk(n)/k) \longrightarrow \mathrm{Gal}(K/k) = \{\pm 1\}.$$

We define δ_n^{cl} for $n \in \mathcal{N}^{cl}$ by

$$\delta_n^{cl} = \sum_{\sigma \in \mathrm{Gal}(Kk(n)/k)} \chi(\sigma)\zeta_k(0,\sigma) \left(\prod_{\ell | n} \log_{\mathbb{F}_\ell}^{cl}(\sigma) \right) \in \mathbb{F}_p\,.$$

We denote by $(C_K \otimes \mathbb{Z}_p)^-$ the subgroup of $C_K \otimes \mathbb{Z}_p$ consisting of elements on which the complex conjugation acts as -1.

The following theorem is the analogous result corresponding to the injectivity theorem for the Selmer group (Theorem 2.1 in §2). We can prove this theorem using Euler systems of Gauss sum type in our paper [13] (see also [25] when $k = \mathbb{Q}$) by the same method as the proof of Theorem 2.1 in §4.6.

Theorem 3.1. *Suppose that $\delta_n^{cl} \neq 0$ for some $n \in \mathcal{N}^{cl}$. Then $(C_K \otimes \mathbb{Z}_p)^-$ is generated by the classes of primes of K dividing n. In other words, the minus component of the homomorphism (9)*

$$(\bigoplus_{\mathcal{L}|n} \mathbb{Z}/p\mathbb{Z})^- \longrightarrow (C_K/pC_K)^-$$

is surjective.

We think that this theorem is interesting in the sense that we know generators of the class group explicitly from the information on zeta values which are computable.

We consider the simplest example. Suppose that $k = \mathbb{Q}$ and K is an imaginary quadratic field. Let $\chi_K : (\mathbb{Z}/d\mathbb{Z})^\times \to \{\pm 1\}$ be the Dirichlet character corresponding to K. For a cyclotomic field $\mathbb{Q}(\mu_m)/\mathbb{Q}$ and $a \in \mathbb{Z}$ with $0 < a < m$ and $(a, m) = 1$, it is well-known that $\zeta(0, \sigma_a) = \frac{1}{2} - \frac{a}{m}$ where $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ corresonds to a mod m. Therefore, δ_n^{cl} has a simple form which is similar to and simpler than (3) in §1.2;

$$\delta_n^{cl} = -\sum_{\substack{a=1 \\ (a,dn)=1}}^{dn} \chi_K(a)\frac{a}{n}\left(\prod_{\ell|n} \log_{\mathbb{F}_\ell}(a)\right) \in \mathbb{F}_p \tag{10}$$

where $\log_{\mathbb{F}_\ell}$ is as in §1.2. So the numerical computation of δ_n^{cl} is very easy in this case.

Example 5. Take $K = \mathbb{Q}(\sqrt{-23})$ over $k = \mathbb{Q}$ and $p = 3$. We know $C_K \simeq \mathbb{Z}/3\mathbb{Z}$, so $(C_K \otimes \mathbb{Z}/3\mathbb{Z})^- = C_K \otimes \mathbb{Z}/3\mathbb{Z} = C_K$. By definition,

$$\begin{aligned} \mathcal{P}^{cl} &= \{\ell \mid \ell \equiv 1 \pmod 3,\ (\frac{-23}{\ell}) = 1\} \\ &= \{13, 31, 73, 127, 139, 151, 163, 193, 211, 223, ...\}. \end{aligned}$$

For $\ell = 13$, 31, 73, 127, 139, 193, by computations using (10) we have $\delta_\ell^{cl} \neq 0$. Also for $\ell = 151$, 163, 211, 223, we have $\delta_\ell = 0$. For ℓ such that $\delta_\ell \neq 0$, we know by Theorem 3.1 that a prime above ℓ generates C_K. In the terminology of quadratic forms, this means that

$$2x^2 + xy + 3y^2 = \ell$$

has an integer solution. This can be also checked easily for the above ℓ's.

The analogy of Conjecture 1.3 for class groups can be formulated as follows. Suppose that $(C_K \otimes \mathbb{Z}_p)^-$ is generated by exactly m elements. Then for $n \in \mathcal{N}^{cl}$ such that $\nu(n) = m$, the analogous claim for class groups is

$$(C_K \otimes \mathbb{Z}_p)^- \text{ is generated by primes of } K \text{ above } n \Longleftrightarrow \delta_n^{cl} \neq 0. \tag{11}$$

We showed that "$\Longleftarrow$" holds true by Theorem 3.1. However, the above equivalence does not hold. In fact, consider Example 5, namely $K = \mathbb{Q}(\sqrt{-23})$. Then the above equivalence claims that

$$2x^2 + xy + 3y^2 = \ell \text{ has an integer soultion} \Longleftrightarrow \delta_\ell^{cl} \neq 0$$

for any $\ell \in \mathcal{P}^{cl}$ with $p = 3$. But the left hand side does not imply the right hand side, in general. For example, for $\ell = 151$, 163, we have $\delta_\ell^{cl} = 0$ but a prime above ℓ generates C_K because $2x^2 + xy + 3y^2 = \ell$ has an integer solution. (In fact, for $\ell = 151$, $(x, y) = (4, -7)$ is a solution, and for $\ell = 163$, $(x, y) = (8, -5)$ is a solution.) Thus the analogy (11) for class groups corresponding to Conjecture 1.3 does not hold.

For $\ell = 211$, 223, we have $\delta_\ell^{cl} = 0$ and primes above ℓ are principal since $211 = 2^2 + 23 \cdot 3^2$ and $223 = 4^2 + 23 \cdot 3^2$.

Next we consider the analogy of Conjecture 1.7, which claims that

$$\dim_{\mathbb{F}_p} C_K/pC_K = \nu(n)$$

if n is "δ^{cl}-minimal". We consider again Example 5, namely $K = \mathbb{Q}(\sqrt{-23})$, and will give a counterexample of the above equality. By computation we know $\delta_{151\times 211}^{cl} \neq 0$. Since $\delta_{151}^{cl} = \delta_{211}^{cl} = 0$, we know that 151×211 is "δ^{cl}-minimal". But, of course, we know $\dim_{\mathbb{F}_3} C_K = 1 \neq 2 = \nu(151 \times 211)$. This shows that the analogy for class groups corresponding to Conjecture 1.7 *does not* hold. This single n which is δ^{cl}-minimal *does not* determine the p-rank of the class group.

An essential difference between the Galois representations $T_p(E)$ and $\mathbb{Z}_p(1)$ is that the former is self-dual.

4 Proofs of statements

4.1 Proof of Proposition 1.6

We first prove Proposition 1.6. We use the notation $\mathrm{Sel}_{\mathcal{F}^n}(\mathbb{Q}, E[p])$ in Remark 1.5. We define $\mathrm{Sel}_{\mathcal{F}_n}(\mathbb{Q}, E[p])$ to be the kernel of

$$r_n^{\mathrm{Sel}} : \mathrm{Sel}(\mathbb{Q}, E[p]) \longrightarrow \bigoplus_{\ell|n} E(\mathbb{F}_\ell)/p.$$

Then by the global duality theorem, the sequence

$$\begin{aligned} 0 \longrightarrow\ & \mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, E[p]) \longrightarrow \mathrm{Sel}_{\mathcal{F}^n}(\mathbb{Q}, E[p]) \xrightarrow{\alpha} \bigoplus_{\ell|n} H^1(\mathbb{Q}_\ell, E[p])/H^1_{tr}(\mathbb{Q}_\ell, E[p]) \\ \longrightarrow\ & \mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, E[p])^\vee \longrightarrow \mathrm{Sel}_{\mathcal{F}_n}(\mathbb{Q}, E[p])^\vee \longrightarrow 0 \end{aligned}$$

is exact where $M^\vee$ means $\mathrm{Hom}(M, \mathbb{F}_p)$ for an $\mathbb{F}_p$-vector space M.

Suppose that r_n^{Sel} is bijective. Then the surjectivity of r_n^{Sel} implies the surjectivity of α in the above exact sequence. Therefore, we have $\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, E[p]) = \mathrm{Sel}_{\mathcal{F}_n}(\mathbb{Q}, E[p])$ by the above exact sequence. The injectivity of r_n^{Sel} means $\mathrm{Sel}_{\mathcal{F}_n}(\mathbb{Q}, E[p]) = 0$, so we have $\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, E[p]) = 0$.

4.2 Construction of equivariant p-adic L-functions in the supersingular case

The rest of this paper is devoted to the proof of Theorem 2.1 in the supersingular setting. We assume $a_p = 0$, so E has supersingular reduction at p. In this subsection, we construct a certain equivariant p-adic L-function explicitly from modular symbols, following the argument in our previous work [15] §2.1 where the ordinary case is treated.

For any $m \in \mathbb{Z}_{>0}$ we denote by μ_m the group of m-th roots of unity, and put $G_m = \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$. We consider a modular element

$$\theta_{\mathbb{Q}(\mu_m)} = \sum_{\substack{a=1 \\ (a,m)=1}}^{m} [\frac{a}{m}]\sigma_a \in \mathbb{Q}[G_m] \tag{12}$$

where $[a/m]$ is the modular symbol defined in §1.2 and σ_a is the automorphism in $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ characterized by $\sigma_a(\zeta) = \zeta^m$ for $\zeta \in \mu_m$ (cf. [19]).

We first construct signed p-adic L-functions $\theta_{K_\infty}^{\pm}$ by the method in §1 in [16]. Suppose that n is a squarefree positive integer which is prime to pN where N is the conductor of E. From our assumption that the action on $E[p]$ is surjective, we know $\theta_{\mathbb{Q}(\mu_{np^i})}$ is in $\mathbb{Z}_p[G_{np^i}]$ for any $i \in \mathbb{Z}_{\geq 0}$ (see [30]). We decompose $G_{p^{i+1}} = \Delta \times \Gamma_i$ where Δ is cyclic of order $p-1$ and Γ_i is cyclic of order p^i. We take a generator γ of $\mathrm{Gal}(\mathbb{Q}(\mu_{np^\infty})/\mathbb{Q}(\mu_{np}))$ and write

$$\mathbb{Z}_p[G_{np^{i+1}}] = \mathbb{Z}_p[G_{np}][\Gamma_i] \simeq \mathbb{Z}_p[G_{np}][[T]]/\omega_i$$

where $1+T$ corresponds to the image of γ in Γ_i and $\omega_i = (1+T)^{p^i} - 1$. Define Φ_i by $\Phi_i = \omega_i/\omega_{i-1}$ which is a cyclotomic polynomial. So $\omega_i = \Phi_i\omega_{i-1}$. Suppose that $i \geq 2$, and denote by

$$\pi : \mathbb{Z}_p[G_{np^{i+1}}] \longrightarrow \mathbb{Z}_p[G_{np^i}]$$

the natural projection. We also write

$$\nu : \mathbb{Z}_p[G_{np^{i-1}}] \longrightarrow \mathbb{Z}_p[G_{np^i}]$$

for the norm homomorphism which is defined by $\sigma \mapsto \sum \tau$ where for $\sigma \in G_{np^{i-1}}$, τ runs over elements in G_{np^i} which projects to σ. Then using the formula in (1.3) (4) in [19] we have

$$\pi(\theta_{\mathbb{Q}(\mu_{np^{i+1}})}) = -\nu(\theta_{\mathbb{Q}(\mu_{np^{i-1}})}). \tag{13}$$

This shows that $\theta_{\mathbb{Q}(\mu_{np^{i+1}})}$ is divisible by Φ_{i-1}. Applying the same argument to $\theta_{\mathbb{Q}(\mu_{np^{i-1}})}$, $\theta_{\mathbb{Q}(\mu_{np^{i-3}})}$,...repeatedly, we know that $\theta_{\mathbb{Q}(\mu_{np^{i+1}})}$ is divisible by $\Phi_{i-1} \cdot \Phi_{i-3} \cdot ... \cdot \Phi_1$ if i is even, and $\Phi_{i-1} \cdot \Phi_{i-3} \cdot ... \cdot \Phi_2$ if i is odd. Put

$$\tilde{\omega}_i^+ = \prod_{2 \leq j \leq i,\ 2|j} \Phi_j, \quad \tilde{\omega}_i^- = \prod_{1 \leq j \leq i,\ 2\nmid j} \Phi_j.$$

When i is even, we write $\theta_{\mathbb{Q}(\mu_{np^{i+1}})} = \tilde{\omega}_i^- h_i(T)$ for some $h_i(T) \in \mathbb{Z}_p[G_{np^{i+1}}]$. Put $\omega_i^{\pm} = T\tilde{\omega}_i^{\pm}$. Then we have $\omega_i = \tilde{\omega}_i^- \omega_i^+$. Therefore, the equation $\theta_{\mathbb{Q}(\mu_{np^{i+1}})} = \tilde{\omega}_i^- h_i(T)$ determines $h_i(T)$ in $\mathbb{Z}_p[G_{np^{i+1}}]/\omega_i^+$. The relation (13) implies that $((-1)^{\frac{i+2}{2}} h_i(T))_{i:\text{even}}$ is a projective system and defines an element in $\varprojlim \mathbb{Z}_p[G_{np^{i+1}}]/\omega_i^+ = \mathbb{Z}_p[[G_{np^\infty}]]$ where $G_{np^\infty} = \varprojlim G_{np^i}$. We put

$$\theta^+_{\mathbb{Q}(\mu_{np^\infty})} = ((-1)^{\frac{i+2}{2}} h_i(T))_{i:\text{even}} \in \varprojlim \mathbb{Z}_p[G_{np^{i+1}}]/\omega_i^+ = \mathbb{Z}_p[[G_{np^\infty}]].$$

When i is odd, we can write $\theta_{\mathbb{Q}(\mu_{np^{i+1}})} = \tilde{\omega}_i^+ h_i(T)$ for some $h_i(T) \in \mathbb{Z}_p[G_{np^{i+1}}]/\omega_i^-$. The same method as above using (13) shows that $((-1)^{\frac{i+1}{2}} h_i(T))_{i:\text{odd}}$ is a projective system, so we define

$$\theta^-_{\mathbb{Q}(\mu_{np^\infty})} = ((-1)^{\frac{i+1}{2}} h_i(T))_{i:\text{odd}} \in \varprojlim \mathbb{Z}_p[G_{np^{i+1}}]/\omega_i^- = \mathbb{Z}_p[[G_{np^\infty}]].$$

These two elements $\theta^{\pm}_{\mathbb{Q}(\mu_{np^\infty})}$ are Pollack's p-adic L-functions in [22], and $\theta^-_{\mathbb{Q}(\mu_{np^\infty})} \log^+ \pm\sqrt{-p}\theta^+_{\mathbb{Q}(\mu_{np^\infty})} \log^-$ gives p-adic L-functions of Amice -Vélu and Vishik.

For a real abelian field K with conductor m, we define θ_K to be the image of $\theta_{\mathbb{Q}(\mu_m)}$ under the natural restriction map $\mathbb{Z}_p[G_m] \to \mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$. Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension. We define $\theta^{\pm}_{K_\infty} \in \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]]$ to be the image of $\theta^{\pm}_{\mathbb{Q}(\mu_{np^\infty})}$ under the natural restriction map $\mathbb{Z}_p[[G_{np^\infty}]] \to \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]]$.

Consider $\theta^{\pm}_{\mathbb{Q}_\infty} \in \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]] \simeq \mathbb{Z}_p[[T]]$. By $\mu^{\pm}$ we denote the μ-invariant of $\theta^{\pm}_{\mathbb{Q}_\infty}$. Therefore, $\mu^{\pm} = 0$ means that p does not divide $\theta^{\pm}_{\mathbb{Q}_\infty}$, respectively.

Lemma 4.1. *Suppose that $K/\mathbb{Q}$ is a finite abelian extension with conductor n which is prime to p. Let $\pi_0 : \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]] \to \mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$ be the natural projection map. Then we have*

$$\pi_0(\theta^+_{K_\infty}) = (\sigma_p + \sigma_p^{-1})\theta_K, \quad \pi_0(\theta^-_{K_\infty}) = (p-1)\theta_K,$$

where σ_p is the Frobenius automorphism of p in $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. This follows from the construction of $\theta^{\pm}_{K_\infty}$. For a finite abelian extension L/K, we denote by $\pi_{L/K}$ the natural projection $\mathbb{Z}_p[\mathrm{Gal}(L/\mathbb{Q})] \to \mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$ and by $\nu_{L/K}$ the norm homomorphism $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})] \to \mathbb{Z}_p[\mathrm{Gal}(L/\mathbb{Q})]$, which sends $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ to $\sum \tau$ where τ runs over elements in $\mathrm{Gal}(L/\mathbb{Q})$ projecting to σ. Using (1.3) (1), (4) in [19], we have

$$\begin{aligned}\pi_{\mathbb{Q}(\mu_{np^3})/\mathbb{Q}(\mu_n)}(h_2(T)) &= \pi_{\mathbb{Q}(\mu_{np^3})/\mathbb{Q}(\mu_n)}(\theta_{\mathbb{Q}(\mu_{np^3})}/\Phi_1) \\ &= \pi_{\mathbb{Q}(\mu_{np})/\mathbb{Q}(\mu_n)}(-\theta_{\mathbb{Q}(\mu_{np})}) = (\sigma_p + \sigma_p^{-1})\theta_{\mathbb{Q}(\mu_n)}\end{aligned}$$

which implies the first formula. The second formula follows from

$$\begin{aligned}\pi_{\mathbb{Q}(\mu_{np^2})/\mathbb{Q}(\mu_n)}(-h_1(T)) &= \pi_{\mathbb{Q}(\mu_{np^2})/\mathbb{Q}(\mu_n)}(-\theta_{\mathbb{Q}(\mu_{np^2})}) \\ &= \pi_{\mathbb{Q}(\mu_{np})/\mathbb{Q}(\mu_n)}(\nu_{\mathbb{Q}(\mu_{np})/\mathbb{Q}(\mu_n)}(\theta_{\mathbb{Q}(\mu_n)})) \\ &= (p-1)\theta_{\mathbb{Q}(\mu_n)}\end{aligned}$$

where we used (1.3) (4) in [19]. □

Next we modify $\theta^{\pm}_{\mathbb{Q}(\mu_{np^\infty})}$, following the argument in our previous work in §2.1 [15]. We assume that n is a squarefree positive integer with $(n, Np) = 1$. For any d and n such that $d \mid n$, we define $\pi_{n,d} : \mathbb{Z}_p[[G_{np^\infty}]] \to \mathbb{Z}_p[[G_{dp^\infty}]]$ to be the natural projection. Let ℓ be a prime not dividing npN. By (1.3) (1) in [19] we have

$$\pi_{n\ell,n}(\theta^{\pm}_{\mathbb{Q}(\mu_{n\ell p^\infty})}) = (a_\ell - \sigma_\ell - \sigma_\ell^{-1})\theta^{\pm}_{\mathbb{Q}(\mu_{np^\infty})} \tag{14}$$

where $\sigma_\ell \in G_{np^\infty}$ is the Frobenius automorphism. We put

$$\alpha^{\pm}_{d,n} = (\prod_{\ell \mid \frac{n}{d}} (-\sigma_\ell^{-1}))\theta^{\pm}_{\mathbb{Q}(\mu_{dp^\infty})} \in \mathbb{Z}_p[[G_{dp^\infty}]]$$

and

$$\xi^{\pm}_{\mathbb{Q}(\mu_{np^\infty})} = \sum_{d \mid n} \nu_{n,d}(\alpha^{\pm}_{d,n}) \in \mathbb{Z}_p[[G_{np^\infty}]] \tag{15}$$

where $\nu_{n,d} : \mathbb{Z}_p[[G_{dp^\infty}]] \to \mathbb{Z}_p[[G_{np^\infty}]]$ is the norm map defined similarly as $\nu_{L/K}$ in the proof of Lemma 4.1.

Put $P_\ell(x) = x^2 - a_\ell x + \ell$.

Lemma 4.2. *Suppose that ℓ is a prime not dividing npN. Then we have*

$$\pi_{n\ell,n}(\xi^{\pm}_{\mathbb{Q}(\mu_{n\ell p^\infty})}) = (-\sigma_\ell^{-1}P_\ell(\sigma_\ell))\xi^{\pm}_{\mathbb{Q}(\mu_{np^\infty})}$$

where $\sigma_\ell \in G_{np^\infty}$ is the Frobenius automorphism.

Proof. This can be proved by the same method as (7) on page 325 in [15] (where we wrote $P'_\ell(x)$ for $P_\ell(x)$). We give here the computation for the convenience of readers. First of all, we note that

$$-\sigma_\ell^{-1} = (-\sigma_\ell^{-1}P_\ell(\sigma_\ell) - (a_\ell - \sigma_\ell - \sigma_\ell^{-1}))/(\ell - 1) \tag{16}$$

which can be verified very easily. We have

$$\begin{aligned}
\pi_{n\ell,n}(\xi^{\pm}_{\mathbb{Q}(\mu_{n\ell p^\infty})}) &= \pi_{n\ell,n}(\sum_{d|n}\nu_{n\ell,d}(\alpha^{\pm}_{d,n\ell}) + \sum_{d|n}\nu_{n\ell,d\ell}(\alpha^{\pm}_{d\ell,n\ell})) \\
&= (\ell-1)\sum_{d|n}\nu_{n,d}(\alpha^{\pm}_{d,n\ell}) + \sum_{d|n}\nu_{n,d}(\pi_{d\ell,d}(\alpha^{\pm}_{d\ell,n\ell})) \\
&= (\ell-1)\sum_{d|n}\nu_{n,d}(-\sigma_\ell^{-1}\alpha^{\pm}_{d,n}) + \sum_{d|n}\nu_{n,d}((a_\ell - \sigma_\ell - \sigma_\ell^{-1})\alpha^{\pm}_{d,n}) \\
&= (-\sigma_\ell^{-1}P_\ell(\sigma_\ell))\sum_{d|n}\nu_{n,d}(\alpha^{\pm}_{d,n}) \\
&= (-\sigma_\ell^{-1}P_\ell(\sigma_\ell))\xi^{\pm}_{\mathbb{Q}(\mu_{np^\infty})}
\end{aligned}$$

where we used (14) to get the third line and (16) to get the fourth line. □

Suppose that K is a real abelian field with conductor n. We define $\xi^{\pm}_{K_\infty} \in \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]]$ to be the image of $\xi^{\pm}_{\mathbb{Q}(\mu_{np^\infty})}$ under the natural restriction map. Thus we have constructed an equivariant p-adic L-function $\xi^{\pm}_{K_\infty}$ *from modular symbols explicitly.*

As in §3, for a prime ℓ in $\mathcal{P}$, we define $n_\ell \in \mathbb{Z}_{>0}$ by $p^{n_\ell} \| \ell - 1$. We write $\mathbb{Q}(\ell)$ the unique subfield of $\mathbb{Q}(\mu_\ell)$ such that $[\mathbb{Q}(\ell) : \mathbb{Q}] = p^{n_\ell}$. For any $n \in \mathcal{N}$, we define $\mathbb{Q}(n)$ to be the composite field of all $\mathbb{Q}(\ell)$ for ℓ dividing n. The conductor of $\mathbb{Q}(n)$ is n and we use these fields below.

4.3 Annihilation results in the supersingular case

In this subsection we still assume $a_p = 0$.

We first consider $\pm$-local conditions to define $\pm$-Selmer groups, which was first defined by Kobayashi [10]. Suppose that $k/\mathbb{Q}_p$ is a finite unramified

extension, k_∞/k the cyclotomic $\mathbb{Z}_p$-extension, and k_i the i-th layer. We define $E^+(k_i)$ (resp. $E^-(k_i)$) to be the module consisting of elements $x \in E(k_i)$ such that $\mathrm{Tr}_{i,j+1}(x) \in E(k_j)$ for any even (resp. odd) j with $0 \leq j < i$ where $\mathrm{Tr}_{i,j+1} : E(k_i) \to E(k_{j+1})$ is the trace map (see [10] Definition 2.1 and [4] Definition 2.2).

Suppose that $K/\mathbb{Q}$ is a finite abelian p-extension which is unramified at p, and that $n \in \mathbb{Z}_{>0}$ is a squarefree integer which is prime to pN. As in the previous subsection, K_i denotes the i-th layer of the cyclotomic $\mathbb{Z}_p$-extension K_∞/K. We define

$$\mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_i) = \mathrm{Ker}(\mathrm{Sel}_{\mathcal{F}^n}(K_i, E[p^\infty]) \longrightarrow \bigoplus_{v|p} H^1(K_{i,v}, E[p^\infty])/E^{\pm}(K_{i,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

and

$$\mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_\infty) = \varinjlim_i \mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_i).$$

Therefore, the local conditions for $\mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_\infty)$ are relaxed for primes above n, $E^{\pm}(K_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ for primes v above p, and $E(K_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ which is zero otherwise. When $n = 1$, we simply write $\mathrm{Sel}^{\pm}(E/K_\infty)$ for $\mathrm{Sel}^{\pm}_{\mathcal{F}^1}(E/K_\infty)$.

Put $\Lambda_{K_\infty} = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]]$. Let n be a positive integer which is prime to pN and a multiple of the conductor of $K/\mathbb{Q}$. We denote by $\mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_\infty)^\vee$ the Pontrjagin dual of $\mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_\infty)$. By a celebrated argument by Kato [6] and Kobayashi [10], it is known that $\mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_\infty)$ is a torsion Λ_{K_∞}-module. We also know by Kataoka [4] Theorem 5.8 that the projective dimension of $\mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_\infty)^\vee$ is ≤ 1 over Λ_{K_∞}. Consider the Fitting ideal of the $\pm$-Selmer groups (for the definition of Fitting ideal, see [21]).

Theorem 4.3. *Suppose that $K/\mathbb{Q}$ is a finite abelian p-extension with conductor n that is prime to pN. We also assume that E satisfies $a_p = 0$ and $\mu^+ = 0$ (resp. $\mu^- = 0$). Then we have $\xi^+_{K_\infty} \in \mathrm{Fitt}_{\Lambda_{K_\infty}}(\mathrm{Sel}^+_{\mathcal{F}^n}(E/K_\infty)^\vee)$ (resp. $\xi^-_{K_\infty} \in \mathrm{Fitt}_{\Lambda_{K_\infty}}(\mathrm{Sel}^-_{\mathcal{F}^n}(E/K_\infty)^\vee)$).*

Proof. This can be proved by the same method as Theorem 6 (1) in our previous paper [15]. We have an exact sequence

$$0 \longrightarrow \mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_\infty) \longrightarrow H^1_{\mathcal{F}^{npN}}(K_\infty, E[p^\infty]) \longrightarrow \bigoplus_{\ell|pN} H^1(K_\infty \otimes \mathbb{Q}_\ell, E[p^\infty])/L_\ell \longrightarrow 0$$

where $L_\ell = \bigoplus_{v|\ell} E(K_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ if ℓ divides N, and $L_p = \bigoplus_{v|p} E^{\pm}(K_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. The surjectivity of the third map follows from [4] Proposition 5.6.

We also note that $H^1_{\mathcal{F}^{npN}}(K_\infty, E[p^\infty])$ is isomorphic to the étale cohomology group $H^1_{et}(\mathrm{Spec}\ \mathcal{O}_{K_\infty}[1/npN], E[p^\infty])$.

Put $G = \mathrm{Gal}(K/\mathbb{Q})$ and regard it as a subgroup of $\mathrm{Gal}(K_\infty/\mathbb{Q})$. For a subgroup H of G, let F be the fixed subfield of K by H. Then taking the H-invariant part of the above exact sequence and comparing it with the same exact sequence for F_∞, we have an isomorphism

$$\mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/F_\infty) \xrightarrow{\simeq} \mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_\infty)^H. \tag{17}$$

Put $X^{\pm}_{K_\infty} = \mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_\infty)^\vee$ and $X^{\pm}_{F_\infty} = \mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/F_\infty)^\vee$ in this proof. Note that n is not necessarily the conductor of $F/\mathbb{Q}$.

By [4] Proposition 5.6, we have an exact sequence

$$0 \longrightarrow \mathrm{Sel}^{\pm}(E/F_\infty) \longrightarrow \mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/F_\infty) \longrightarrow \bigoplus_{v|n} H^1(F_{\infty,v}, E[p^\infty]) \longrightarrow 0.$$

Let $T_p = T_p(E)$ be the Tate module. For a prime v of F_∞ dividing n we consider the maximal unramified extension $F_{\infty,v,nr}$ and $\Gamma_v = \mathrm{Gal}(F_{\infty,v,nr}/F_{\infty,v})$ which is isomorphic to $\prod_{\ell \neq p} \mathbb{Z}_\ell$ since n is prime to p. Since primes dividing n are good reduction primes, the inertia group of v acts trivially on T_p and we regard T_p as a Γ_v-module. Taking the dual of the above exact sequence, we have an exact sequence

$$0 \longrightarrow \bigoplus_{v|n} (T_p)^{\Gamma_v} \longrightarrow X^{\pm}_{F_\infty} \longrightarrow \mathrm{Sel}^{\pm}(E/F_\infty)^\vee \longrightarrow 0. \tag{18}$$

Since $(T_p)^{\Gamma_v}$ is $\mathbb{Z}_p$-torsion free and $\mathrm{Sel}^{\pm}(E/F_\infty)^\vee$ has no non-trivial finite submodule by Kitajima and Otsuki [9] Theorem 1.3, $X^{\pm}_{F_\infty}$ also has no non-trivial finite submodule (this fact also follows from the projective dimension of $X^{\pm}_{F_\infty} \leq 1$ by Kataoka [4] Theorem 5.8).

Let ψ be any character of G. For any $\mathbb{Z}_p[G]$-module M we denote by M_ψ the ψ-quotient $M_\psi = M \otimes_{\mathbb{Z}_p[G]} \mathcal{O}_\psi$ where $\mathcal{O}_\psi = \mathbb{Z}_p[\mathrm{Image}\ \psi]$ on which G acts via ψ,

Lemma 4.4. *For any character ψ of G, $(X^{\pm}_{K_\infty})_\psi$ has no non-trivial finite submodule.*

Proof. Let H be the kernel of ψ, and F the subfield of K corresponding to H. So ψ is a faithful character of $G/H = \mathrm{Gal}(F/\mathbb{Q})$ which is a cyclic p-group. We use the notation $X^{\pm}_{F_\infty}$ above.

By the above isomorphism (17) we have

$$(X^{\pm}_{K_\infty})_\psi \simeq (X^{\pm}_{F_\infty})_\psi$$

where $X^{\pm}_{F_\infty} = \mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_\infty)^\vee$. Note that n is not necessarily the conductor of $F/\mathbb{Q}$.

We first assume $H \neq G$. Let F' be the subfield of F such that $[F : F'] = p$. Put $N_{F/F'} = \Sigma_{\sigma \in \mathrm{Gal}(F/F')}\sigma$, which we regard as an element of $\mathbb{Z}_p[G/H]$. Then $\mathcal{O}_\psi = \mathbb{Z}_p[G/H]/(N_{F/F'})$. Let σ be a generator of $\mathrm{Gal}(F/F')$. Then $\sigma - 1$ induces a homomorphism

$$\sigma - 1 : (X^{\pm}_{K_\infty})_\psi = X^{\pm}_{F_\infty}/(N_{F/F'}) \longrightarrow X^{\pm}_{F_\infty}.$$

This homomorphism is injective because $H^1(\mathrm{Gal}(F/F'), X^{\pm}_{F_\infty}) = 0$. Also, since $X^{\pm}_{F_\infty}$ has no non-trivial finite submodule as we saw before Lemma 4.4, the above injective homomorphism shows that $(X^{\pm}_{K_\infty})_\psi$ also has no non-trivial finite submodule.

In the case $H = G$, ψ has to be the trivial character and $(X^{\pm}_{K_\infty})_\psi \simeq (X^{\pm}_{\mathbb{Q}_\infty})$ which has no non-trivial finite submodule as we explained before Lemma 4.4. □

Put $\Lambda_\psi = \Lambda_{K_\infty} \otimes_{\mathbb{Z}_p[G]} \mathcal{O}_\psi \simeq \mathcal{O}_\psi[[\mathrm{Gal}(K_\infty/K)]]$ for a character ψ of G. We write $\psi_{K_\infty} : \Lambda_{K_\infty} \to \Lambda_\psi$ for the ring homomorphism induced by ψ.

Lemma 4.5. *We have $\psi_{K_\infty}(\xi^{\pm}_{K_\infty}) \in \mathrm{Fitt}_{\Lambda_\psi}((X^{\pm}_{K_\infty})_\psi)$ for any character ψ of G.*

Proof. Let H be the kernel of ψ as above, F the subfield corresponding to H, $\pi_{K_\infty/F_\infty} : \Lambda_{K_\infty} \to \Lambda_{F_\infty}$ the restriction map, and $\psi_{F_\infty} : \Lambda_{F_\infty} \to \Lambda_\psi$ the ring homomorphism induced by ψ. We denote by $u(\psi)$ the product of primes dividing n, that are unramified in F. Then Lemma 4.2 implies that

$$\psi_{K_\infty}(\xi^{\pm}_{K_\infty}) = \psi_{F_\infty}(\pi_{K_\infty/F_\infty}(\xi^{\pm}_{K_\infty})) = \psi_{F_\infty}(\prod_{\ell | u(\psi)} (-\sigma_\ell^{-1} P_\ell(\sigma_\ell))\psi_{F_\infty}(\xi^{\pm}_{F_\infty}).$$

The construction of the p-adic L-function ξ_{F_∞} in (15) shows that $\psi_{F_\infty}(\xi^{\pm}_{F_\infty}) = \psi_{F_\infty}(\theta^{\pm}_{F_\infty})$, so we get

$$\psi_{K_\infty}(\xi^{\pm}_{K_\infty}) = \psi_{F_\infty}(\prod_{\ell | u(\psi)} (-\sigma_\ell^{-1} P_\ell(\sigma_\ell))\psi_{F_\infty}(\theta^{\pm}_{F_\infty}). \tag{19}$$

On the other hand, by the isomorphism (17) we have $(X^{\pm}_{K_\infty})_\psi = (X^{\pm}_{F_\infty})_\psi$. Lemma 4.4 implies that

$$\mathrm{Fitt}_{\Lambda_\psi}((X^{\pm}_{K_\infty})_\psi) = \mathrm{Fitt}_{\Lambda_\psi}((X^{\pm}_{F_\infty})_\psi) = \mathrm{char}_{\Lambda_\psi}((X^{\pm}_{F_\infty})_\psi) \tag{20}$$

where the right hand side means the characteristic ideal.

We take ψ-quotients of the exact sequence (18). If a rational prime ℓ dividing n is ramified in F, $(\bigoplus_{v|\ell}(T_p)^{\Gamma_v})_\psi$ is finite. If ℓ divides $u(\psi)$, namely ℓ is unramified in F, then $\mathrm{char}_{\Lambda_\psi}((\bigoplus_{v|\ell}(T_p)^{\Gamma_v})_\psi) = (\psi_{F_\infty}(P_\ell(\sigma_\ell)))$ where $P_\ell(x)$ is the polynomial defined just before Lemma 4.2 in the previous subsection.

By an argument due to Kato and Kobayashi we know that $\psi_{F_\infty}(\theta^\pm_{F_\infty})$ is in $\mathrm{char}_{\Lambda_\psi}((\mathrm{Sel}^\pm(E/F_\infty)^\vee)_\psi)$, which we will explain briefly in the following. Put $\mathbf{H}^1(F_{\infty,v}) = \varprojlim H^1(F_{i,v}, T_p(E))$ for a prime v of F_∞ above p. Let $\mathbf{H}^1_\pm(F_{\infty,v}) \subset \mathbf{H}^1(F_{\infty,v})$ be the exact annihilator of $E^\pm(F_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset H^1(F_{\infty,v}, E[p^\infty])$ with respect to the Tate pairing, $\mathrm{Sel}_0(E/F_\infty)$ the kernel of $\mathrm{Sel}^\pm(E/F_\infty) \to \bigoplus_{v|p} E^\pm(F_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, $\mathbf{H}^1_{\mathcal{F}^p}(F_\infty) = \varprojlim H^1_{\mathcal{F}^p}(F_i, T_p(E))$. Then by definitions and global duality theorem we have an exact sequence

$$\mathbf{H}^1_{\mathcal{F}^p}(F_\infty) \xrightarrow{\mathrm{loc}_p} \bigoplus_{v|p} \mathbf{H}^1(F_{\infty,v})/\mathbf{H}^1_\pm(F_{\infty,v}) \longrightarrow \mathrm{Sel}^\pm(E/F_\infty)^\vee \longrightarrow \mathrm{Sel}_0(E/F_\infty)^\vee \longrightarrow 0. \tag{21}$$

There exists Kato's zeta element $z_{F_\infty} \in \mathbf{H}^1_{\mathcal{F}^p}(F_\infty)$ and Coleman homomorphisms

$$\mathrm{Col}^\pm : \bigoplus_{v|p} \mathbf{H}^1(F_{\infty,v})/\mathbf{H}^1_\pm(F_{\infty,v}) \xrightarrow{\simeq} \Lambda_{F_\infty},$$

which are bijective in our setting (see Kataoka [4] Theorem 4.26) such that $\mathrm{Col}^\pm(\mathrm{loc}_p(z_{F_\infty})) = \theta^\pm_{F_\infty}$ by Kataoka [4] Theorem 6.9. Let M be the cokernel of loc_p in (21). Then, putting Z to be the submodule generated by z_{F_∞}, we have an exact sequence

$$(\mathbf{H}^1_{\mathcal{F}^p}(F_\infty)/Z)_\psi \longrightarrow \Lambda_\psi/(\psi_{F_\infty}(\theta^\pm_{F_\infty})) \longrightarrow M_\psi \longrightarrow 0.$$

Since $\psi_{F_\infty}(\theta^\pm_{F_\infty}) \neq 0$, the first map is injective. Therefore, by (21) and the above exact sequence we have

$$\begin{aligned}
&\mathrm{char}_{\Lambda_\psi}(\mathrm{Sel}_0(E/F_\infty)^\vee)_\psi \,\mathrm{char}_{\Lambda_\psi} M_\psi \\
&= \mathrm{char}_{\Lambda_\psi}(\mathrm{Sel}_0(E/F_\infty)^\vee)_\psi (\mathrm{char}_{\Lambda_\psi}(\mathbf{H}^1_{\mathcal{F}^p}(F_\infty)/Z)_\psi)^{-1} \psi_{F_\infty}(\theta^\pm_{F_\infty}) \\
&\subset \mathrm{char}_{\Lambda_\psi} \mathrm{Sel}^\pm(E/F_\infty)^\vee.
\end{aligned}$$

Applying Theorem 12.5 (4) in Kato [6] for the modular form f_E twisted by ψ where f_E is the modular form corresponding to E, we know that $\mathrm{char}_{\Lambda_\psi}(\mathbf{H}^1_{\mathcal{F}^p}(F_\infty)/Z)_\psi \subset \mathrm{char}_{\Lambda_\psi}(\mathrm{Sel}_0(E/F_\infty)^\vee)_\psi$. Therefore, using the above inclusion, we have

$$\psi_{F_\infty}(\theta^\pm_{F_\infty}) \in \mathrm{char}_{\Lambda_\psi} \mathrm{Sel}^\pm(E/F_\infty)^\vee. \tag{22}$$

It follows from (18), (19), (20), (22) that $\psi_{K_\infty}(\xi^{\pm}_{K_\infty}) \in \mathrm{Fitt}_{\Lambda_\psi}((X^{\pm}_{K_\infty})_\psi)$. $\square$

We go back to the proof of Theorem 4.3. Suppose that $\mu^+ = 0$. Then there is a coefficient of $\theta^+_{\mathbb{Q}_\infty} \in \Lambda_{\mathbb{Q}_\infty} = \mathbb{Z}_p[[T]]$ which is not divisible by p. Then by the construction of $\theta^{\pm}_{K_\infty}$ and (1.3) (1) in [19], there is a coefficient of $\theta^+_{K_\infty} \in \Lambda_{K_\infty} = \mathbb{Z}_p[G][[T]]$ which is not divisible by p. Thus for any character ψ of G, the μ-invariant of $\psi_{F_\infty}(\theta^+_{F_\infty})$ is zero. Therefore, the μ-invariant of $(\mathbf{H}^1_{\mathcal{F}^p}(F_\infty)/Z)_\psi$ is zero. By Kato [6] Theorem 12.5 (4) the μ-invariant of $(\mathrm{Sel}_0(E/F_\infty)^\vee)_\psi$ is also zero, which implies the vanishing of the μ-invariant of $(\mathrm{Sel}^+(E/F_\infty)^\vee)_\psi$. Therefore, applying Lemma 4.1 in [11] for example, we obtain $\xi^+_{K_\infty} \in \mathrm{Fitt}_{\Lambda_{K_\infty}}(X^+_{K_\infty})$ from Lemma 4.5.

The same proof works in the case $\mu^- = 0$. This completes the proof of Theorem 4.3. $\square$

Remark 4.6. (1) It is conjectured that $\mathrm{Fitt}_{\Lambda_{K_\infty}}(\mathrm{Sel}^{\pm}_{\mathcal{F}^n}(E/K_\infty)^\vee)$ is generated by $\xi^{\pm}_{K_\infty}$. The main conjecture for $\mathbb{Q}_\infty / \mathbb{Q}$, namely $\mathrm{char}(\mathrm{Sel}^{\pm}(E/\mathbb{Q}_\infty)^\vee) = (\theta^{\pm}_{\mathbb{Q}_\infty})$, implies this conjecture.
(2) We cannot apply Theorem 1.5 in Kataoka [4] to show Theorem 4.3 because he assumes $E(\mathbb{Q}_\ell)[p] = 0$ for primes dividing the conductor n of $K/\mathbb{Q}$ in Theorem 1.5 (a) in [4].

Theorem 4.3 implies the following.

Theorem 4.7. *Let K be as in Theorem 4.3.*
(1) *If $\mu^+ = 0$ (resp. $\mu^- = 0$), then $\theta^+_{K_\infty}$ (resp. $\theta^-_{K_\infty}$) annihilates $\mathrm{Sel}^+(E/K_i)^\vee$ (resp. $\mathrm{Sel}^-(E/K_i)^\vee$) for any $i > 0$.*
(2) *Suppose that $\mu^+ = 0$ or $\mu^- = 0$. Then θ_K annihilates $\mathrm{Sel}(E/K)^\vee$.*

Proof. (1) This can be proved by the same method as Theorem 8 in our previous paper [15] which treats the ordinary case. We prove the statement for $+$. The statement for $-$ can be proved by the same method. If $\mu^+ = 0$, then by Theorem 4.3, $\xi^+_{K_\infty}$ annihilates $\mathrm{Sel}^+(E/K_\infty)^\vee$. We can show that $\theta^+_{K_\infty}$ annihilates $\mathrm{Sel}^+(E/K_\infty)^\vee$ by induction on $[K : \mathbb{Q}]$. In fact, $\theta^+_{F_\infty}$ is in $\mathrm{Ann}_{\Lambda_{F_\infty}} \mathrm{Sel}^+(E/K_\infty)^\vee$ for any subfield $F \subsetneq K$ by induction on $[K : \mathbb{Q}]$, which implies $\nu_{K_\infty/F_\infty}(\theta^+_{F_\infty}) \in \mathrm{Ann}_{\Lambda_{K_\infty}} \mathrm{Sel}^+(E/K_\infty)^\vee$. By the construction of $\xi^+_{K_\infty}$, we know that $\xi^+_{K_\infty} - \theta^+_{K_\infty}$ is a linear combination of $(\nu_{K_\infty/F_\infty}(\theta^+_{F_\infty}))_{F \subsetneq K}$ where F runs over all subfields of K with $F \subsetneq K$. It follows from $\xi^+_{K_\infty} \in \mathrm{Ann}_{\Lambda_{K_\infty}} \mathrm{Sel}^+(E/K_\infty)^\vee$ that

$$\theta^+_{K_\infty} \in \mathrm{Ann}_{\Lambda_{K_\infty}} \mathrm{Sel}^+(E/K_\infty)^\vee.$$

Since $E(K)[p] = 0$, the natural map $\mathrm{Sel}^{\pm}(E/K_i) \to \mathrm{Sel}^{\pm}(E/K_\infty)$ is injective. So the dual of this map is surjective. Therefore, $\theta^{+}_{K_\infty}$ annihilates $\mathrm{Sel}^{+}(E/K_i)^{\vee}$.
(2) Using Lemma 4.1, we know that the image of $\theta^{\pm}_{K_\infty}$ in $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$ is $u\theta_K$ for some unit $u \in \mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]^{\times}$. Therefore, the injectivity of $\mathrm{Sel}(E/K) \to \mathrm{Sel}^{\pm}(E/K_\infty)$ and $\theta^{\pm}_{K_\infty} \in \mathrm{Ann}_{\Lambda_{K_\infty}} \mathrm{Sel}^{\pm}(E/K_\infty)^{\vee}$ imply $\theta_K \in \mathrm{Sel}(E/K)^{\vee}$. □

4.4 Euler systems of Gauss sum type in the supersingular case

We continue to assume $a_p = 0$ in this subsection. We also assume $\mu^{\pm} = 0$ by which we mean $\mu^{+} = 0$ or $\mu^{-} = 0$. In this and the next subsections we prove several statements on the objects with $\pm$, which mean that if we assume $\mu^{+} = 0$, then the statements on the objects with $+$ hold, and if we assume $\mu^{-} = 0$, then the statements on the objects with $-$ hold.

In this subsection we construct Euler systems of Gauss sum type in the case $a_p = 0$. Concerning the ordinary case, see our previous papers [15] §3 and [14] §§6, 7.

We defined the set $\mathcal{P}^{(m)}$ of prime numbers for $m \in \mathbb{Z}_{>0}$ in the beginning of §2.1. For any number field F, we define

$$\mathcal{P}^{(m)}(F) = \{\ell \in \mathcal{P}^{(m)} \mid \ell \text{ splits completely in } F\}.$$

If ℓ is in $\mathcal{P}^{(m)}(F)$ and v is a prime of F above ℓ, we have

$$H^1(F_v, E[p^m])/(E(F_v)\otimes\mathbb{Z}/p^m) \simeq E(F_v)[p^m](-1) = E(\mathbb{F}_\ell)[p^m](-1) \simeq \mathbb{Z}/p^m.$$

For any $\ell \in \mathcal{P}^{(m)}$, we define

$$\mathcal{H}^2_\ell(F) = \bigoplus_{v|\ell} H^1(F_v, E[p^m])/(E(F_v) \otimes \mathbb{Z}/p^m) \simeq \bigoplus_{v|\ell} E(F_v)[p^m](-1). \quad (23)$$

The notation $\mathcal{H}^2_\ell(F)$ comes from the second local cohomology with support (cf. Milne [20] II §1). For a finite abelian extension $F/\mathbb{Q}$ we put $R_F = \mathbb{Z}/p^m[\mathrm{Gal}(F/\mathbb{Q})]$. For $\ell \in \mathcal{P}^{(m)}(F)$ we fix a prime v of F above ℓ and a generator $t_v \in E(F_v)[p^m](-1) \simeq \mathbb{Z}/p^m$, and take an element $t_{\ell,F} \in \mathcal{H}^2_\ell(F)$ whose v component is t_v and whose other components are zero. Then $\mathcal{H}^2_\ell(F)$ is a free R_F-module of rank 1 with basis t_ℓ. When $F' \subset F$ and $\ell \in \mathcal{P}^{(m)}(F)$, we always take the prime $v_{F'}$ of F' below v and define $t_{\ell,F'}$ as the image of $t_{\ell,F}$ in $\mathcal{H}^2_\ell(F')$.

Let $K/\mathbb{Q}$ be a finite abelian p-extension which is unramified at p, and K_i the i-th layer of the cyclotomic $\mathbb{Z}_p$-extension K_∞/K. For a p-adic prime v of K_i with $i \in \mathbb{Z}_{>0}$, $E^\pm(K_{i,v})$ is defined in the previous subsection. For $i = 0$, namely for $K_0 = K$, we define $E^\pm(K_{0,v}) = E(K_{0,v})$. Note that for a prime v of K_i with $i \geq 0$, $E(K_{0,v}) \subset E^\pm(K_{i,v})$. As in the previous subsection, we define $\mathrm{Sel}^\pm(E/K_i)$ to be the kernel of the natural map from $H^1_{\mathcal{F}^p}(K_i, E[p^\infty])$ to $\bigoplus_{v|p} H^1(K_{i,v}, E[p^\infty])/(E^\pm(K_{i,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ for any $i \geq 0$. When $i = 0$, $\mathrm{Sel}^\pm(E/K) = \mathrm{Sel}(E/K)$ by definition.

For any $m > 0$ we define $L^\pm_{i,v,m}$ to be the inverse image of $E^\pm(K_{i,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ under $E(K_{i,v})/p^m \to E(K_{i,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, and define $\mathrm{Sel}^\pm(K_i, E[p^m])$ by

$$\mathrm{Sel}^\pm(K_i, E[p^m]) = \mathrm{Ker}(\mathrm{Sel}(K_i, E[p^m]) \longrightarrow \bigoplus_{v|p} H^1(K_{i,v}, E[p^m])/L^\pm_{i,v,m}).$$

Since $E(\mathbb{Q})[p] = 0$, we get $E(K_i)[p] = 0$, which implies that $\mathrm{Sel}^\pm(K_i, E[p^m])$ coincides with the kernel of the multiplication by p^m on $\mathrm{Sel}^\pm(E/K_i)$.

Put $T_p = T_p(E)$. Let $H^1_\pm(K_{i,v}, T_p) \subset H^1(K_{i,v}, T_p)$ be the exact annihilator of $E^\pm(K_{i,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ in $H^1(K_{i,v}, E[p^\infty])$ with respect to the Tate pairing. We define $H^\pm_{i,v,m}$ to be the image of $H^1_\pm(K_{i,v}, T_p)$ under the map $H^1(K_{i,v}, T_p) \to H^1(K_{i,v}, E[p^m])$. So $H^\pm_{i,v,m} \subset H^1(K_{i,v}, E[p^m])$ is the exact annihilator of $L^\pm_{i,v,m}$ in $H^1(K_{i,v}, E[p^m])$. We define $H^1_{\mathcal{F}_\pm}(K_i, E[p^m])$ by

$$H^1_{\mathcal{F}_\pm}(K_i, E[p^m]) = \mathrm{Ker}(H^1_{\mathcal{F}^p}(K_i, E[p^m]) \longrightarrow \bigoplus_{v|p} H^1(K_{i,v}, E[p^m])/H^\pm_{i,v,m}).$$

For any squarefree positive integer n which is prime to p, we also define

$$H^1_{\mathcal{F}^n_\pm}(K_i, E[p^m]) = \mathrm{Ker}(H^1_{\mathcal{F}^{np}}(K_i, E[p^m]) \longrightarrow \bigoplus_{v|p} H^1(K_{i,v}, E[p^m])/H^\pm_{i,v,m}).$$

Note that for $i = 0$, we know $L^\pm_{0,v,m} = E(K_v) \otimes \mathbb{Z}/p^m$, so $H^1_{\mathcal{F}^n_\pm}(K, E[p^m]) = \mathrm{Sel}_{\mathcal{F}^n}(K, E[p^m])$.

By global duality theorem (see [18] Theorem 2.3.4) we get

Lemma 4.8. *The sequence*

$$0 \longrightarrow H^1_{\mathcal{F}_\pm}(K_i, E[p^m]) \longrightarrow H^1_{\mathcal{F}^n_\pm}(K_i, E[p^m]) \longrightarrow \bigoplus_{\ell|n} \mathcal{H}^2_\ell(K_i) \longrightarrow \mathrm{Sel}^\pm(K_i, E[p^m])^\vee$$

is exact.

We will define an element $g_\ell^\pm \in \mathrm{Sel}_{\mathcal{F}^\ell}(K, E[p^m])$.

As in the proof of Theorem 4.3 (see (21)) we put $\mathbf{H}^1_{\mathcal{F}^p}(K_\infty) = \varprojlim H^1_{\mathcal{F}^p}(K_i, T_p(E))$, $\mathbf{H}^1(K_{\infty,v}) = \varprojlim H^1(K_{i,v}, T_p(E))$, and $\mathbf{H}^1_\pm(K_{\infty,v}) = \varprojlim H^1_\pm(K_{i,v}, T_p(E))$. Then Kato's zeta element z_{K_∞} goes to $\theta^\pm_{K_\infty}$ by the homomorphism

$$\mathrm{Col}^\pm \circ \mathrm{loc}_p : \mathbf{H}^1_{\mathcal{F}^p}(K_\infty) \longrightarrow \bigoplus_{v|p} \mathbf{H}^1(K_{\infty,v})/\mathbf{H}^1_\pm(K_{\infty,v}) \xrightarrow{\simeq} \Lambda_{K_\infty}$$

as we mentioned in the proof of Theorem 4.3. Since $\theta^\pm_{K_\infty}$ is a non-zero divisor and $\mathbf{H}^1_{\mathcal{F}^p}(K_\infty)$ is $\mathbb{Z}_p$-torsion free, the above map $\mathbf{H}^1_{\mathcal{F}^p}(K_\infty) \longrightarrow \bigoplus_{v|p} \mathbf{H}^1(K_{\infty,v})/\mathbf{H}^1_\pm(K_{\infty,v})$ is injective, which implies that $\varprojlim H^1_{\mathcal{F}_\pm}(K_i, T_p(E)) = 0$. Also, since $\mathrm{Sel}^\pm(E/K_\infty)^\vee$ is a free $\mathbb{Z}_p$-module of finite rank by our assumption $\mu^\pm = 0$ as we explained in the proof of Theorem 4.3, we have $\varprojlim H^1_{\mathcal{F}_\pm}(K_i, E[p^m]) = 0$. Therefore, we can take $i > 0$ such that the corestriction map $H^1_{\mathcal{F}_\pm}(K_i, E[p^m]) \to H^1_{\mathcal{F}_\pm}(K, E[p^m])$ is the zero map.

For a prime $\ell \in \mathcal{P}^{(m)}(K_i)$, we will define $g_\ell^\pm \in \mathrm{Sel}_{\mathcal{F}^\ell}(K, E[p^m])$ using the method of Lemma 6.9 in [14]. By Lemma 4.8 we have an exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}_\pm}(K_i, E[p^m]) \longrightarrow H^1_{\mathcal{F}^\ell_\pm}(K_i, E[p^m]) \xrightarrow{\partial_\ell} \mathcal{H}^2_\ell(K_i) \xrightarrow{\lambda_\ell} \mathrm{Sel}^\pm(K_i, E[p^m])^\vee$$

where we named the third map and the fourth map ∂_ℓ and λ_ℓ.

Lemma 4.9. *We take K_i such that $H^1_{\mathcal{F}_\pm}(K_i, E[p^m]) \to H^1_{\mathcal{F}_\pm}(K, E[p^m])$ is the zero map. Suppose that two elements g, g' in $H^1_{\mathcal{F}^\ell_\pm}(K_i, E[p^m])$ satisfy $\partial_\ell(g) = \partial_\ell(g')$. Then we have $\mathrm{Cor}_{K_i/K}(g) = \mathrm{Cor}_{K_i/K}(g')$ where $\mathrm{Cor}_{K_i/K} : H^1_{\mathcal{F}^\ell_\pm}(K_i, E[p^m]) \to H^1_{\mathcal{F}^\ell_\pm}(K, E[p^m]) = \mathrm{Sel}_{\mathcal{F}^\ell}(K, E[p^m])$ is the corestriction map.*

Proof. In fact, $g - g'$ is in the kernel of ∂_ℓ, so in $H^1_{\mathcal{F}_\pm}(K_i, E[p^m])$. Therefore, $\mathrm{Cor}_{K_i/K}(g - g') = 0$, which implies $\mathrm{Cor}_{K_i/K}(g) = \mathrm{Cor}_{K_i/K}(g')$. □

We define $u_\pm \in \mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$ by $u_+ = \sigma_p + \sigma_p^{-1}$ and $u_- = (p-1)$. They are units in $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$ and we regard them as units in $\mathbb{Z}_p[\mathrm{Gal}(K_i/\mathbb{Q})] = \mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})][\mathrm{Gal}(K_i/K)]$. Since

$$\lambda_\ell((u_\pm)^{-1}\theta^\pm_{K_\infty} t_{\ell,K_i}) = (u_\pm)^{-1}\theta^\pm_{K_\infty}\lambda_\ell(t_{\ell,K_i}) = 0$$

in $\mathrm{Sel}^\pm(K_i, E[p^m])^\vee$ by Theorem 4.7 (1), there is $\tilde{g}_\ell^\pm \in H^1_{\mathcal{F}^\ell_\pm}(K_i, E[p^m])$ such that $\partial_\ell(\tilde{g}_\ell^\pm) = (u_\pm)^{-1}\theta^\pm_{K_\infty} t_{\ell,K_i}$ by the above exact sequence. We define

$$g^\pm_{\ell,K} = \mathrm{Cor}_{K_i/K}(\tilde{g}_\ell^\pm) \in H^1_{\mathcal{F}^\ell_\pm}(K, E[p^m]) = \mathrm{Sel}_{\mathcal{F}^\ell}(K, E[p^m]). \tag{24}$$

Then $g^{\pm}_{\ell,K}$ does not depend on the choice of $\tilde{g}^{\pm}_{\ell} \in H^1_{\mathcal{F}^{\ell}_{\pm}}(K_i, E[p^m])$ by Lemma 4.9. When no confusion arises, we write $g^{\pm}_{\ell}$ for $g^{\pm}_{\ell,K}$.

For any finite abelian p-extension $K/\mathbb{Q}$ which is unramified at p, we take minimal i such that $H^1_{\mathcal{F}_{\pm}}(K_i, E[p^m]) \to H^1_{\mathcal{F}_{\pm}}(K, E[p^m])$ is the zero map, and define the subset $\mathcal{P}^{(m)}(K)'$ of $\mathcal{P}^{(m)}(K)$ by $\mathcal{P}^{(m)}(K)' = \mathcal{P}^{(m)}(K_i)$.

Proposition 4.10. *Suppose that $K/\mathbb{Q}$ is a finite abelian p-extension which is unramified at p, and that $\ell \in \mathcal{P}^{(m)}(K)'$.*
(1) *For $g^{\pm}_{\ell,K} \in \mathrm{Sel}_{\mathcal{F}^{\ell}}(K, E[p^m])$ we have*

$$\partial_{\ell}(g^{\pm}_{\ell,K}) = \theta_K t_{\ell,K} \in \mathcal{H}^2_{\ell}(K) = R_F t_{\ell,K}$$

where ∂_{ℓ} is the natural map $\mathrm{Sel}_{\mathcal{F}^{\ell}}(K, E[p^m]) \to \mathcal{H}^2_{\ell}(K)$.
(2) *For any subfield $F \subset K$ we can define $g^{\pm}_{\ell,F} \in \mathrm{Sel}_{\mathcal{F}^{\ell}}(F, E[p^m])$ using F_i similarly. Then denoting the conductor of K and F by n_K and n_F, we have*

$$\mathrm{Cor}_{K/F}(g^{\pm}_{\ell,K}) = (\prod_{r|(n_K/n_F)} (a_r - \sigma_r - \sigma_r^{-1}))g^{\pm}_{\ell,F}$$

where r runs over primes which are ramified in K and unramified in F, and σ_r is the Frobenius automorphism.

Proof. (1) By definition we have

$$\partial_{\ell}(g^{\pm}_{\ell,K}) = (u_{\pm})^{-1}\theta^{\pm}_{K_{\infty}} t_{\ell,K} = (u_{\pm})^{-1}\pi_{K_{\infty}/K}(\theta_{K_{\infty}})t_{\ell,K}.$$

Therefore, Proposition 4.10 (1) follows from Lemma 4.1.
(2) Suppose that $H^1_{\mathcal{F}_{\pm}}(K_i, E[p^m]) \to H^1_{\mathcal{F}_{\pm}}(K, E[p^m])$ is the zero map. First of all, since $E(F_i)[p] = 0$, the restriction maps $H^1_{\mathcal{F}_{\pm}}(F_j, E[p^m]) \to H^1_{\mathcal{F}_{\pm}}(K_j, E[p^m])$ with $j = i, 0$ are both injective. So the corestriction map $H^1_{\mathcal{F}_{\pm}}(F_i, E[p^m]) \to H^1_{\mathcal{F}_{\pm}}(F, E[p^m])$ is also the zero map, and we can define $g^{\pm}_{\ell,F}$ as $\mathrm{Cor}_{F_i/F}(\tilde{g}^{\pm}_{\ell,F_i})$, using $\tilde{g}^{\pm}_{\ell,F_i}$ such that $\partial_{\ell}(\tilde{g}^{\pm}_{\ell,F_i}) = (u_{\pm})^{-1}\theta^{\pm}_{F_{\infty}} t_{\ell,F_i}$.

We write $\tilde{g}^{\pm}_{\ell,K_i}$ for $\tilde{g}^{\pm}_{\ell}$ which was used as $\mathrm{Cor}_{K_i/K}(\tilde{g}^{\pm}_{\ell}) = g_{\ell,K}$ when we defined $g_{\ell,K}$. Since

$$\pi_{K_{\infty}/F_{\infty}}(\theta^{\pm}_{K_{\infty}}) = (\prod_{r|(n_K/n_F)} (a_r - \sigma_r - \sigma_r^{-1}))\theta^{\pm}_{F_{\infty}}$$

by (1.3) (1) in [19], we have

$$\partial_{\ell}(\mathrm{Cor}_{K_i/F_i}(\tilde{g}^{\pm}_{\ell,K_i})) = \partial_{\ell}((\prod_{r|(n_K/n_F)} (a_r - \sigma_r - \sigma_r^{-1}))\tilde{g}^{\pm}_{\ell,F_i}).$$

It follows from Lemma 4.9 applying to F_i/F with two elements $\mathrm{Cor}_{K_i/F_i}(\tilde{g}^{\pm}_{\ell,K_i})$ and $(\prod_{r|(n_K/n_F)}(a_r-\sigma_r-\sigma_r^{-1}))\tilde{g}^{\pm}_{\ell,F_i}$ that we get the conclusion of Proposition 4.10 (2). □

Proposition 4.10 (2) means that $(g_{\ell,F})_{F\subset K}$ forms an Euler system. We have to note that this is a finite family unlike usual Euler systems, and several arguments in [26] cannot be applied.

Remark 4.11. The method to construct Euler systems of Gauss sum type explained here is the same as in [14]. We recently have a new method to construct Euler and Kolyvagin systems of Gauss sum type, and can define $g_{\ell,F}$ for any $\ell \in \mathcal{P}^{(m)}(F)$ (see [17]).

4.5 Kolyvagin derivatives and systems of Gauss sum type in the supersingular case

In this subsection we construct Kolyvagin derivatives by a standard method.

Let n be an integer in $\mathcal{N}^{(m)}$ and consider the abelian p-extension $\mathbb{Q}(n)/\mathbb{Q}$ which was defined in the end of §4.2. For $\mathbb{Q}(n)$ and $\ell \in \mathcal{P}^{(m)}(\mathbb{Q}(n))'$, we constructed $g^{\pm}_{\ell,\mathbb{Q}(n)} \in \mathrm{Sel}_{\mathcal{F}^\ell}(K, E[p^m])$ in Proposition 4.10.

For a prime $r \in \mathcal{P}^{(m)}$, we put $\mathcal{G}_r = \mathrm{Gal}(\mathbb{Q}(r)/\mathbb{Q})$. We defined $n_r \in \mathbb{Z}_{>0}$ in the end of §4.2, which can be regarded as $p^{n_r} = [\mathbb{Q}(r) : \mathbb{Q}]$. For $n \in \mathcal{N}^{(m)}$, we define $\mathcal{G}_n$ by $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}(n)/\mathbb{Q})$. Recall that we fixed a generator g_r of $\mathbb{F}_r^\times$ for each prime $r \in \mathcal{P}$ when we defined $\log_{\mathbb{F}_r}$ in (2). We take a generator τ_r of $\mathcal{G}_r \simeq \mathbb{F}_\ell^\times$ corresponding to the generator g_r of $\mathbb{F}_r^\times$, and define

$$N_r = \textstyle\sum_{i=0}^{p^{n_r}-1} \tau_r^i \in \mathbb{Z}[\mathcal{G}_r], \quad D_r = \sum_{i=0}^{p^{n_r}-1} i\tau_r^i \in \mathbb{Z}[\mathcal{G}_r],$$

$$N_n = \textstyle\prod_{r|n} N_r \in \mathbb{Z}[\mathcal{G}_n], \qquad D_n = \prod_{r|n} D_r \in \mathbb{Z}[\mathcal{G}_n]$$

as usual.

Lemma 4.12. *For $n \in \mathcal{N}^{(m)}$, we have*

$$D_n g^{\pm}_{\ell,\mathbb{Q}(n)} \in \mathrm{Sel}_{\mathcal{F}^\ell}(\mathbb{Q}(n), E[p^m])^{\mathcal{G}_n}.$$

Proof. For any r dividing n, since r is a good reduction prime, r is unramified in $\mathbb{Q}(E[p^m])$. The action of the Frobenius automorphism σ_r on $E[p^m]$ is conjugate to $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ since $E(\mathbb{F}_r)[p^m] \simeq \mathbb{Z}/p^m$ and the determinant is $r \equiv 1 \pmod{p^m}$. Thus $a_r \equiv 2 \pmod{p^m}$. Therefore, $\sigma_r - 1$ divides $a_r - \sigma_r - \sigma_r^{-1}$

in $\mathbb{Z}/p^m[\mathrm{Gal}(\mathbb{Q}(n/r)/\mathbb{Q})]$. Using this divisibility and a well-known formula $D_r(\tau_r - 1) = p^{n_r} - N_r$, we have

$$D_n g^{\pm}_{\ell,\mathbb{Q}(n)} \in \mathrm{Sel}_{\mathcal{F}^\ell}(\mathbb{Q}(n), E[p^m])^{\mathcal{G}_n}$$

by the argument of Lemma 2.1 in Rubin [24]. □

Lemma 4.13. *Suppose that p does not divide* $\mathrm{Tam}(E)$*, and $n\ell \in \mathcal{N}^{(m)}$. Then the natural homomorphism*

$$\mathrm{Sel}_{\mathcal{F}^{n\ell}}(\mathbb{Q}, E[p^m]) \xrightarrow{\simeq} \mathrm{Sel}_{\mathcal{F}^{n\ell}}(\mathbb{Q}(n), E[p^m])^{\mathcal{G}_n}$$

is bijective.

Proof. This can be proved by the same method as Lemma 2 on page 338 in our previous paper [15]. This lemma follows from the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}_{\mathcal{F}^{n\ell}}(\mathbb{Q}, E[p^m]) & \longrightarrow & H^1_{\mathcal{F}^{n\ell p^N}}(\mathbb{Q}, E[p^m]) & \longrightarrow & \bigoplus_{\ell|pN} \mathcal{H}^2_\ell(\mathbb{Q}) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Sel}_{\mathcal{F}^{n\ell}}(\mathbb{Q}(n), E[p^m])^{\mathcal{G}_n} & \longrightarrow & H^1_{\mathcal{F}^{n\ell p^N}}(\mathbb{Q}(n), E[p^m])^{\mathcal{G}_n} & \longrightarrow & \bigoplus_{\ell|pN} \mathcal{H}^2_\ell(\mathbb{Q}(n))^{\mathcal{G}_n}.
\end{array}$$

In fact, $H^0(\mathbb{Q}, E[p^m]) = 0$ implies the bijectivity of the middle vertical arrow. For $\ell \mid N$, our assumption $p \nmid \mathrm{Tam}(E)$ implies that $\mathcal{H}^2_\ell(\mathbb{Q}) \to \mathcal{H}^2_\ell(\mathbb{Q}(n))$ is injective (see Greenberg [3] §3). For $\ell = p$, the Pontrjagin dual of $\mathcal{H}^2_p(\mathbb{Q}) \to \mathcal{H}^2_p(\mathbb{Q}(n))$ is $\bigoplus_{v|p} E(\mathbb{Q}(n)_v)/p^m \to E(\mathbb{Q}_p)/p^m$. Since $a_p = 0$, $E(\mathbb{Q}(n)_v)/p^m$ is $\hat{E}(m_{\mathbb{Q}(n)_v})/p^m$ where $\hat{E}$ is the formal group associated to E and $m_{\mathbb{Q}(n)_v}$ is the maximal ideal of the ring of integers of $\mathbb{Q}(n)_v$. Since $\mathbb{Q}(n)_v/\mathbb{Q}_p$ is unramified, the norm map $\hat{E}(m_{\mathbb{Q}(n)_v}) \to \hat{E}(p\mathbb{Z}_p)$ is surjective. Thus the right vertical arrow is injective, which implies that the left vertical arrow is bijective. □

Recall that we defined $\delta^{(m)}_n \in \mathbb{Z}/p^m$ in (7). By definition, $\delta^{(m)}_n \bmod p$ is δ_n.

Proposition 4.14. *There exists a unique element $\kappa^{\pm}_{n,\ell} \in \mathrm{Sel}_{\mathcal{F}^{n\ell}}(\mathbb{Q}, E[p^m])$ whose image in $\mathrm{Sel}_{\mathcal{F}^{n\ell}}(\mathbb{Q}(n), E[p^m])$ is $D_n g^{\pm}_{\ell,\mathbb{Q}(n)}$. We have*

$$\partial_\ell(\kappa^{\pm}_{n,\ell}) = (-1)^{\nu(n)} \delta^{(m)}_n t_{\ell,\mathbb{Q}}$$

where $\partial_\ell : \mathrm{Sel}_{\mathcal{F}^{n\ell}}(\mathbb{Q}, E[p^m]) \to \mathcal{H}^2_\ell(\mathbb{Q}) = (\mathbb{Z}/p^m)t_{\ell,\mathbb{Q}}$ is the natural map.

Proof. The existence of $\kappa^{\pm}_{n,\ell}$ follows from Lemmas 4.12 and 4.13.

Suppose that $n = r_1 \cdot ... \cdot r_t$. Using $D_r(\tau_r - 1) = p^{n_r} - N_r$, (1.3) (1) in [19], and the fact that $\sigma_r - 1$ divides $a_r - \sigma_r - \sigma_r^{-1}$, we can show by induction on $\nu(n)$ that $\theta_{\mathbb{Q}(n)}$ can be written as

$$\theta_{\mathbb{Q}(n)} \equiv c \prod_{i=1}^{t} (\tau_{r_i} - 1) \mod (p^m, (\tau_{r_1} - 1)^2, ..., (\tau_{r_t} - 1)^2) \tag{25}$$

for some $c \in \mathbb{Z}/p^m$ (see [12] Lemma 4.4). We regard $\theta_{\mathbb{Q}(n)}$ as a polynomial in τ_{r_1},...,τ_{r_t}, and take $\dfrac{\partial}{\partial \tau_{r_1}} ... \dfrac{\partial}{\partial \tau_{r_t}}$ of both sides of the above formula. Then we get

$$c = \sum_{\substack{a=1 \\ (a,n)=1}}^{n} [\frac{a}{n}](\prod_{\ell | n} \log_{\mathbb{F}_\ell}(a)) = \delta_n^{(m)} \in \mathbb{Z}/p^m$$

since $\theta_{\mathbb{Q}(n)}$ is the image of $\theta_{\mathbb{Q}(\mu_n)}$ in (12) under the natural restriction map.

We take D_n of (25) to get

$$D_n \theta_{\mathbb{Q}(n)} = (-1)^{\nu(n)} N_n \delta_n^{(m)} \quad \in \mathbb{Z}/p^m[\mathcal{G}_n]$$

using $D_r(\tau_r - 1) = p^{n_r} - N_r$. Therefore, the above equation together with the commutative diagram

$$\begin{array}{ccc} \mathrm{Sel}_{\mathcal{F}^{n\ell}}(\mathbb{Q}, E[p^m]) & \xrightarrow{\partial_\ell} & \mathcal{H}^2_\ell(\mathbb{Q}) \simeq \mathbb{Z}/p^m \\ \downarrow & & \downarrow N_n \\ \mathrm{Sel}_{\mathcal{F}^{n\ell}}(\mathbb{Q}(n), E[p^m]) & \xrightarrow{\partial_\ell} & \mathcal{H}^2_\ell(\mathbb{Q}(n)) \simeq \mathbb{Z}/p^m[\mathcal{G}_n] \end{array}$$

shows that the image of $\kappa^{\pm}_{n,\ell}$ in $\mathcal{H}^2_\ell(\mathbb{Q}(n))$ is $(-1)^{\nu(n)} N_n \delta_n^{(m)} t_{\ell,\mathbb{Q}(n)}$. Since the right vertical arrow which is the multiplication by N_n is injective, this implies the conclusion. □

Remark 4.15. These $\kappa_{n,\ell}$ satisfy interesting 4 properties (see Proposition 2 on page 341 in [15] and Proposition 7.16 in [14]), but we do not expalin them in this paper because we do not use them here.

We also note here that we have a different construction of Kolyvagin systems in [28] and [17].

4.6 Proof of the injectivity theorem

We first prove Theorem 2.1. If E has ordinary reduction at p, this was proved in Corollary 2 on page 342 in [15]. So we consider the case $a_p = 0$.

We use Proposition 5.16 in our previous paper [14], which holds in our setting without changing the proof in [14]. Let $\mathcal{P}^{(m)}(\mathbb{Q}(n))' = \mathcal{P}^{(m)}(\mathbb{Q}(n)_i)$ be the set of primes defined before Proposition 4.10 for $K = \mathbb{Q}(n)$. Let x be any element in $\mathrm{Sel}(\mathbb{Q}, E[p^m])^\vee$. We take $y \in H^1_{\mathcal{F}^{npN}}(\mathbb{Q}, E[p^m])^\vee$ whose image under the natural map is x. Then by Proposition 5.16 in [14] we can take $\ell \in \mathcal{P}^{(m)}(\mathbb{Q}(n))'$ such that $\lambda'_\ell(t_{\ell,\mathbb{Q}}) = y$ where $\lambda'_\ell : \mathcal{H}^2_\ell(\mathbb{Q}) \to H^1_{\mathcal{F}^{npN}}(\mathbb{Q}, E[p^m])^\vee$ is the dual of the natural map $H^1_{\mathcal{F}^{npN}}(\mathbb{Q}, E[p^m]) \to H^1(\mathbb{F}_\ell, E[p^m]) = E(\mathbb{F}_\ell)/p^m$ of étale cohomology groups. Let

$$\lambda_\ell : \mathcal{H}^2_\ell(\mathbb{Q}) \longrightarrow \mathrm{Sel}_{\mathcal{F}^n}(\mathbb{Q}, E[p^m])^\vee$$

denote the dual of the natural map $r^{\mathrm{Sel}}_\ell : \mathrm{Sel}(\mathbb{Q}, E[p^m]) \to E(\mathbb{F}_\ell)/p^m$. Then $\lambda_\ell(t_{\ell,\mathbb{Q}}) = x$. By Lemma 4.8 we have an exact sequence

$$\mathrm{Sel}_{\mathcal{F}^{n\ell}}(\mathbb{Q}, E[p^m]) \overset{\partial_{n\ell}=(\partial_r)}{\longrightarrow} \bigoplus_{r|n\ell} \mathcal{H}^2_r(\mathbb{Q}) \overset{\lambda_{n\ell}=(\lambda_r)}{\longrightarrow} \mathrm{Sel}(\mathbb{Q}, E[p^m])^\vee \qquad (26)$$

where we named the maps $\partial_{n\ell}$ and $\lambda_{n\ell}$ which consist of the natural maps $\partial_r : \mathrm{Sel}_{\mathcal{F}^{n\ell}}(\mathbb{Q}, E[p^m]) \to \mathcal{H}^2_r(\mathbb{Q})$ and $\lambda_r : \mathcal{H}^2_r(\mathbb{Q}) \to \mathrm{Sel}(\mathbb{Q}, E[p^m])^\vee$ for $r \mid n$, respectively. Since $\kappa^{\pm}_{n,\ell}$ satisfies $\partial_\ell(\kappa^{\pm}_{n,\ell}) = (-1)^{\nu(n)}\delta^{(m)}_n t_{\ell,\mathbb{Q}}$ by Proposition 4.14, the above exact sequence gives

$$(-1)^{\nu(n)}\delta^{(m)}_n \lambda_\ell(t_{\ell,\mathbb{Q}}) + \sum_{r|n} \lambda_r(\partial_\ell(\kappa^{\pm}_{n,\ell})) = 0.$$

Suppose that $\delta^{(m)}_n \equiv \delta_n \not\equiv 0 \pmod{p}$. Then $\delta^{(m)}_n$ is a unit. The above equation and $\lambda_\ell(t_{\ell,\mathbb{Q}}) = x$ imply

$$x = (-1)^{\nu(n)+1}(\delta^{(m)}_n)^{-1} \sum_{r|n} \lambda_r(\partial_\ell(\kappa^{\pm}_{n,\ell})).$$

This shows that

$$\lambda_n = (\lambda_r) : \bigoplus_{r|n} \mathcal{H}^2_r(\mathbb{Q}) \longrightarrow \mathrm{Sel}(\mathbb{Q}, E[p^m])^\vee$$

is surjective. Taking the dual, we obtain that $r^{\mathrm{Sel}}_n : \mathrm{Sel}(\mathbb{Q}, E[p^m]) \to \bigoplus_{r|n} E(\mathbb{F}_r)/p^m$ is injective.

Remark 4.16. We can show that $\kappa_{n,\ell}$ is in $\mathrm{Sel}_{\mathcal{F}(n)^\ell}(\mathbb{Q}, E[p^m])$. Using this fact, we can prove the injectivity of the map

$$\mathrm{Sel}_{\mathcal{F}^n}(\mathbb{Q}, E[p^m]) \longrightarrow \bigoplus_{r|n} E(\mathbb{F}_r)/p^m = \bigoplus_{r|n} H^1(\mathbb{Q}_\ell, E[p^m])/H^1_{tr}(\mathbb{Q}_\ell, E[p^m]),$$

which is slightly more general than Theorem 2.1.

References

[1] Pierrette Cassou-Noguès, Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques, Invent. math. **51** (1979), 29-59.

[2] P. Deligne and K. Ribet, Values of abelian L-functions at negative integers over totally real fields, Invent. math. **59** (1980), 227-286.

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

[4] T. Kataoka, Equivariant Iwasawa theory for elliptic curves, Mathematische Zeitschrift **298** (2021), 1653-1725.

[5] T. Kataoka, Stark systems and equivariant main conjectures, Osaka Journal of Mathematics **59** (2) (2020), 417-452.

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

[7] Chan-Ho Kim, Myougil Kim and Hae-Sang Sun, On the indivisibility of derived Kato's Euler systems and the main conjecture for modular forms, Selecta Math. **26** (2020), Article number: 31.

[8] Chan-Ho Kim, The structure of Selmer groups and the Iwasawa main conjecture for elliptic curves, preprint, arXiv:2203.12159.

[9] T. Kitajima and R. Otsuki, On the plus and the minus Selmer groups for elliptic curves at supersingular primes, Tokyo J. Math. **41** (2018), 273-303.

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

[11] M. Kurihara, Iwasawa theory and Fitting ideals, J. reine angew. Math. **561** (2003), 39-86.

[12] M. Kurihara, On the structure of ideal class groups of CM-fields, Documenta Mathematica, Extra Volume Kato (2003), 539-563.

[13] M. Kurihara, Refined Iwasawa theory and Kolyvagin systems of Gauss sum type, Proceedings of the London Mathematical Society **104** (2012), 728-769.

[14] M. Kurihara, Refined Iwasawa theory for p-adic representations and the structure of Selmer groups, Münster Journal of Mathematics **7** (2014), 149-223.

[15] M. Kurihara, The structure of Selmer groups of elliptic curves and modular symbols, *Iwasawa theory 2012*, Contributions in Math. and Comput.Sci. **7**, (2014), 317-356.

[16] M. Kurihara and R. Pollack, Two p-adic L-functions and rational points on elliptic curves with supersingular reduction, in *L-functions and Galois representations*, edited by D.Burns, K. Buzzard, and J. Nekovár, London Math. Soc. Lecture Note Ser. **320** (2007), 300-332.

[17] M. Kurihara and R. Sakamoto, Euler and Kolyvagin systems of rank 0 and the structure of Selmer groups, in preparation.

[18] B. Mazur and K. Rubin, *Kolyvagin systems*, Memoirs of the AMS Vol. **168**, Number **799** (2004).

[19] B. Mazur and J. Tate, Refined conjectures of the "Birch and Swinnerton-Dyer type", Duke Math. J. **54** (1987), 711-750.

[20] J. S. Milne, *Arithmetic duality theorems*, Perspective in Math., Academic Press (1986).

[21] D. G. Northcott, *Finite free resolutions*, Cambridge Univ. Press (1976).

[22] R. Pollack, On the p-adic L-functions of a modular form at a supersingular prime, Duke Math. **118** (2003), 523-558.

[23] D. Prasad and S. Shekhar, Relating Tate-Shafarevich group of an elliptic curve with class group, Pacific Journal of Mathematics **312** (1) (2021), 203-218.

[24] K. Rubin, The main conjecture, Appendix to *Cyclotomic fields I and II* by S. Lang, Graduate Texts in Math. **121**, Springer-Verlag (1990), 397-419.

[25] K. Rubin, Kolyvagin's system of Gauss sums, *Arithmetic Algebraic Geometry*, G. van der Geer et al eds, Progress in Math 89 (1991) 309-324.

[26] K. Rubin, *Euler systems*, Annals of Math. Studies 147, Princeton Univ. Press (2000).

[27] R. Sakamoto, On the theory of Kolyvagin systems of rank 0, Journal de Théorie des Nombres de Bordeaux **33** (2021), 1077-1102.

[28] R. Sakamoto, p-Selmer Group and Modular Symbols, Doc. Math. **27** (2022), 1891-1922.

[29] C. Skinner and E. Urban, The Iwasawa Main Conjectures for GL_2, Invent. math. **195** (2014), 1-277.

[30] G. Stevens, Stickelberger elements and modular parametrizations of elliptic curves, Invent. math. **98** (1989), 75-106.

[31] X. Wan, Iwasawa main conjecture for supersingular elliptic curves and BSD conjecture, preprint (2019), arXiv: 1411.6352v7.