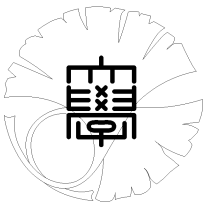
UTMS 2002–4 February 4, 2002

Iwasawa theory for elliptic curves at supersingular primes

by

Shin-ichi KOBAYASHI



UNIVERSITY OF TOKYO

GRADUATE SCHOOL OF MATHEMATICAL SCIENCES

KOMABA, TOKYO, JAPAN

Iwasawa theory for elliptic curves at supersingular primes

Shin-ichi Kobayashi

Author address:

Graduate School of Mathematical Sciences, University of Tokyo, Komaba 3-8-1, Tokyo, 153-8914 Japan

E-mail address: koba@ms406ss5.ms.u-tokyo.ac.jp

Contents

CHAPTER 1

Introduction

As stated in the introduction of Kato [**8**], one of the most fascinating subjects in number theory is the study of mysterious relations between zeta functions and arithmetically important groups. The origin of such a study is the class number formula in the 19-th century. The Birch and Swinnerton-Dyer conjecture is also such a kind of study.

In the study of the subject, p-adic approaches, which begin from Kummer's work for cyclotomic fields, are important. In the mid 1950's, around a century after Kummer, Iwasawa found a new point of view to Kummer's work. The point is to investigate not a single cyclotomic field $\mathbb{Q}(\zeta_{p^n})$ but a family of cyclotomic fields $\mathbb{Q}(\zeta_{p^n})$, $n = 1, 2, \ldots$. Then the family of the p-primary parts of the ideal class groups of $\mathbb{Q}(\zeta_{p^n})$, $n = 1, 2, ..$ is related with the Kubota-Leopoldt p-adic L-function, which is a p-adic function interpolating special values of the Riemann zeta function.

In 1970's, Mazur showed that Iwasawa's point of view is also useful in the study of the arithmetic of elliptic curves. At present, for a good ordinary prime p, we have a completely satisfactory framework for Iwasawa theory for elliptic curves. In particular, the cyclotomic family of the Selmer groups, which are very important arithmetic groups containing the Mordell-Weil groups, is related with the Mazur and Swinnerton-Dyer p-adic L function interpolating special values of the Hasse-Weil L-function.

For a good supersingular p, the situation is different. Iwasawa's point of view is also important but a direct analogy with the cyclotomic field or the good ordinary case does not work well. The reason is that the cyclotomic family of the Selmer groups and the p-adic L-function are too big compared with the Iwasawa algebra Λ. Kato and Perrin-Riou proposed a candidate for Iwasawa theory for elliptic curves at a good supersingular p, and generalized it to Iwasawa theory for motives. However, their framework remains still very conjectural except for elliptic curves or modular forms. Even for elliptic curves, in spite of very significant work by Kato, it is not as satisfactory as in the good ordinary case.

The aim of this paper is to give another formulation of Iwasawa theory for elliptic curves at a good supersingular p. Our formulation goes along with the cyclotomic field case and the good ordinary case in the following sense. Firstly, we define new Selmer groups which are smaller than the usual Selmer groups

(Λ-cotorsion) but have enough information. Secondly the cyclotomic family of our Selmer groups is related with Pollack's p-adic L-function, which lives in the Iwasawa algebra Λ but has enough information as much as the usual p-adic L-function.

1. Main results

We outline main results of this paper. We first fix notations. Let p be an odd prime number. Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension, which is the unique subfield of $\mathbb{Q}(\zeta_{p^\infty})$ whose Galois group $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_p$. We fix a topological generator γ of Γ, so that $\mathbb{Z}_p[[\Gamma]]$ is isomorphic to $\mathbb{Z}_p[[X]]$ by $\gamma \mapsto 1+X$. Let $\mathbb{Q}_n$ be the subextension of $\mathbb{Q}_\infty$ such that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$. For a place v of $\mathbb{Q}_\infty$, we denote by $\mathbb{Q}_{n,v}$ the completion of $\mathbb{Q}_n$ at v.

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction at p. We assume that $a_p := 1 + p - \sharp\widetilde{E}(\mathbb{F}_p) = 0$. If $p \geq 5$, this assumption is equivalent to that E has supersingular reduction at p. We define subgroups of $E(\mathbb{Q}_{n,v})$ by

$$E^+(\mathbb{Q}_{n,v}) = \{P \in E(\mathbb{Q}_{n,v}) \mid \mathrm{Tr}_{n/m}P \in E(\mathbb{Q}_{m-1,v}) \text{ for even } m \leq n\},$$

$$E^-(\mathbb{Q}_{n,v}) = \{P \in E(\mathbb{Q}_{n,v}) \mid \mathrm{Tr}_{n/m}P \in E(\mathbb{Q}_{m-1,v}) \text{ for odd } m \leq n\}.$$

Here $\mathrm{Tr}_{n/m} : E(\mathbb{Q}_{n,v}) \to E(\mathbb{Q}_{m,v})$ is the map induced by the trace of $\mathbb{Q}_{n,v}/\mathbb{Q}_{m,v}$.

Definition 1.1.1 (Definition 5.1.3). *We define the plus (minus) Selmer group by*

$$\mathrm{Sel}^\pm(E/\mathbb{Q}_n) := \mathrm{Ker}\left(H^1(\mathbb{Q}_n, E[p^\infty]) \longrightarrow \prod_v \frac{H^1(\mathbb{Q}_{n,v}, E[p^\infty])}{E^\pm(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)$$

where v ranges over all places of K and the map is induced by the restrictions of the Galois cohomology groups.

We remark that the above local condition is essentially considered in Perrin-Riou [**16**] and Knospe [**9**]. By the restriction maps, the plus (minus) Selmer groups make an inductive system for n. We put $\mathrm{Sel}^\pm(E/\mathbb{Q}_\infty) := \varinjlim_n \mathrm{Sel}^\pm(E/\mathbb{Q}_n)$. We denote the Pontryagin dual by $^\vee$. Then $\mathrm{Sel}^\pm(E/\mathbb{Q}_\infty)^\vee$ is a $\mathbb{Z}_p[[\Gamma]]$-module by the natural Galois action.

Theorem 1.1.2 (Theorem 5.2.6). *Suppose $a_p = 0$. Then the Pontryagin dual of the plus (minus) Selmer group $\mathrm{Sel}^\pm(E/\mathbb{Q}_\infty)^\vee$ is $\mathbb{Z}_p[[\Gamma]]$-torsion.*

Here we recall Pollack's p-adic L-function. Let α and $\overline{\alpha}$ be the roots of the p-Euler factor $X^2 - a_pX + p = X^2 + p = 0$. Then there exist two p-adic L-functions $\mathscr{L}(E, \alpha, X)$ and $\mathscr{L}(E, \overline{\alpha}, X)$ which interpolate special values of the Hasse-Weil L-function of E (cf. Chapter 2, Section 3). The crucial difference between the good ordinary case and the supersingular case is that the p-adic

L-functions in the supersingular case are no longer elements of $\mathbb{Z}_p[[X]] \otimes \overline{\mathbb{Q}_p}$. However, Pollack showed that there exist two power series $\mathscr{L}_p^+(E,X)$ and $\mathscr{L}_p^-(E,X)$ in $\mathbb{Z}_p[[X]]$, and the p-adic L-functions are described as

$$\mathscr{L}_p(E,\alpha,X) = \mathscr{L}_p^+(E,X)\,\Phi^+(X) \,+\, \mathscr{L}_p^-(E,X)\,\Phi^-(X)\,\alpha,$$
$$\mathscr{L}_p(E,\overline{\alpha},X) = \mathscr{L}_p^+(E,X)\,\Phi^+(X) \,+\, \mathscr{L}_p^-(E,X)\,\Phi^-(X)\,\overline{\alpha}$$

where $\Phi^{\pm}(X) \in \mathbb{Q}_p[[X]]$ are defined by taking products of cyclotomic polynomials (cf. Chapter 3).

Since Pollack's p-adic L-functions $\mathscr{L}_p^{\pm}(E,X)$ are in $\mathbb{Z}_p[[X]]$, their λ- and μ-invariants are defined, and these invariants play important roles as in the good ordinary case. (e.g. the Iwasawa formula for the Tate-Shafarevich group.)

We formulate main conjecture in the case $a_p = 0$ as follows. (cf. Section 3 of Chapter 5.)

Conjecture (Plus main conjecture). *The characteristic ideal of the Pontryagin dual of the plus Selmer group is generated by Pollack's plus p-adic L-function*:

$$\mathrm{Char}\,(\,\mathrm{Sel}^+(E/\mathbb{Q}_\infty)^\vee\,) \;=\; (\,\mathscr{L}_p^+(E,X)\,).$$

Conjecture (Minus main conjecture). *The characteristic ideal of the Pontryagin dual of the minus Selmer group is generated by Pollack's minus p-adic L-function*:

$$\mathrm{Char}\,(\,\mathrm{Sel}^-(E/\mathbb{Q}_\infty)^\vee\,) \;=\; (\,\mathscr{L}_p^-(E,X)\,).$$

We recall Kato's main conjecture (cf. Chapter 5, Section 3). In the cyclotomic field case, there are two types of formulations of the Iwasawa main conjecture. In one formulation, the p-adic L-function is used and in the other formulation, the cyclotomic units are used instead of the p-adic L-function. By using his zeta elements instead of the p-adic L-function, Kato generalized the latter type of formulation to Iwasawa theory for elliptic curves. The relations between Kato's main conjecture and our main conjectures are

Theorem 1.1.3 (Theorem 5.3.1). *The three conjectures, Kato's main conjecture, the plus main conjecture and the minus main conjecture are equivalent.*

By using Kato's Euler system, we can prove a half of our main conjectures.

Theorem 1.1.4 (Theorem 5.3.2). *Suppose E has no complex multiplication, then for almost all prime p, we have*

$$\mathrm{Char}\,(\,\mathrm{Sel}^+(E/\mathbb{Q}_\infty)^\vee\,) \;\supseteq\; (\,\mathscr{L}_p^+(E,X)\,),$$
$$\mathrm{Char}\,(\,\mathrm{Sel}^-(E/\mathbb{Q}_\infty)^\vee\,) \;\supseteq\; (\,\mathscr{L}_p^-(E,X)\,).$$

2. The plus (minus) Perrin-Riou map

The key of the proofs of main theorems in this paper is a construction of a new Perrin-Riou map.

We first fix notations. Let K_n be $\mathbb{Q}(\zeta_{p^n})$ and let k_n be $\mathbb{Q}_p(\zeta_{p^n})$. We put $\mathcal{G}_n = \mathrm{Gal}(K_n/\mathbb{Q})$ and $\mathcal{G}_\infty = \varprojlim \mathcal{G}_n = \mathrm{Gal}(K_\infty/\mathbb{Q})$ where $K_\infty = \cup_n K_n$. We also put $\Lambda = \mathbb{Z}_p[[\mathcal{G}_\infty]]$ and $\Lambda_n = \mathbb{Z}_p[[\mathcal{G}_n]]$.

Let T be the p-adic Tate module of E. We introduce several morphisms

$$\mathbf{H}^1_{\mathrm{Iw}}(T) \longrightarrow \Lambda,$$

any of which we call Perrin-Riou map. Here $\mathbf{H}^1_{\mathrm{Iw}}(T) = \varprojlim_n H^1(k_n, T)$. We construct a Perrin-Riou map called the plus (minus) Perrin-Riou map which sends Kato's zeta element to Pollack's plus (minus) p-adic L-function. Perrin-Riou constructed a morphism $\mathbf{H}^1_{\mathrm{Iw}}(T) \to \mathscr{H}_\infty$ such that the image of Kato's zeta element is the usual p-adic L-function. Here $\mathscr{H}_\infty$ is a certain subring of $\mathbb{Q}_p[[X]]$ (see, Chapter 2, Section 3).

Perrin-Riou [**18**] actually constructed a morphism interpolating Bloch-Kato exponential maps, and the morphism mentioned above is obtained by taking the dual of of her morphism (cf. Kato [**8**], Remark 16.5). This construction is sophisticated, however, we propose the following simple mind to construct a Perrin-Riou map. (This construction is inspired by studying the P_n-pairing in Kurihara [**10**]. I also learned the idea to use Honda's theory from Kurihara [**10**].)

Suppose that we have a local norm compatible system $(\mathrm{c}_n)_{n=1,2,..}$, $\mathrm{c}_n \in H^1(k_n, T)$. Then we consider a morphism

$$H^1(k_n, T) \longrightarrow \Lambda_n, \quad z \longmapsto \sum_{\sigma \in \mathcal{G}_n} (\, \mathrm{c}_n^\sigma,\, z\,)\, \sigma. \tag{1.2.1}$$

Here $(\ ,\ )$ is the Tate pairing. By the norm compatibility of c_n, we can take the limit of the above morphisms. Then we get a Perrin-Riou map $\mathbf{H}^1_{\mathrm{Iw}}(T) \to \Lambda$. Hence, a key of constructions of good Perrin-Riou maps is to find good local norm compatible systems $(\mathrm{c}_n)_n$. We do it by using Honda's theory of formal groups.

By Honda's theory, we have a canonical formal group $\mathscr{F}$ and a canonical isomorphism $\mathscr{F}$ to the formal group of E given by an Artin-Hasse type power series. Then a good c_n is given by almost the image of the cyclotomic unit $\zeta_{p^n} - 1 \in \mathscr{F}(\mathfrak{m}_n)$ by the Artin-Hasse type canonical isomorphism followed by the Kummer map. (Here $\mathfrak{m}_n$ is the maximal ideal of O_{k_n}.)

$$\begin{array}{ccccc} \mathscr{F}(\mathfrak{m}_n) & \xrightarrow{\text{A-H}} & \hat{E}(\mathfrak{m}_n) & \xrightarrow{\text{Kum}} & H^1(k_n, T) \\ \cup & & & & \cup \\ \text{“}\zeta_{p^n} - 1\text{”} & & \longmapsto & & \mathrm{c}_n \end{array}$$

Actually, in the good ordinary case, the cyclotomic units produce a kind of norm compatible system $(\mathrm{c}_n)_n$ such that

$$\mathrm{Tr}_{n+1/n}\,(\mathrm{c}_{n+1}) \;=\; \alpha\,\mathrm{c}_n$$

where α is a unit root of $X^2 - a_pX + p = 0$. After an elementary modification, we have an exactly norm compatible system. This norm compatible system produces Perrin-Riou's map or so called the Coleman map. In the supersingular case, the cyclotomic units produce a system $(\mathrm{c}_n)_n$ satisfying

$$\mathrm{Tr}_{n+1/n}\,(\mathrm{c}_{n+1}) - a_p\,\mathrm{c}_n + \mathrm{c}_{n-1} = 0. \tag{1.2.2}$$

Then from the above relation, we have

$$\mathrm{Tr}_{n/n-1}(\,\mathrm{Tr}_{n+1/n}\,\mathrm{c}_{n+1} - \beta\,\mathrm{c}_n\,) \;=\; \alpha\,(\,\mathrm{Tr}_{n/n-1}\,\mathrm{c}_n - \beta\,\mathrm{c}_{n-1}\,)$$

where α and β are the roots of $X^2 - a_pX + p = 0$. Hence we have an exactly norm compatible system as in the good ordinary case. This norm compatible system produces the morphism constructed by Perrin-Riou. In this case, since α cannot be taken as a unit, we have to admit denominators to get the exactly norm compatible system, and the image of the morphism is in $\mathscr{H}_\infty$ instead of Λ.

If $a_p = 0$, the relation (1.2.2) becomes

$$\mathrm{Tr}_{n+1/n}\,(\mathrm{c}_{n+1}) \;=\; -\,\mathrm{c}_{n-1}.$$

Hence, according to the parity of n, we have two another kind of norm compatible systems. Then, for these norm compatible systems, we investigate the images of the morphisms (1.2.1). It turns out that the images are generated by products of cyclotomic polynomials. Eliminating these products of cyclotomic polynomials, we get our plus (minus) Perrin-Riou maps. We remark that the subgroup $E^{\pm}(k_n)$, which is used to define the plus (minus) Selmer group, is generated by the image of $(\mathrm{c}_n^{\sigma})_{\sigma\in\mathcal{G}_n}$, and the kernel of our Perrin-Riou map is the exact annihilator of $E^{\pm}(k_n)$ with respect to the Tate pairing.

Hence, in either case, we may say that p-adic L-functions are obtained by the twisted Tate pairing (1.2.1) of cyclotomic units and Kato's zeta elements.

Perrin-Riou [**16**] also gave canonical systems satisfying the relation (1.2.2) by using the theory of norm fields by Fontaine and Wintenberger. The above constructions of Perrin-Riou maps answer why such norm compatible systems are important.

We finally remark that since the image of Kato's zeta element by (1.2.1) is related with the modular element, the relation between the modular elements in Mazur-Tate [**13**, p. 717, (4)], which is shown by using the action of Hecke operators, is also explained by the relation (1.2.2).

Acknowledgments. This paper is based on the author's thesis. It is a pleasure to thank his thesis advisor, Takeshi Saito, who read the manuscript carefully and pointed out mathematical mistakes. He would like to thank Robert Pollack for showing me the paper [**21**]. He is grateful to Kazuya Kato for showing me the great paper [**8**]. He expresses his sincere gratitude to Masato Kurihara. The author could construct the plus (minus) Perrin-Riou map by studying his P_n-pairing in [**10**]. He also learned the idea to use Honda's theory from [**10**].

CHAPTER 2

A review of Iwasawa theory for elliptic curves

We recall basic definitions and facts on Iwasawa theory, and review Iwasawa theory for elliptic curves, especially at good ordinary primes. Then we see differences between the good ordinary case and the good supersingular case, and point out difficulties to formulate Iwasawa theory at supersingular primes. The basic references of this chapter are Washington [**29**] for basic facts on Iwasawa theory, Greenberg [**3**] for Iwasawa theory for elliptic curves, and Mazur-Tate-Teitelbaum [**14**] for p-adic L-functions. See also Kato [**8**] and Greenberg-Vatsal [**4**].

1. Basic notations

Let p be an odd prime number. We fix a generator (ζ_{p^n}) of $\mathbb{Z}_p(1)$, namely ζ_{p^n} is a primitive p^n-th root of unity, and $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ and $\zeta_{p^0} = 1$. For an integer $n \geq 0$, let $K_n = \mathbb{Q}(\zeta_{p^n})$ and $k_n = \mathbb{Q}_p(\zeta_{p^n})$. We put

$$\begin{aligned} &\mathcal{G}_n = \mathrm{Gal}(K_n/\mathbb{Q}) \quad \text{for } n \geq 0, \\ &\mathcal{G}_\infty = \varprojlim \mathcal{G}_n = \mathrm{Gal}(K_\infty/\mathbb{Q}) \text{ where } K_\infty = \cup_n K_n. \end{aligned}$$

Then the cyclotomic character gives an isomorphism

$$\kappa : \mathcal{G}_\infty \longrightarrow \mathbb{Z}_p^\times.$$

We put $\Lambda = \mathbb{Z}_p[[\mathcal{G}_\infty]]$ and $\Lambda_n = \mathbb{Z}_p[[\mathcal{G}_n]]$. We recall the structure of Λ. Let Δ be the torsion part of $\mathcal{G}_\infty$, and let $\mathcal{G}_\infty^1 = \{\sigma \in \mathcal{G}_\infty \,|\, \kappa(\sigma) \equiv 1 \mod p\}$. Then

$$\mathcal{G}_\infty = \mathcal{G}_\infty^1 \times \Delta, \ \mathcal{G}_\infty^1 \cong \mathbb{Z}_p \text{ and } \Delta \cong \mathbb{Z}/(p-1)\mathbb{Z}.$$

We fix a topological generator γ of $\mathcal{G}_\infty^1 \cong \mathbb{Z}_p$. Then

$$\begin{aligned} \Lambda &= \mathbb{Z}_p[[\mathcal{G}_\infty]] = \mathbb{Z}_p[[\mathcal{G}_\infty^1 \times \Delta]] = \mathbb{Z}_p[\Delta][[\mathcal{G}_\infty^1]] \\ &= \varprojlim_n \mathbb{Z}_p[\Delta][\mathcal{G}_n^1] = \varprojlim_n \mathbb{Z}_p[\Delta][X]/((X+1)^{p^n} - 1) = \mathbb{Z}_p[\Delta][[X]], \end{aligned}$$

where $\mathcal{G}_n^1$ is the quotient of $\mathcal{G}_\infty^1$ isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$ and γ is corresponded to $1+X$. We have $\mathcal{G}_n = \mathcal{G}_{n-1}^1 \times \Delta$, and denote the image of γ in $\mathcal{G}_n^1$ by γ_n.

Let $\mathbb{C}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$. Throughout the paper, we fix an embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}_p$.

2. The Selmer groups

We recall the definition of the Selmer group. Let F be a field (e.g. a number field or a local field) and $\overline{F}$ the algebraic closure of F. Let E be an elliptic curve over F. We consider the Kummer sequence

$$0 \to E[p^n] \to E(\overline{F}) \xrightarrow{p^n} E(\overline{F}) \to 0.$$

By taking the $\mathrm{Gal}(\overline{F}/F)$-fixed part, the connecting morphism induces

$$E(F) \otimes \frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p \hookrightarrow H^1(F, E[p^n]).$$

Taking the direct limit for n, we have $E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(F, E[p^\infty])$.

Here we take F as a number field K, then by the above inclusion, the Mordell-Weil group $E(K)$ is regarded as a subgroup of the Galois cohomology group $H^1(K, E[p^\infty])$, which is easier to handle. We would like to characterize the subgroup in the Galois cohomology group coming from the Mordell-Weil group by a local-global principle. Namely, we consider the subgroup of $H^1(K, E[p^\infty])$ consisting the elements which are locally rational points of $E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(K_v, E[p^\infty])$.

Definition 2.2.1. *We define the (p-primary) Selmer group by*

$$\mathrm{Sel}(E/K) := \mathrm{Ker}\left(H^1(K, E[p^\infty]) \longrightarrow \prod_v \frac{H^1(K_v, E[p^\infty])}{E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

where v ranges over all places of K and the map is induced by the restrictions of the Galois cohomology groups.

The Selmer group contains the Mordell-Weil group, and the difference between these is measured by the (p-primary) Tate-Shafarevich group

$$Ш(E/K) := \mathrm{Ker}\left(\frac{H^1(K, E[p^\infty])}{E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \longrightarrow \prod_v \frac{H^1(K_v, E[p^\infty])}{E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right).$$

The Tate-Shafarevich group is conjectured to be finite, however, this group is very hard to analyze.

In Iwasawa theory for elliptic curves, we consider the cyclotomic family of the Selmer groups $\mathrm{Sel}(E/K_n)$, $n = 1, 2, 3, \ldots$. The Selmer groups and the Tate-Shafarevich groups play analogous roles with ideal class groups in the classical Iwasawa theory.

Let $\mathrm{Sel}(E/K_\infty) := \varinjlim_n \mathrm{Sel}(E/K_n)$. Let $\mathscr{X}(E/K_n)$ and $\mathscr{X}(E/K_\infty)$ be the Pontryagin dual of $\mathrm{Sel}(E/K_n)$ and $\mathrm{Sel}(E/K_\infty)$:

$$\mathscr{X}(E/K_n) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}(E/K_n), \mathbb{Q}_p/\mathbb{Z}_p),$$
$$\mathscr{X}(E/K_\infty) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p).$$

Since $\mathrm{Sel}(E/K_n)$ has the natural Galois action of $\mathcal{G}_n$ induced by the Galois action on cohomology groups, one can consider $\mathscr{X}(E/K_n)$ as $\mathbb{Z}_p[\mathcal{G}_n]$-module and $\mathscr{X}(E/K_\infty)$ as Λ-module. It is known that $\mathscr{X}(E/K_\infty)$ is finitely generated Λ-module. Here, we recall properties of finitely generated Λ-modules.

Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character. For a $\mathbb{Z}_p[\Delta]$-module M, we denote the η-component of M by M^η, which is the largest submodule on which Δ acts by η. If we put

$$\epsilon_\eta = \frac{1}{\sharp\Delta} \sum_{\tau\in\Delta} \eta^{-1}(\tau)\, \tau,$$

M^η is given by $\epsilon_\eta M$.

The Iwasawa algebra Λ is the product $\Pi_\eta \Lambda^\eta$, and Λ^η is isomorphic to $\mathbb{Z}_p[[X]]$. Let $R = \mathbb{Z}_p[[X]]$ and we recall properties of finitely generated R-modules. See, Washington [**29**], Section 13.2. (Usually, R is denoted by Λ.)

We first define the λ- and μ-invariant of an element of R.

THEOREM 2.2.2 (The p-adic Weierstraß preparation theorem). *Let f be a non-zero element of $R = \mathbb{Z}_p[[X]]$. Then f is uniquely written as*

$$f(X) = p^\mu \left(X^\lambda + pa_1 X^{\lambda-1} + \cdots + pa_\lambda\right) u(X)$$

where λ and μ are non-negative integers and $u(X)$ is a unit of R.

The above λ and μ are called the λ- and μ-invariants of f and denoted by $\lambda(f)$ and $\mu(f)$.

THEOREM 2.2.3 (The structure theorem of R-modules). *Let M be a finitely generated R-module. Then, there exists a morphism of R-modules*

$$M \to R^r \oplus R/f_1^{n_1} \oplus \cdots \oplus R/f_k^{n_k}$$

whose kernel and cokernel is finite. Here, f_i's are irreducible elements of R and n_j's are positive integers. The non-negative integer r and the ideals $(f_i^{n_i})$ are uniquely determined.

We call r the R-rank of M. If $r = 0$, that is, M is a torsion R-module, then the characteristic ideal of M is defined by

$$\mathrm{Char}(M) = (f)$$

where $f = \Pi_{i=1}^k f_i^{n_i}$ and (f) is the ideal of R generated by f. The λ- and μ-invariants of M are defined by

$$\lambda(M) = \lambda(f), \quad \mu(M) = \mu(f).$$

As we see in Section 4 of this chapter, if E has good ordinary reduction at p, then $\mathscr{X}(E/K_\infty)$ is Λ-torsion, and the characteristic ideal is conjectured to be generated by the p-adic L-function of E.

3. The p-adic L-function of elliptic curves

The Kubota-Leopoldt p-adic L-function is constructed by interpolating the special values of the Riemann zeta function at negative integers. For elliptic curves, since the Hasse-Weil L-function has the critical values only at $s = 1$, the p-adic L-functions of elliptic curves are constructed by interpolating the special value at $s = 1$ of the p-adically twisted Hasse-Weil L-function. The p-adic L-functions are in general no longer elements of $\Lambda \otimes \overline{\mathbb{Q}_p}$, and live in a bigger ring $\mathscr{H}_\infty \subset \overline{\mathbb{Q}_p}[[X]]$. We recall $\mathscr{H}_\infty$ following Kato [**8**], Chapter IV, Section 16.

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction at p. Let α be a root of the p-Euler factor $X^2 - a_p X + p$ such that $\mathrm{ord}_p(\alpha) < 1$. (In the good ordinary case, there is only one α satisfying the above relation and in the good supersingular case, any root α satisfies.) Let $L = \mathbb{Q}_p(\alpha)$. We regard $\Lambda \otimes O_L = O_L[\Delta][[X]]$ (cf. Section 1). For an integer $h \geq 1$, let

$$\mathscr{H}_{h,L} = \{ \sum_{n \geq 0,\, \sigma \in \Delta} a_{n,\sigma}\, \sigma\, X^n \in L[\Delta][[X]] \ \mid \ \lim_{n \to \infty} \frac{|a_{n,\sigma}|_p}{n^h} = 0 \ \text{ for all } \sigma \in \Delta \}$$

where $|\ |_p$ denotes the multiplicative valuation of L normalized by $|p|_p = \frac{1}{p}$. Define

$$\mathscr{H}_{\infty,L} = \cup_h \, \mathscr{H}_{h,L}.$$

Then $\mathscr{H}_{\infty,L}$ is a ring.

THEOREM 2.3.1 (Amice-Vélu [**1**], Vishik [**28**]). *We fix real and imaginary Néron periods $\Omega_E^{\pm}$. Then there exists a unique element*

$$L_p(E, \alpha, X) \ \in \ \mathscr{H}_{1,L}$$

having the following interpolation properties.

i) *For an integer $n \geq 1$, let $\psi : \mathcal{G}_n \to \overline{\mathbb{Q}_p}^{\times}$ be a Dirichlet character of conductor p^n. We put $\delta = \psi(-1)$ and $\psi(\gamma) = \zeta$. We define the Gauss sum $\tau(\psi)$ as $\sum_{a \in \mathcal{G}_n} \psi(a)\, \zeta_{p^n}^a$ where we regard $\mathcal{G}_n \cong (\mathbb{Z}/p^n\mathbb{Z})^{\times}$.*
   Then

$$L_p(E, \alpha, \zeta - 1) = \frac{p^n}{\tau(\overline{\psi})\, \alpha^n} \, \frac{L(E, \overline{\psi}, 1)}{\Omega_E^{\delta}} \tag{2.3.1}$$

   where $\overline{\psi} = \psi^{-1}$ and the coefficients of $L_p(E, \alpha, X) \in L[\Delta][[X]]$ is evaluated by ψ.

ii) *For the trivial character,*

$$L_p(E, \alpha, 0) = (1 - \alpha^{-1})^2 \, \frac{L(E, 1)}{\Omega_E} \tag{2.3.2}$$

   where the coefficients of $L_p(E, \alpha, X) \in L[\Delta][[X]]$ is evaluated by the trivial character.

We call the power series $L_p(E,\alpha,X)$ the p-adic L-function. (Usually, the function $L_p(E,\alpha,\kappa(\gamma)^{s-1}-1)$ for variable $s \in \mathbb{Z}_p$ is called the p-adic L-function.) The p-adic L-function $L_p(E,\alpha,X)$ is not identically zero by Rohrlich's theorem [**23**], which assures that the value $L(E,\psi,1)$ is not zero for almost all ψ. The p-adic L-function has or conjecturally has amazing properties such as the p-adic Birch and Swinnerton-Dyer conjecture. (See, Mazur-Tate-Teitelbaum [**14**].)

Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character. We define $\mathscr{L}_p(E,\alpha,\eta,X) \in L[\Delta][[X]]$ as the function obtained by evaluating the coefficients of $L_p(E,\alpha,X)$ by η. If η is trivial, we simply write $\mathscr{L}_p(E,\alpha,\eta,X)$ by $\mathscr{L}_p(E,\alpha,X)$. Then the p-adic Birch and Swinnerton- Dyer conjecture says that the order of zero of $\mathscr{L}_p(E,\alpha,X)$ at $X=0$ is the rank of the Mordell-Weil group of E.

The p-adic L-function has the following functional equation.

THEOREM 2.3.2. *Let N be the conductor of E, and denote the canonical projection of N by $\mathbb{Z}_p \to 1+2p\mathbb{Z}_p$ by $\langle N\rangle$. We put $c = \log_\gamma\langle N\rangle$, and define the dual p-adic L-function $\mathscr{L}_p^\vee(E,\alpha,\eta,X)$ by $\mathscr{L}_p(E,\alpha,\eta^{-1},\frac{-X}{X+1})$. Then,*

$$\mathscr{L}_p^\vee(E,\alpha,\eta,X) = w_E\ \eta(-N)\ (1+X)^c\ \mathscr{L}_p(E,\alpha,\eta,X)$$

where $w_E = \pm 1$ is the root number of the Hasse-Weil L-function $L(E,s)$.

PROOF. The proof is found in many literatures, but we give it since the proof is simple. It suffices to show that the power series on the both sides of the functional equation have the same interpolation properties. (Since they are in $\mathscr{H}_{1,L}$.) Let $\chi : \mathcal{G}_n \to \mu_{p^\infty}$ be a Dirichlet character of conductor n. By the functional equation of the Hasse-Weil L-function $L(E,\eta\chi,s)$, we have $L(E,\eta\chi,1) = w_E\ \chi(N)\ \tau(\chi)^2\ p^{-n}L(E,\overline{\eta\chi},1)$. (See, Shimura [**26**], Theorem 3.66.) Therefore, by the interpolation property (2.3.1) of the p-adic L-function, we have

$$\mathscr{L}_p^\vee(E,\alpha,\eta,\zeta-1) = w_E\ \eta\chi(-N)\ \mathscr{L}_p(E,\alpha,\eta,\zeta-1)$$

where $\eta\chi(\gamma) = \chi(\gamma) = \zeta$. Since $\chi(-N) = \zeta^c$, we have the functional equation. □

In Greenberg-Vatsal [**4**], the dual p-adic L-function $\mathscr{L}_p^\vee(E,\alpha,\eta,X)$ is denoted by $\mathscr{L}(E,\eta,T)$.

COROLLARY 2.3.3. *Let n be the order of zero of $\mathscr{L}_p(E,\alpha,X)$ at $X=0$. Then $w_E = (-1)^n$.*

PROOF. Compare the leading coefficients of the power series in the both sides of the functional equation. □

Since w_E is conjectured to be the parity of the Mordell-Weil rank of E, the above corollary has an interest in view of the p-adic Birch and Swinnerton-Dyer conjecture.

4. The good ordinary case

In this section, we assume that E has good ordinary reduction at p. We review Iwasawa theory for elliptic curves at good ordinary primes.

4.1. The Selmer group at a good ordinary p.

THEOREM 2.4.1 (Kato-Rohrlich). *Suppose $E/\mathbb{Q}$ has good ordinary reduction at p. Then $\mathrm{Sel}(E/K_\infty)$ is Λ-cotorsion ($\mathscr{X}(E/K_\infty)$ is Λ-torsion).*

Thus, we can define the characteristic ideal and the λ- and μ-invariants of $\mathscr{X}(E/K_\infty)$. We denote the λ- and μ-invariants of the η-part of $\mathscr{X}(E/K_\infty)$ by λ^η and μ^η.

COROLLARY 2.4.2. *For all n, we have*

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}(E/K_n)^\eta \leq \lambda^\eta.$$

In particular, $\mathrm{rank}\, E(K_\infty)^\eta \leq \lambda^\eta$.

THEOREM 2.4.3 (Mazur's control theorem). *Suppose $E/\mathbb{Q}$ has good ordinary reduction at p. Let $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$. Then the natural maps*

$$\mathrm{Sel}(E/K_n) \to \mathrm{Sel}(E/K_\infty)^{\Gamma_n}$$

have finite kernel and cokernel of bounded order as n varies.

This theorem is very important since by this theorem, we can obtain information on $\mathrm{Sel}(E/K_n)$ from information such as λ and μ on $\mathrm{Sel}(E/K_\infty)$.

As a direct application of the above two theorems, we can show Iwasawa formula for the Tate-Shafarevich group.

THEOREM 2.4.4 (Iwasawa formula). *There exist non-negative integers λ, μ and ν such that*

$$\mathrm{ord}_p \sharp Ш(E/K_n)^\eta = \lambda\, n + \mu\, p^n + \nu$$

for all $n \gg 0$. The invariants λ and μ are described explicitly as $\mu = \mu^\eta$ and $\lambda = \lambda^\eta - \mathrm{rank}\, E(K_\infty)^\eta$.

4.2. The p-adic L-function at a good ordinary p.

In the good ordinary case, there is only one allowable choice of α, namely the unit root of $X^2 - a_p X + p = 0$. So we omit the index α from the notation of the p-adic L-function.

THEOREM 2.4.5. *Suppose that E has good ordinary reduction at p, then the p-adic L-function $L_p(E, X)$ is an element of $\Lambda \otimes \mathbb{Q}$. Furthermore, if $E[p]$ is irreducible as $\mathbb{F}_p[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module, then $L_p(E, X) \in \Lambda$.*

PROOF. See, Kato [**8**, Theorem 17.4], Greenberg-Vatsal [**4**, Proposition 3.7] and Stevens [**27**, Theorem 4.6]. □

The p-adic L-function at a good ordinary prime is conjectured to be always an element of Λ. By the above theorem, we can define λ and μ-invariants of $L_p(E, X)$. The λ-invariant of $\mathscr{L}_p(E, \eta, X)$ is the number of the zeros of $\mathscr{L}_p(E, \eta, X)$ in $\mathbb{C}_p$.

COROLLARY 2.4.6. *Let λ be the λ-invariant of $\mathscr{L}_p(E, X)$ and w_E the root number of the Hasse-Weil L-function $L(E, s)$. Then $w_E = (-1)^\lambda$.*

PROOF. Take modulo p of the functional equation (Theorem 2.3.2) after multiplying $p^{-\mu}$, then compare the leading coefficients of the both sides. □

Nekovář [**15**] showed that w_E is the parity of the corank of $\mathrm{Sel}(E/\mathbb{Q}_\infty)$. So the above corollary has an interest in view of the main conjecture.

4.3. Main conjecture. At a good ordinary prime, Mazur conjectured that the characteristic ideal of the Pontryagin dual of $\mathrm{Sel}(E/K_\infty)$ is generated by the p-adic L-function. The Selmer group contains important arithmetic information such as the Mordell-Weil group, on the other hand, the p-adic L-function is related with the Hasse-Weil L-function and can be computed numerically. Hence main conjecture connects two objects of completely different natures and gives fruitful consequences.

CONJECTURE (Main conjecture). *Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character. Then*

$$\mathrm{Char}\,(\mathscr{X}(E/K_\infty)^\eta) \;=\; (\,\mathscr{L}_p(E, \eta, X)\,).$$

THEOREM 2.4.7 (Rubin). *If E has complex multiplication, then the main conjecture holds.*

For non-CM case, Kato proved a half of the main conjecture by constructing an Euler system.

THEOREM 2.4.8 (Kato). *There exists an integer $n \geq 0$ such that*

$$\mathrm{Char}\,(\mathscr{X}(E/K_\infty)^\eta) \;\supseteq\; (\,p^n\,\mathscr{L}_p(E, \eta, X)\,).$$

For almost all prime p, we can take $n = 0$.

PROOF. See Theorem 17.4 in Kato [**8**]. See also Chapter 5, Section 3. □

By the above theorem, the main conjecture is reduced to the equalities of the λ- and μ-invariants of the both sides. A half of the p-adic Birch and Swinnerton-Dyer conjecture is deduced from the above theorem, namely,

COROLLARY 2.4.9. *We have*

$$\mathrm{rank}\, E(\mathbb{Q}) \;\leq\; \mathrm{ord}_{X=0}\, \mathscr{L}_p(E, X).$$

We remark that the main conjecture does not imply the equality in the corollary. For the equality, one needs a kind of semi-simplicity property of the Selmer group.

5. The good supersingular case

In this section, we recall basic facts on Iwasawa theory for elliptic curves at a good supersingular p comparing with the good ordinary case.

5.1. The Selmer group at a good supersingular p.

THEOREM 2.5.1 (Kato-Rohrlich). *Suppose $E/\mathbb{Q}$ has good supersingular reduction at p. Then $\mathrm{Sel}(E/K_\infty)$ has Λ-corank 1 ($\mathscr{X}(E/K_\infty)$ has Λ-rank 1).*

Thus, the Selmer group $\mathrm{Sel}(E/K_\infty)$ is no longer Λ-cotorsion. Hence one cannot define the characteristic ideal and the λ and μ-invariants in the naive way.

The Selmer group $\mathrm{Sel}(E/K_\infty)$ has no longer good properties, however, the Selmer groups $\mathrm{Sel}(E/K_n)$ are considered to have good properties.

THEOREM 2.5.2 (Kato-Rohrlich). *The $\mathbb{Z}_p$-corank of $\mathrm{Sel}(E/K_n)$ is bounded as n varies.*

In Section 5 of Chapter 5, we give a bound of the rank of $E(K_\infty)$ as in Corollary 2.4.2.

The above theorems imply that Mazur's control theorem is no longer true. The Selmer group $\mathrm{Sel}(E/K_\infty)^{\Gamma_n}$ is very large compared with $\mathrm{Sel}(E/K_n)$.

Since in the good supersingular case the definition of the λ- and μ-invariants were not known, the Iwasawa formula for the Tate-Shafarevich group was mysterious before Kurihara [**10**].

THEOREM 2.5.3 (Kurihara [**10**]). *Let $E/\mathbb{Q}$ be a non CM elliptic curve with good supersingular reduction at p. Suppose p does not divide $L(E,1)/\Omega_E$ or the Tamagawa numbers of E. Then for almost all prime p, we have*

$$\mathrm{ord}_p\, \sharp Ш(E/\mathbb{Q}_n) = \begin{cases} p^{n-1} + p^{n-3} + \cdots + p - \frac{n}{2} & \text{for even } n \geq 2 \\ p^{n-1} + p^{n-3} + \cdots + p^2 - \frac{n-1}{2} & \text{for odd } n \geq 3. \end{cases}$$

Here, the field $\mathbb{Q}_n$ is the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

In the good ordinary case, the assumption $p \nmid L(E,1)/\Omega_E$ implies the λ- and μ-invariant are zero. Therefore, the Iwasawa formula (Theorem 2.4.4) is simply that $\sharp Ш(E/\mathbb{Q}_n)$ is constant for $n \gg 0$. On the other hand, in the supersingular case, the order of the Tate-Shafarevich groups grow rapidly large as n varies. Since the Tate-Shafarevich group measures the failure of a

local-global principle, this phenomena shows that in the good supersingular case, the usual local condition defining the Selmer group is not good enough to capture global information as n grows.

In general, Kurihara conjectured that

CONJECTURE (Kurihara). i) *There exist rational numbers* λ, μ, μ', ν, ν' *such that*

$$\mathrm{ord}_p \sharp Ш(E/\mathbb{Q}_n) = \begin{cases} [\lambda n + \mu p^n + \nu] & \textit{for even } n \gg 0 \\ [\lambda n + \mu' p^n + \nu'] & \textit{for odd } n \gg 0 \end{cases}$$

where $[\,\cdot\,]$ *is the Gaussian symbol.*
ii) *In the above, we can take* $\mu = \mu' = p/(p^2-1)$.

The case i) in the above conjecture is announced in [**11**]. Theorem 2.5.3 is written of the above form as $\lambda = -\frac{1}{2}$ and $\nu = 0$.

Recently, Kurihara announced that he obtained an Iwasawa formula, which coincides with the above if the supersingular version of Greenberg's conjecture about the μ-invariant is true (cf. Chapter 3, Section 3). Perrin-Riou defined the λ- and μ-invariants in the good supersingular case and obtained an Iwasawa formula by a method different from Kurihara's ([**20**]).

5.2. The p-adic L-function at a supersingular p. In the supersingular case, the p-adic L-function is no longer an element of $\Lambda \otimes \overline{\mathbb{Q}_p}$, and the λ- and μ-invariants cannot be defined in the same way as in the good ordinary case. In the good ordinary case, the λ-invariant is the number of zeros of the p-adic L-function, however, in the good supersingular case, the p-adic L-function has infinitely many zeros when $a_p = 0$ (cf. Theorem 5.4 in Pollack [**21**]).

Recently, Pollack showed that when $a_p = 0$, the p-adic L-function is described by using certain two power series in Λ. By using the λ- and μ-invariants of these power series, he obtained an Iwasawa formula for the Tate-Shafarevich group analytically. If his μ-invariants are zero and the Birch and Swinnerton-Dyer conjecture for cyclotomic fields are true, his formula is the one conjectured by Kurihara. We recall Pollack's result in the next chapter.

5.3. Main conjecture. In the supersingular case, the Selmer group is not Λ-cotorsion, and the p-adic L-function is not an element of Λ. Therefore, main conjecture can not be formulated in the same way as in the good ordinary case.

However, there is another formulation of main conjecture due to Kato, in which, the p-adic L-function does not appear, and instead, Kato's zeta element is used. A half of Kato's main conjecture is proved as in the good ordinary case. We recall Kato's main conjecture in Section 3 of Chapter 5.

There is also another formulation of main conjecture due to Perrin-Riou [**17**]. Perrin-Riou constructed some function on the arithmetic side using so

called Perrin-Riou map, and her main conjecture asserts that this function is equal to the p-adic L-function. This formulation is known to be equivalent to Kato's formulation.

CHAPTER 3

Pollack's theory of the p-adic L-functions at supersingular primes

We review Pollack's theory of the p-adic L-functions for elliptic curves with $a_p = 0$ ([**21**]). (He constructed his theory for modular forms and for any primes, but we review for elliptic curves and for odd primes.) In the supersingular case, the p-adic L-function is no longer an element of Iwasawa algebra $\Lambda \otimes \overline{\mathbb{Q}_p}$, and we cannot define the λ- and μ-invariant in the same way as in the good ordinary case. Hence the situation looks very different from the good ordinary case. However, Pollack showed that there exist two power series in Iwasawa algebra $\mathbb{Z}_p[[X]]$ and the p-adic L-function is described in terms of these power series. The λ- and μ-invariants of the two power series have important arithmetic information as the λ- and μ-invariant have in the good ordinary case. For example, in analytic point of view, Iwasawa formula for the Tate-Shafarevich group is obtained by using these λ- and μ-invariants.

1. Pollack's p-adic L-function

The story began from an observation by Perrin-Riou in [**16**] on a kind of trivial zeros of the p-adic L-function.

Let p be an odd prime number. We assume that $a_p = 0$, and let α and $\overline{\alpha}$ be the two roots of the Euler p-factor $x^2 + p$. Then there exist two p-adic L-function $\mathscr{L}_p(E, \alpha, X)$ and $\mathscr{L}_p(E, \overline{\alpha}, X)$. Perrin-Riou observed that by the interpolation property (2.3.1) and by $\alpha + \overline{\alpha} = 0$, the function $\mathscr{L}_p(E, \alpha, X) + \mathscr{L}_p(E, \overline{\alpha}, X)$ has trivial zeros at $X = \zeta_{p^{2n}}^i - 1$ for $n \geq 1$ and $i = 1, \ldots, p-1$, and the function $\mathscr{L}_p(E, \alpha, X) - \mathscr{L}_p(E, \overline{\alpha}, X)$ has trivial zeros at $X = \zeta_{p^{2n-1}}^i - 1$ for $n \geq 1$ and $i = 1, \ldots, p-1$.

Then, Pollack compared the sum (subtraction) of two p-adic L functions with the following two functions $\Phi^+(X)$ and $\Phi^-(X)$, which also have trivial zeros at $X = \zeta_{p^{2n}}^i - 1$ and at $X = \zeta_{p^{2n-1}}^i - 1$ respectively.

$$\Phi^+(X) = \frac{1}{p} \prod_{m=1}^{\infty} \frac{\Phi_{2m}(X+1)}{p}, \quad \Phi^-(X) = \frac{1}{p} \prod_{m=1}^{\infty} \frac{\Phi_{2m-1}(X+1)}{p},$$

where $\Phi_n(X) = \sum_{i=0}^{p-1} X^{p^{n-1}i}$ is the p^n-th cyclotomic polynomial.

THEOREM 3.1.1 (Pollack). *Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character. Let $\mathscr{L}_p^+(E,\eta,X)$ and $\mathscr{L}_p^-(E,\eta,X)$ be the power series in $\mathbb{Q}_p[[X]]$ satisfying*

$$\mathscr{L}_p(E,\alpha,\eta,X) = \mathscr{L}_p^+(E,\eta,X)\,\Phi^+(X) + \mathscr{L}_p^-(E,\eta,X)\,\Phi^-(X)\,\alpha.$$

Then $\mathscr{L}_p^+(E,\eta,X)$ and $\mathscr{L}_p^-(E,\eta,X)$ are elements of $\mathbb{Z}_p[[X]]$.

PROOF. See Pollack [**21**] (Theorem 7.1 and Theorem 7.8). Note that $\mathscr{L}_p(E,\alpha,\eta,X)+\mathscr{L}_p(E,\overline{\alpha},\eta,X) = 2\,\mathscr{L}_p^+(E,\eta,X)\,\Phi^+(X)$ and $\mathscr{L}_p(E,\alpha,\eta,X) - \mathscr{L}_p(E,\overline{\alpha},\eta,X) = 2\,\mathscr{L}_p^-(E,\eta,X)\,\Phi^-(X)\,\alpha$. □

We call $\mathscr{L}_p^+(E,\eta,X)$ and $\mathscr{L}_p^-(E,\eta,X)$ Pollack's plus (minus) p-adic L-functions, and if η is trivial, we write simply $\mathscr{L}_p^+(E,X)$ and $\mathscr{L}_p^-(E,X)$.

Let $\chi : \mathcal{G}_n \to \mu_{p^\infty}$ be a character of conductor $p^n \neq 1$. We put $\psi = \eta\chi$ and $\chi(\gamma) = \zeta$. Then Pollack's p-adic L-functions are characterized by the following interpolation properties.

$$\mathscr{L}_p^+(E,\eta,\zeta-1) = (-1)^{\frac{n}{2}}\frac{p^n}{\tau(\overline{\psi})}\prod_{1\le k\le n-1,\,k:\,\text{even}}\Phi_k(\zeta)^{-1}\;\frac{L(E,\overline{\psi},1)}{\Omega_E^\delta} \tag{3.1.1}$$

for even n and

$$\mathscr{L}_p^-(E,\eta,\zeta-1) = (-1)^{\frac{n+1}{2}}\frac{p^n}{\tau(\overline{\psi})}\prod_{1\le k\le n-1,\,k:\,\text{odd}}\Phi_k(\zeta)^{-1}\;\frac{L(E,\overline{\psi},1)}{\Omega_E^\delta} \tag{3.1.2}$$

for odd n. Here $\overline{\psi} = \psi^{-1}$, $\delta = \eta(-1)$ and $\tau(\overline{\psi})$ is the Gauss sum.

For the trivial χ, the interpolation properties are

$$\mathscr{L}_p^+(E,0) = (p-1)\,\frac{L(E,1)}{\Omega_E},\quad \mathscr{L}_p^-(E,0) = 2\,\frac{L(E,1)}{\Omega_E} \tag{3.1.3}$$

and

$$\mathscr{L}_p^+(E,\eta,0) = 0,\quad \mathscr{L}_p^-(E,\eta,0) = -\,\frac{p}{\tau(\overline{\eta})}\,\frac{L(E,\overline{\eta},1)}{\Omega_E^\delta}. \tag{3.1.4}$$

Hence, for a non-trivial η, $\mathscr{L}_p^+(E,\eta,X)$ has a trivial zero at $X=0$. In Chapter 5, we reconstruct Pollack's p-adic L-functions, without mentioning the usual p-adic L-functions, as the power series satisfying the above interpolation properties. They are given as the images of Kato's zeta elements by the plus (minus) Perrin-Riou maps (Theorem 5.2.5). Then Theorem 3.1.1 follows from the construction. The trivial zero phenomena of $\mathscr{L}_p^+(E,\eta,X)$ is also explained in terms of the plus Perrin-Riou map.

2. The functional equations of Pollack's p-adic L-functions

Pollack's p-adic L-functions inherit the functional equation of the usual p-adic L-function.

Let N be the conductor of E, and denote the canonical projection of N by $\mathbb{Z}_p \to 1 + 2p\mathbb{Z}_p$ by $\langle N \rangle$. We put $c = \log_\gamma \langle N \rangle$. We define the dual of Pollack's p-adic L-function $\mathscr{L}_p^{\pm,\vee}(E, \eta, X)$ by $\mathscr{L}_p^{\pm}(E, \eta^{-1}, \frac{-X}{X+1})$. Then,

THEOREM 3.2.1. *Pollack's p-adic L-functions have the functional equation*

$$\mathscr{L}_p^{\pm,\vee}(E, \eta, X) = w_E \, \eta(-N) \, (1+X)^c \, \mathscr{L}_p^{\pm}(E, \eta, X)$$

where w_E is the root number of the Hasse-Weil L-function $L(E, s)$.

PROOF. This follows from the functional equation of the usual p-adic L-function (Theorem 2.3.2) and the functional equation of $\Phi^{\pm}(X)$. See Theorem 7.14 of Pollack [**21**]. □

Let $\lambda_\pm$ and $\mu_\pm$ be the λ and μ-invariants of $\mathscr{L}_p^{\pm}(E, X) \in \mathbb{Z}_p[[X]]$.

COROLLARY 3.2.2. *Let $n_\pm$ be the order of zero of $\mathscr{L}_p^{\pm}(E, X)$ at $X = 0$. Then $w_E = (-1)^{\lambda_+} = (-1)^{\lambda_-} = (-1)^{n_+} = (-1)^{n_-}$.*

PROOF. The corollary is proved in the same way as Corollary 2.3.3 and Corollary 2.4.6. □

3. Pollack's analytic Iwasawa formula for the order of the Tate-Shafarevich group

Assuming the Birch and Swinnerton-Dyer conjecture for cyclotomic fields, Pollack gave analytically an Iwasawa formula for Tate-Shafarevich groups in terms of the λ- and μ-invariants of his p-adic L-functions.

Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension and let $\mathbb{Q}_n$ be the n-th layer. The order of the Tate-Shafarevich group $Ш(E/\mathbb{Q}_n)$ is conjectured to appear the leading coefficient of the Taylor expansion of the Hasse-Weil L-function $L(E/\mathbb{Q}_n, s)$ at $s = 1$. In other words, the order of the Tate-Shafarevich group is analytically computed by using the higher derivative of $L(E/\mathbb{Q}_n, s)$. Namely,

$$\sharp Ш(E/\mathbb{Q}_n) = \frac{L^{(r_n)}(E/\mathbb{Q}_n, 1) \, \sharp E_{\mathrm{tor}}(\mathbb{Q}_n)^2 \, \sqrt{D(\mathbb{Q}_n)}}{\Omega_{E/\mathbb{Q}_n} \, 2^{r_n} \, R(E/\mathbb{Q}_n) \, \mathrm{Tam}(E/\mathbb{Q}_n)}, \tag{3.3.1}$$

where $D(\cdot)$ is the discriminant over $\mathbb{Q}$, $R(E/\cdot)$ is the regulator, $\mathrm{Tam}(E/\cdot)$ is the product of the Tamagawa numbers, $\Omega_{E/\cdot}$ is the real period and r_n is the rank of $E(\mathbb{Q}_n)$.

The key to obtain Pollack's analytic Iwasawa formula is, instead of looking directly (3.3.1), to see the difference of the order of the $n+1$-th and the n-th Tate-Shafarevich groups for sufficiently large n. Then the regulator terms

disappear, and the formula is simply written as

$$\frac{\sharp Ш(E/\mathbb{Q}_{n+1})}{\sharp Ш(E/\mathbb{Q}_n)} = \left(\Pi_\chi \frac{L(E/\mathbb{Q},\chi,1)}{\Omega_{E/\mathbb{Q}}}\right) d_n. \tag{3.3.2}$$

Here the product is taken over all χ corresponding to $\mathbb{Q}_{n+1}$ but not to $\mathbb{Q}_n$, and d_n is an integer whose p-adic valuation is

$$\mathrm{ord}_p(d_n) = \phi(p^n)\,\frac{n+1}{2} - r_\infty$$

where $r_\infty = \mathrm{rank}\, E(\mathbb{Q}_\infty)$ and $\phi(p^n) = p^n - p^{n-1}$.

Then the right hand side of (3.3.2) is computed by Pollack's p-adic L-functions from the interpolation properties.

THEOREM 3.3.1 (Analytic Iwasawa formula). *Let*

$$e_n = \mathrm{ord}_p(\sharp Ш(E/\mathbb{Q}_n)).$$

We assume the Birch and Swinnerton-Dyer conjecture for cyclotomic fields. Then, for sufficiently large n,

$$e_n = \begin{cases} p^{n-1} + p^{n-3} + \cdots + p + \frac{n}{2}\,(\lambda_- + \lambda_+ - 2r_\infty - 1) + \\ \sum_{k=1}^{\frac{n}{2}} (\phi(p^{2k})\,\mu_- + \phi(p^{2k-1})\,\mu_+) + \nu \quad \textit{if } n \mid 2 \\ \\ p^{n-1} + p^{n-3} + \cdots + p^2 + \frac{n-1}{2}\,(\lambda_+ + \lambda_- - 2r_\infty - 1) + \\ \sum_{k=1}^{\frac{n-1}{2}} (\phi(p^{2k+1})\,\mu_+ + \phi(p^{2k})\,\mu_-) + \nu \quad \textit{if } n \nmid 2 \end{cases}$$

where ν is a non-negative constant independent of n.

By comparing with Greenberg's conjecture in the good ordinary case and by numerical data, Pollack conjectured that μ_+ and μ_- are always equal to zero. Then the above formula coincides with the formula conjectured by Kurihara.

COROLLARY 3.3.2. *Assume that $\mu_+ = \mu_- = 0$. Then for sufficiently large n,*

$$e_n = [\mu p^n + \lambda n + \nu] \quad \textit{with } \mu = \frac{p}{p^2-1},\ \ \lambda = \frac{\lambda_+ + \lambda_- - 1}{2} - r_\infty$$

where $[\,\cdot\,]$ is the Gaussian symbol.

CHAPTER 4

The plus (minus) Perrin-Riou map

We study a certain canonical formal group $\mathscr{F}_{ss}$ over $\mathbb{Z}_p$, which is isomorphic to the formal groups of the elliptic curves with $a_p = 0$. Then the plus (minus) Perrin-Riou map is defined and studied in the language of $\mathscr{F}_{ss}$. We define a certain subgroup of $\mathscr{F}_{ss}$, called the norm subgroup, which plays important roles to investigate properties of $\mathscr{F}_{ss}$ and our Perrin-Riou map. The norm subgroup also gives an answer how to put a local condition at p to define a good Selmer group. We remark that the plus (minus) Perrin-Riou map is obtained by modifying the P_n-pairing in Kurihara [**10**] where Honda's theory is used to study the P_n-pairing.

1. Honda's theory of formal groups

We recall Honda's theory of formal groups. We restrict ourselves to commutative formal groups over $\mathbb{Z}_p$ of dimension 1.

Let $\mathcal{P}$ be the $\mathbb{Z}_p$-submodule of $\mathbb{Q}_p[[X]]$ consisting of the elements such that $f(X) = \sum_{k=1}^{\infty} a_k X^k$, $ka_k \in \mathbb{Z}_p$ for all k. Let φ be an element of $\mathbb{Z}_p[[X]]$ such that $\varphi(X) \equiv X^p \mod p\mathbb{Z}_p$. We define an endomorphism φ of $\mathcal{P}$ by

$$\varphi(\sum a_k X^k) := \sum a_k \varphi(X)^k.$$

(φ is well-defined by Lemma 1.1 of Perrin-Riou [**16**].) We denote the n-iterated composition of the endomorphism φ by $\varphi^{(n)}$. For $u(X) = \sum_{k=0}^{\infty} b_k X^k \in \mathbb{Z}_p[[X]]$, we define an endomorphism $u(\varphi)$ by

$$u(\varphi)(f)(X) := \sum_{k=0}^{\infty} b_k f(\varphi^{(k)}(X)).$$

LEMMA 4.1.1. *Let φ be a power series in $\mathbb{Z}_p[[X]]$ such that $\varphi(X) \equiv X^p \mod p\mathbb{Z}_p$. Then φ induces the Frobenius operator $F : \sum a_k X^k \mapsto \sum a_k X^{pk}$ on $\mathcal{P}$ modulo $p\mathbb{Z}_p[[X]]$.*

PROOF. Lemma 1.1 of Perrin-Riou [**16**]. □

DEFINITION 4.1.2. *For $u(X) \in \mathbb{Z}_p[[X]]$, we say $f \in \mathcal{P}$ is of the Honda type u when $u(\varphi)(f) \equiv 0 \mod p\mathbb{Z}_p[[X]]$ for some φ.*

By Lemma 4.1.1, if f satisfies $u(\varphi)(f) \equiv 0 \mod p\mathbb{Z}_p[[X]]$ for some φ, then for any φ. Honda constructed his theory for $\varphi(X) = X^p$, and this remark

enables us to apply his theory for any φ. We use $\varphi(X) = (X+1)^p - 1$. In [**10**], Kurihara used Honda's theory for $\varphi(X) = X^p$. By taking $\varphi(X) = (X+1)^p - 1$, his arguments become simpler.

A polynomial $u(X) = a_0 + a_1 X + \cdots + a_h X^h \in \mathbb{Z}_p[X]$ is called an Eisenstein polynomial, or of the Eisenstein type, if a_h is a unit, $p \mid a_i$ for all $i \neq h$ and $a_0 = p$.

Let $\mathscr{F}$ be a formal group over $\mathbb{Z}_p$ of dimension 1. We denote the logarithm of $\mathscr{F}$ by $\log_{\mathscr{F}}$ and the exponential by $\exp_{\mathscr{F}}$. We remark that $\log_{\mathscr{F}}(X) \in \mathcal{P}$. If $\log_{\mathscr{F}}(X)$ is of the Honda type u, we say that $\mathscr{F}$ is of Honda type u. An isomorphism $i : \mathscr{F} \to \mathscr{G}$ is called a strong isomorphism if $i(X) \equiv X$ modulo degree 2.

THEOREM 4.1.3 (Honda). *There is a one-to-one correspondence between the set of the isomorphism classes of commutative formal groups over $\mathbb{Z}_p$ of dimension 1 and the set of Eisenstein polynomials in $\mathbb{Z}_p[X]$. In the correspondence, the height of a formal group corresponds to the degree of an Eisenstein polynomial. More precisely,*

i) *Let $\mathscr{F}$ be a formal group of dimension 1 over $\mathbb{Z}_p$. Then there exists a unique Eisenstein polynomial u such that $\log_{\mathscr{F}}$ is of the Honda type u. The polynomial u depends only on the isomorphism class of $\mathscr{F}$.*
ii) *Let $\mathscr{F}$ and $\mathscr{G}$ be formal groups over $\mathbb{Z}_p$ of dimension 1 whose logarithms are of the same Honda type u for an Eisenstein polynomial u. Then $\exp_{\mathscr{G}} \circ \log_{\mathscr{F}}(X) \in \mathbb{Z}_p[[X]]$ and $\exp_{\mathscr{G}} \circ \log_{\mathscr{F}}(X) \equiv X$ modulo degree 2. In particular, $\exp_{\mathscr{G}} \circ \log_{\mathscr{F}}(X)$ gives a strong isomorphism between $\mathscr{F}$ and $\mathscr{G}$.*
iii) *Let u be an Eisenstein polynomial. Then there exists a formal group $\mathscr{F}$ whose logarithm is of the Honda type u.*

PROOF. The theorem is a combination of theorems and propositions in Honda [**6**]. See Theorem 2, Theorem 4, Proposition 2.6 and Proposition 3.5 in Honda [**6**]. □

For a fixed φ and a given Eisenstein polynomial $u(X) = p + a_1 X + \cdots + a_h X^h$, we can explicitly construct a formal group over $\mathbb{Z}_p$ of the Honda type u. Let $(x_n)_{n \geq -h+1}$ be the sequence of elements of $\mathbb{Q}$ satisfying $x_n = 0$ if $n < 0$, $x_0 = 1$ and $p x_{n+h} + a_1 x_{n+h-1} + \cdots + a_h x_n = 0$. We put

$$f(X) = \sum_{n=0}^{\infty} x_n \, \varphi^{(n)}(X).$$

Then, we have $u(\varphi)(f(X)) = pX$. Hence $f(X)$ is of Honda type u. By Honda's theory, $F(X,Y) = f^{-1}(f(X) + f(Y))$ is in $\mathbb{Z}_p[[X,Y]]$. Hence there exists a formal group $\mathscr{F}$ whose group law is given by $F(X,Y) = f^{-1}(f(X) + f(Y))$

and the logarithm by f.

EXAMPLE (The case $\mathbb{G}_m$). *The logarithm of $\mathbb{G}_m$ is given by*

$$\log_{\mathbb{G}_m}(X) = \sum_{n=1}^{\infty} (-1)^n \frac{X^n}{n}.$$

Let $\varphi(X) = X^p$. Then $(p-\varphi)\log_{\mathbb{G}_m}(X) = p\sum_{n,\, p\nmid n} (-1)^n \frac{X^n}{n}$. Hence $\mathbb{G}_m$ is of the Honda type $p - X$. The canonical formal group $\mathscr{F}_m$ of type $p-X$ is the formal group whose logarithm is given by

$$\log_{\mathscr{F}_m}(X) = \sum_{n=0}^{\infty} \frac{\varphi^{(n)}(X)}{p^n} = \sum_{n=0}^{\infty} \frac{X^{p^n}}{p^n}.$$

The strong isomorphism $\mathscr{F}_m \to \mathbb{G}_m$ is given by the Artin-Hasse exponential

$$\exp_{\mathbb{G}_m} \circ \log_{\mathscr{F}_m}(X) = \exp\,(\sum_{n=0}^{\infty} \frac{X^{p^n}}{p^n}).$$

2. Canonical formal groups of elliptic curves

For an elliptic curve E over $\mathbb{Q}_p$ with non-additive reduction, by using Honda's theory, we define a canonical formal group which is isomorphic to the formal group of the minimal model of E.

We denote the Euler factor of E by $L_p(X)$, which is $L_p(X) = X^2 - a_p X + p$ if E has good reduction and $L_p(X) = X - a_p$ if E has multiplicative reduction ($a_p = 1$ or -1 according to E has split or non-split multiplicative reduction).

We put $\ell_p(X) = X^{\deg L_p(X)} L_p(\frac{p}{X})$. Explicitly, $\ell_p(X) = L_p(X)$ if E has good reduction, and $\ell_p(X) = p - a_p X$ if E has multiplicative reduction.

THEOREM 4.2.1 (Honda [**6**], Theorem 9, p. 240). *Let E be an elliptic curve over $\mathbb{Q}_p$ with non-additive reduction. Then the formal group $\hat{E}$ of the minimal model of E is of Honda type $\ell_p(X)$.*

We fix φ as $\varphi(X) = (1+X)^p - 1$.

2.1. The good ordinary case. Suppose E has good ordinary reduction at p. Then $\ell_p(X) = X^2 - a_p X + p$ has a unit root α, and is factorized as $\ell_p(X) = (1-\alpha^{-1}X)(p-\alpha X)$. The polynomial $1-\alpha^{-1}X$ is a unit in $\mathbb{Z}_p[[X]]$ and $p-\alpha X$ is of Eisenstein type. The canonical formal group $\mathscr{F}_\alpha$ of the type $p-\alpha X$ is the formal group whose logarithm is given by

$$\log_{\mathscr{F}_\alpha}(X) = \sum_{k=0}^{\infty} \alpha^k \frac{(X+1)^{p^k} - 1}{p^k}.$$

By Theorem 4.2.1, $\mathscr{F}_\alpha$ is isomorphic to the formal group of E. The Artin-Hasse type power series $\exp_{\hat{E}} \circ \log_{\mathscr{F}_\alpha}(X)$ gives a strong isomorphism $\mathscr{F}_\alpha \to \hat{E}$.

2.2. The good supersingular case. Suppose E has good supersingular reduction at p. Then $\ell_p(X) = X^2 - a_pX + p$ is an Eisenstein polynomial. For simplicity, we assume that $a_p = 0$ (note that if $p \geq 5$, we have automatically $a_p = 0$). The canonical formal group $\mathscr{F}_{ss}$ of the type $p + X^2$ is the formal group whose logarithm is given by

$$\log_{\mathscr{F}_{ss}}(X) = \sum_{k=0}^{\infty} (-1)^k \frac{(X+1)^{p^{2k}} - 1}{p^k}.$$

By Theorem 4.2.1, $\mathscr{F}_{ss}$ is isomorphic to the formal group of E. The Artin-Hasse type power series $\exp_{\hat{E}} \circ \log_{\mathscr{F}_{ss}}(X)$ gives a strong isomorphism $\mathscr{F}_{ss} \to \hat{E}$. We remark that the p-adic Tate module of any E with $a_p = 0$ is isomorphic to the p-adic Tate module of $\mathscr{F}_{ss}$.

2.3. The multiplicative reduction case. Suppose E has multiplicative reduction at p. Then $\ell_p(X) = p - a_pX$ is an Eisenstein polynomial. The canonical formal group of the type $p - a_pX$ is $\mathscr{F}_\alpha$, $\alpha = a_p = \pm 1$ (cf. the good ordinary case). Note that $\mathscr{F}_1 = \mathscr{F}_m$ is strongly isomorphic to $\mathbb{G}_m$ (see the example in the previous section).

We investigate properties of $\mathscr{F}_{ss}$ in the next two sections. We can construct a similar theory for $\mathscr{F}_\alpha$.

3. Torsion subgroups of $\mathscr{F}_{ss}$

We show that the p-power torsion subgroup over $k_n = \mathbb{Q}_p(\zeta_{p^n})$ of the canonical formal group $\mathscr{F}_{ss}$ is trivial.

PROPOSITION 4.3.1. *Over the unramified quadratic extension of $\mathbb{Q}_p$, the formal group $\mathscr{F}_{ss}$ is isomorphic to the Lubin-Tate formal group of height two with the parameter $-p$.*

PROOF. We show that the multiplication $[-p]$ of $\mathscr{F}_{ss}$ satisfies that i) $[-p]X \equiv -pX$ modulo degree 2 and ii) $[-p]X \equiv X^{p^2}$ modulo p. The condition i) follows from general properties of commutative formal groups. We show the condition ii). The multiplication $[-p]$ of $\mathscr{F}_{ss}$ is given by $\exp_{\mathscr{F}_{ss}}(-p \log_{\mathscr{F}_{ss}}(X))$, which is in $\mathbb{Z}_p[[X]]$ by Honda. Since $(\varphi^{(2)} + p) \log_{\mathscr{F}_{ss}}(X) \equiv 0$ modulo $p\,\mathbb{Z}_p[[X]]$, we have $\exp_{\mathscr{F}_{ss}}(-p \log_{\mathscr{F}_{ss}}(X)) \equiv \exp_{\mathscr{F}_{ss}}(\varphi^{(2)} \log_{\mathscr{F}_{ss}}(X)) \equiv \exp_{\mathscr{F}_{ss}}(\log_{\mathscr{F}_{ss}}(\varphi^{(2)}(X))) \equiv \varphi^{(2)}(X)$ modulo $p\,\mathbb{Z}_p[[X]]$. (cf. $\exp_{\mathscr{F}_{ss}}(p\mathbb{Z}_p) = p\mathbb{Z}_p$.) □

PROPOSITION 4.3.2. *The formal group $\mathscr{F}_{ss}$ has no p-power torsion point on the cyclotomic field k_n.*

PROOF. Let L be the composite field of k_n and the unramified quadratic extension K of $\mathbb{Q}_p$. Let $\mathfrak{m}_L$ be the maximal ideal of the integer ring O_L. We denote the field obtained by adjoining all p-torsion points of $\mathscr{F}_{ss}$ to K

by $K(\mathscr{F}_{ss}[p])$, which is an abelian extension of K of degree p^2-1 by the Lubin-Tate theory. Suppose that there is a p-torsion point in $\mathscr{F}_{ss}(\mathfrak{m}_L)$. Since $K(\mathscr{F}_{ss}[p])/K$ is abelian, all subextensions are normal over K. Therefore L contains all p-torsion points, namely, $L \supseteq K(\mathscr{F}_{ss}[p])$. However, the degree of L/K is $\phi(p^n) = p^n - p^{n-1}$, which is not a multiple of p^2-1. Hence we have a contradiction. □

4. Norm subgroups of $\mathscr{F}_{ss}$

Let $\mathfrak{m}_n$ be the maximal ideal of $\mathbb{Z}_p[\zeta_{p^n}]$ for $n \geq 1$ and $\mathfrak{m}_0 = p\mathbb{Z}_p$. We show that there exists a canonical norm compatible system $(\mathrm{c}_n)_n$, $\mathrm{c}_n \in \mathscr{F}_{ss}(\mathfrak{m}_n)$. The element c_n is almost a cyclotomic unit $\zeta_{p^n}-1 \in \mathscr{F}_{ss}(\mathfrak{m}_n)$. We study a subgroup $\mathscr{C}_{ss}(\mathfrak{m}_n)$ of $\mathscr{F}_{ss}(\mathfrak{m}_n)$ called the n-th norm subgroup, which is generated over $\mathbb{Z}_p$ by $(\mathrm{c}_n^{\sigma})_{\sigma \in \mathcal{G}_n}$.

We fix a generator (ζ_{p^n}) of $\mathbb{Z}_p(1)$ as in Chapter 1. For $m \geq n$, we denote the trace (norm) map $\mathscr{F}_{ss}(\mathfrak{m}_m) \to \mathscr{F}_{ss}(\mathfrak{m}_n)$ by $\mathrm{Tr}^{ss}_{m/n}$.

Let $\varepsilon \in \mathfrak{m}_0$ be an element such that $\log_{\mathscr{F}_{ss}}(\varepsilon) = \frac{p}{p+1}$ (cf. $\log_{\mathscr{F}_{ss}}(\mathfrak{m}_0) = \mathfrak{m}_0$). We put

$$\mathrm{c}_n = (\zeta_{p^n} - 1)[+]_{\mathscr{F}_{ss}}\varepsilon$$

where $[+]_{\mathscr{F}_{ss}}$ is the addition of $\mathscr{F}_{ss}$. We also put $\mathrm{c}_0 = \varepsilon$ and $\mathrm{c}_{-1} = 2\varepsilon$.

Lemma 4.4.1. *For $n \geq 1$, we have*

$$\mathrm{Tr}^{ss}_{n/n-1}(\mathrm{c}_n) = -\mathrm{c}_{n-2}.$$

Proof. By Proposition 4.3.2, $\log_{\mathscr{F}_{ss}}$ is injective on $\mathscr{F}_{ss}(\mathfrak{m}_n)$. Hence it suffices to show that the image of c_n by $\log_{\mathscr{F}_{ss}}$ satisfies the above relation. For $n \geq 2$, we have

$$\begin{aligned}
\mathrm{Tr}_{n/n-1} \log_{\mathscr{F}_{ss}}(\mathrm{c}_n) &= \mathrm{Tr}_{n/n-1}\left(\frac{p}{p+1} + \sum_{k=0}^{[\frac{n+1}{2}]} (-1)^k \frac{\zeta_{p^{n-2k}} - 1}{p^k} \right) \\
&= \frac{p^2}{p+1} - p + p\left(\sum_{k=1}^{[\frac{n+1}{2}]} (-1)^k \frac{\zeta_{p^{n-2k}} - 1}{p^k} \right) \\
&= -\log_{\mathscr{F}_{ss}}(\mathrm{c}_{n-2}).
\end{aligned}$$

The case $n = 1$ is proved similarly. □

Definition 4.4.2. *For $n \geq 0$, we define the n-th norm subgroup by*

$$\mathscr{C}_{ss}(\mathfrak{m}_n) = \{P \in \mathscr{F}_{ss}(\mathfrak{m}_n) \mid \mathrm{Tr}^{ss}_{n/m} P \in \mathscr{F}_{ss}(\mathfrak{m}_{m-1}) \text{ for all } m \equiv n-1 \bmod 2\}.$$

The following lemma is very useful and played essential roles in Honda's works.

LEMMA 4.4.3 (Honda's lemma). *Let X and Y be indeterminants. For an arbitrary integer $m \geq 1$, we have*

$$\frac{(X+pY)^m}{m} \equiv \frac{X^m}{m} \mod p\mathbb{Z}_p[X,Y].$$

PROOF. The lemma is found in Honda [**5**] as Lemma 4. See also Lemma 2.1 in Honda [**6**]. □

PROPOSITION 4.4.4. *We have $\log_{\mathscr{F}_{ss}}(\mathfrak{m}_n) \subseteq \mathfrak{m}_n + k_{n-1}$. In particular, there exists a canonical isomorphism*

$$\mathscr{F}_{ss}(\mathfrak{m}_n)/\mathscr{F}_{ss}(\mathfrak{m}_{n-1}) \cong \log_{\mathscr{F}_{ss}}(\mathfrak{m}_n)/\log_{\mathscr{F}_{ss}}(\mathfrak{m}_{n-1}) \cong \mathfrak{m}_n/\mathfrak{m}_{n-1}.$$

By this isomorphism, c_n^σ is sent to c_n^σ itself. In particular, $(\mathrm{c}_n^\sigma)_{\sigma\in\mathcal{G}_n}$ generates $\mathscr{F}_{ss}(\mathfrak{m}_n)/\mathscr{F}_{ss}(\mathfrak{m}_{n-1})$ as $\mathbb{Z}_p$-module.

PROOF. As a set, $\mathscr{F}_{ss}(\mathfrak{m}_n)$ is the maximal ideal $\mathfrak{m}_n$, and we write $x \in \mathscr{F}_{ss}(\mathfrak{m}_n)$ of the form $x = \sum_i a_i\,\zeta_{p^n}^i$, $a_i \in \mathbb{Z}_p$. Then $x^{p^k} \equiv \sum_i a_i\,\zeta_{p^n}^{ip^k} \mod p\mathbb{Z}_p[\zeta_{p^n}]$ and $y_k = \sum_i a_i\,\zeta_{p^n}^{ip^k} \in \mathfrak{m}_{n-1}$ for $k \geq 1$. Therefore by Honda's lemma, we have

$$\frac{x^{p^{2k}}}{p^k} = \frac{(x^{p^k})^{p^k}}{p^k} \equiv \frac{y_k^{p^k}}{p^k} \mod \mathfrak{m}_n.$$

Hence we have $\frac{x^{p^{2k}}}{p^k} \in \mathfrak{m}_n + k_{n-1}$. By Lemma 4.1.1 or Honda's lemma, there exists $f(X) \in p\mathbb{Z}_p[[X]]$ such that

$$\log_{\mathscr{F}_{ss}}(X) = \sum_{k=0}^{\infty} \frac{X^{p^{2k}}}{p^k} + f(X).$$

Since for sufficiently large N, $\sum_{k=N}^{\infty} \frac{x^{p^{2k}}}{p^k}$ is in $\mathfrak{m}_n$, we have $\log_{\mathscr{F}_{ss}}(x) \in \mathfrak{m}_n + k_{n-1}$.

Since $\log_{\mathscr{F}_{ss}}$ is injective on $\mathscr{F}_{ss}(\mathfrak{m}_n)$ and is compatible with the Galois action, we have $\log_{\mathscr{F}_{ss}}\mathfrak{m}_n \cap k_{n-1} = \log_{\mathscr{F}_{ss}}\mathfrak{m}_{n-1}$. Therefore we have an injection

$$\log_{\mathscr{F}_{ss}}(\mathfrak{m}_n)/\log_{\mathscr{F}_{ss}}(\mathfrak{m}_{n-1}) \hookrightarrow (\mathfrak{m}_n + k_{n-1})/k_{n-1} \cong \mathfrak{m}_n/\mathfrak{m}_{n-1}.$$

By direct calculations, we have $\log_{\mathscr{F}_{ss}}(\mathrm{c}_n^\sigma) \equiv \mathrm{c}_n^\sigma \mod k_{n-1}$. Since $(\mathrm{c}_n^\sigma)_{\sigma\in\mathcal{G}_n}$ generates $\mathfrak{m}_n/\mathfrak{m}_{n-1}$ by the usual addition, the above injection is in fact a bijection. □

PROPOSITION 4.4.5. i) *The n-th norm subgroup $\mathscr{C}_{ss}(\mathfrak{m}_n)$ is generated by $(\mathrm{c}_n^\sigma)_{\sigma\in\mathcal{G}_n}$ as $\mathbb{Z}_p$-module.*
ii) *We have $\mathscr{C}_{ss}(\mathfrak{m}_n) \cap \mathscr{C}_{ss}(\mathfrak{m}_{n-1}) = \mathscr{F}_{ss}(\mathfrak{m}_0)$ and $\mathscr{F}_{ss}(\mathfrak{m}_n) = \mathscr{C}_{ss}(\mathfrak{m}_n) + \mathscr{C}_{ss}(\mathfrak{m}_{n-1})$. In other words, we have an exact sequence*

$$0 \to \mathscr{F}_{ss}(\mathfrak{m}_0) \to \mathscr{C}_{ss}(\mathfrak{m}_n) \oplus \mathscr{C}_{ss}(\mathfrak{m}_{n-1}) \to \mathscr{F}_{ss}(\mathfrak{m}_n) \to 0$$

where the first map is the diagonal embedding by inclusions, and the second map is $(a, b) \mapsto [-1]^n(a[-]_{\mathscr{F}_{ss}} b)$.

PROOF. We first show that $\mathscr{C}_{ss}(\mathfrak{m}_n) \cap \mathscr{C}_{ss}(\mathfrak{m}_{n-1}) = \mathscr{F}_{ss}(\mathfrak{m}_0)$. Let $P \in \mathscr{C}_{ss}(\mathfrak{m}_n) \cap \mathscr{C}_{ss}(\mathfrak{m}_{n-1})$. Suppose $P \in \mathscr{F}_{ss}(\mathfrak{m}_m) \setminus \mathscr{F}_{ss}(\mathfrak{m}_{m-1})$ for some $m \geq 1$. Then $\mathrm{Tr}^{ss}_{n/m} P = p^{n-m} P \in \mathscr{F}_{ss}(\mathfrak{m}_{m-1})$ since $P \in \mathscr{C}_{ss}(\mathfrak{m}_n) \cap \mathscr{C}_{ss}(\mathfrak{m}_{n-1})$. Therefore for $\sigma \in \mathrm{Gal}(k_m/k_{m-1})$, we have $p^{n-m}(P^\sigma - P) = 0$. Hence, by Proposition 4.3.2, $P \in \mathscr{F}_{ss}(\mathfrak{m}_{m-1})$. This is a contradiction.

For the moment, let $\mathscr{C}'_{ss}(\mathfrak{m}_n)$ be the $\mathbb{Z}_p$-submodule generated by $(\mathrm{c}_n^\sigma)_{\sigma \in \mathcal{G}_n}$. We prove i) and $\mathscr{F}_{ss}(\mathfrak{m}_n) = \mathscr{C}_{ss}(\mathfrak{m}_n) + \mathscr{C}_{ss}(\mathfrak{m}_{n-1})$ by induction. Suppose they are true for $n-1$. Then $\mathscr{F}_{ss}(\mathfrak{m}_{n-1}) = \mathscr{C}_{ss}(\mathfrak{m}_{n-1}) + \mathscr{C}_{ss}(\mathfrak{m}_{n-2})$ and

$$\mathscr{C}_{ss}(\mathfrak{m}_{n-2}) = \mathscr{C}'_{ss}(\mathfrak{m}_{n-2}) \subseteq \mathscr{C}'_{ss}(\mathfrak{m}_n) \subseteq \mathscr{C}_{ss}(\mathfrak{m}_n)$$

by Lemma 4.4.1 and the inductive hypothesis. Therefore, by Proposition 4.4.4, we have

$$\mathscr{F}_{ss}(\mathfrak{m}_n) = \mathscr{C}'_{ss}(\mathfrak{m}_n) + \mathscr{F}_{ss}(\mathfrak{m}_{n-1}) = \mathscr{C}'_{ss}(\mathfrak{m}_n) + \mathscr{C}_{ss}(\mathfrak{m}_{n-1}).$$

In particular, $\mathscr{C}'_{ss}(\mathfrak{m}_n) + \mathscr{C}_{ss}(\mathfrak{m}_{n-1}) \supseteq \mathscr{C}_{ss}(\mathfrak{m}_n)$. Since $\mathscr{C}_{ss}(\mathfrak{m}_n) \cap \mathscr{C}_{ss}(\mathfrak{m}_{n-1}) = \mathscr{F}_{ss}(\mathfrak{m}_0)$, we have $\mathscr{C}'_{ss}(\mathfrak{m}_n) = \mathscr{C}_{ss}(\mathfrak{m}_n)$. □

Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character. For a $\mathbb{Z}_p[\Delta]$-module M, we denote the η-component of M by M^η, which is the largest submodule on which Δ acts by η. If we put

$$\epsilon_\eta = \frac{1}{\sharp\Delta} \sum_{\tau \in \Delta} \eta^{-1}(\tau)\, \tau,$$

M^η is given by $\epsilon_\eta M$.

For a non-trivial η, we put

$$q_n^\eta = \sum_{k=0}^{n-1} (-1)^{n-k-1}\, p^k.$$

For the trivial character, we put

$$q_n^\eta = q_n^1 = \begin{cases} \sum_{k=0}^{n-1} (-1)^{n-k-1}\, p^k & \text{for odd } n, \\ \sum_{k=0}^{n-1} (-1)^{n-k-1}\, p^k \ +1 & \text{for even } n. \end{cases}$$

Finally, we put

$$q_n = \begin{cases} \sum_{k=1}^{n} (-1)^{n-k}\, \phi(p^k) & \text{for odd } n, \\ \sum_{k=1}^{n} (-1)^{n-k}\, \phi(p^k) \ +1 & \text{for even } n \end{cases}$$

where $\phi(p^k) = p^k - p^{k-1}$. By definition, we have $q_n = \sum_{\eta \in \Delta^\vee} q_n^\eta$.

PROPOSITION 4.4.6. i) $\operatorname{rank}_{\mathbb{Z}_p} \mathscr{C}_{ss}(\mathfrak{m}_n)^\eta = q_n^\eta$. *In particular, we have* $\operatorname{rank}_{\mathbb{Z}_p} \mathscr{C}_{ss}(\mathfrak{m}_n) = q_n$.
ii) *We put* $N = \mathrm{Tr}^{ss}_{n+1/n}$. *Then*

$$\dim_{\mathbb{F}_p} \mathscr{F}_{ss}(\mathfrak{m}_n)^\eta/N\mathscr{F}_{ss}(\mathfrak{m}_{n+1})^\eta = \begin{cases} q_n^\eta & \text{if } \eta \text{ is non-trivial,} \\ q_n^1 - 1 & \text{if } \eta \text{ is trivial.} \end{cases}$$

In particular, we have $\dim_{\mathbb{F}_p} \mathscr{F}_{ss}(\mathfrak{m}_n)/N\mathscr{F}_{ss}(\mathfrak{m}_{n+1}) = q_n - 1$.

PROOF. Since the $\mathbb{Z}_p$-rank of $\mathscr{F}_{ss}(\mathfrak{m}_n)$ is $\phi(p^n)$ and $\mathscr{F}_{ss}(\mathfrak{m}_n)^\eta$ is p^{n-1}, i) follows from Proposition 4.4.5 ii) by induction. For ii), we consider a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathscr{F}_{ss}(\mathfrak{m}_0)^\eta & \longrightarrow & \mathscr{C}_{ss}(\mathfrak{m}_{n+1})^\eta \oplus \mathscr{C}_{ss}(\mathfrak{m}_n)^\eta & \longrightarrow & \mathscr{F}_{ss}(\mathfrak{m}_{n+1})^\eta & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \times p} & & \downarrow{\scriptstyle N} \quad \downarrow{\scriptstyle \times p} & & \downarrow{\scriptstyle N} & & \\
0 & \longrightarrow & \mathscr{F}_{ss}(\mathfrak{m}_0)^\eta & \longrightarrow & \mathscr{C}_{ss}(\mathfrak{m}_{n-1})^\eta \oplus \mathscr{C}_{ss}(\mathfrak{m}_n)^\eta & \longrightarrow & \mathscr{F}_{ss}(\mathfrak{m}_n)^\eta & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \dfrac{\mathscr{F}_{ss}(\mathfrak{m}_0)^\eta}{p\,\mathscr{F}_{ss}(\mathfrak{m}_0)^\eta} & \xrightarrow{i} & \dfrac{\mathscr{C}_{ss}(\mathfrak{m}_n)^\eta}{p\,\mathscr{C}_{ss}(\mathfrak{m}_n)^\eta} & \longrightarrow & \dfrac{\mathscr{F}_{ss}(\mathfrak{m}_n)^\eta}{N\mathscr{F}_{ss}(\mathfrak{m}_{n+1})^\eta} & \longrightarrow & 0
\end{array}$$

The top and the second horizontal sequences are exact by Proposition 4.4.5. Since the norm map $\mathscr{C}_{ss}(\mathfrak{m}_{n+1})^\eta \to \mathscr{C}_{ss}(\mathfrak{m}_{n-1})^\eta$ is surjective by Lemma 4.4.1 and Proposition 4.4.5 i), the middle vertical sequence is exact. We show that i is injective. If η is not trivial, then $\mathscr{F}_{ss}(\mathfrak{m}_0)^\eta = 0$. Suppose that η is trivial. Let $x \in \mathscr{F}_{ss}(\mathfrak{m}_0) \cap p\,\mathscr{C}_{ss}(\mathfrak{m}_n)$. We write $x = [p]\,y$ for some $y \in \mathscr{C}_{ss}(\mathfrak{m}_n)$. For arbitrary $\sigma \in \mathcal{G}_n$, we have $[p](y^\sigma[-]y) = x^\sigma[-]x = 0$, where $[-]$ is the subtraction of $\mathscr{F}_{ss}$. Since $\mathscr{F}_{ss}(\mathfrak{m}_n)$ has no p-torsion point, we have $y^\sigma = y$, that is, $y \in \mathscr{F}_{ss}(\mathfrak{m}_0)$.

Hence the bottom horizontal sequence is exact, and ii) follows from this sequence and i) in this corollary. □

5. The Perrin-Riou map of elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction and $a_p = 0$. Let T be the Tate module of E and $V = T \otimes \mathbb{Q}_p$. We put $i(X) = \exp_{\hat{E}} \circ \log_{\mathscr{F}_{ss}}(X)$. By Theorem 4.1.3, the power series $i(X)$ is in $\mathbb{Z}[[X]]$ and gives an strong isomorphism $i : \mathscr{F}_{ss} \to \hat{E}$. The isomorphism $i : \mathscr{F}_{ss}(\mathfrak{m}_n) \to \hat{E}(\mathfrak{m}_n)$ and the Kummer map $\hat{E}(\mathfrak{m}_n) \to H^1(k_n, T)$ induce the cup product pairing

$$(\ ,\ )_n : \mathscr{F}_{ss}(\mathfrak{m}_n) \times H^1(k_n, T) \to H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p. \tag{4.5.1}$$

For $x \in \mathscr{F}_{ss}(\mathfrak{m}_n)$, we define a morphism $P_{n,x} : H^1(k_n, T) \to \mathbb{Z}_p[\mathcal{G}_n]$ by

$$z \quad \longmapsto \sum_{\sigma \in \mathcal{G}_n} (x^\sigma, z)_n \, \sigma,$$

which is compatible with the natural Galois action. In Section 6 of this chapter, we see that $P_{n,x}$ is nothing but Kurihara's $z \mapsto p^n P_n(x, z)$ (cf. [**10**]).

LEMMA 4.5.1. *Let $x \in \mathscr{F}_{ss}(\mathfrak{m}_n)$. The morphisms $P_{n,x}$ are compatible for $n \geq 1$:*

$$\begin{array}{ccc} H^1(k_n, T) & \xrightarrow{P_{n,x}} & \mathbb{Z}_p[\mathcal{G}_n] \\ \downarrow & & \downarrow \\ H^1(k_{n-1}, T) & \xrightarrow{P_{n-1,Nx}} & \mathbb{Z}_p[\mathcal{G}_{n-1}] \end{array}$$

where the vertical maps are the corestriction and the projection.

PROOF. The lemma follows from the definition of $P_{n,x}$ and basic properties of the cup product. □

We define two sequences $(\mathrm{c}_n^+)_{n\geq 1}$, $(\mathrm{c}_n^-)_{n\geq 1}$, $\mathrm{c}_n^+, \mathrm{c}_n^- \in \mathscr{F}_{ss}(\mathfrak{m}_n)$, by

$$\mathrm{c}_n^+ : \mathrm{c}_0,\ \mathrm{c}_2,\ \mathrm{c}_2,\ \mathrm{c}_4,\ \mathrm{c}_4,\ \ldots, \quad \mathrm{c}_n^- : \mathrm{c}_1,\ \mathrm{c}_1,\ \mathrm{c}_3,\ \mathrm{c}_3,\ \mathrm{c}_5,\ \ldots.$$

Namely,

$$\mathrm{c}_n^+ = \begin{cases} \mathrm{c}_n & \text{if } n \text{ is even,} \\ \mathrm{c}_{n-1} & \text{if } n \text{ is odd,} \end{cases} \qquad \mathrm{c}_n^- = \begin{cases} \mathrm{c}_n & \text{if } n \text{ is odd,} \\ \mathrm{c}_{n-1} & \text{if } n \text{ is even.} \end{cases}$$

We put $P_n^\pm = (-1)^{[\frac{n+1}{2}]} P_{n,\mathrm{c}_n^\pm}$.

DEFINITION 4.5.2. *We define the n-th norm subgroup, the n-th plus norm subgroup and the n-th minus norm subgroup of $\hat{E}(\mathfrak{m}_n)$ by*

$$\mathscr{C}_{\hat{E}}(\mathfrak{m}_n) = \{P \in \hat{E}(\mathfrak{m}_n) \mid \mathrm{Tr}_{n/m} P \in \hat{E}(\mathfrak{m}_{m-1}) \text{ for all } m \equiv n-1 \bmod 2\},$$
$$\hat{E}^+(\mathfrak{m}_n) = \{P \in \hat{E}(\mathfrak{m}_n) \mid \mathrm{Tr}_{n/m} P \in \hat{E}(\mathfrak{m}_{m-1}) \text{ for odd } m,\ 1 \leq m \leq n\},$$
$$\hat{E}^-(\mathfrak{m}_n) = \{P \in \hat{E}(\mathfrak{m}_n) \mid \mathrm{Tr}_{n/m} P \in \hat{E}(\mathfrak{m}_{m-1}) \text{ for even } m,\ 1 \leq m \leq n\}$$

where $\mathrm{Tr}_{n/m} : \hat{E}(\mathfrak{m}_n) \to \hat{E}(\mathfrak{m}_m)$ is the trace map of $\hat{E}$.

The relations between the norm subgroups and the plus (minus) norm subgroups are

(4.5.2)

$$\hat{E}^+(\mathfrak{m}_n) = \begin{cases} \mathscr{C}_{\hat{E}}(\mathfrak{m}_n) & \text{if } n \text{ is even,} \\ \mathscr{C}_{\hat{E}}(\mathfrak{m}_{n-1}) & \text{if } n \text{ is odd,} \end{cases} \qquad \hat{E}^-(\mathfrak{m}_n) = \begin{cases} \mathscr{C}_{\hat{E}}(\mathfrak{m}_n) & \text{if } n \text{ is odd,} \\ \mathscr{C}_{\hat{E}}(\mathfrak{m}_{n-1}) & \text{if } n \text{ is even.} \end{cases}$$

DEFINITION 4.5.3. *We define $H^1_\pm(k_n,T)$ as the exact annihilator with respect to the Tate pairing*

$$(\ ,\ )_n :\ H^1(k_n,V/T)\times H^1(k_n,T)\to \mathbb{Q}_p/\mathbb{Z}_p$$

of the n-th plus (minus) norm subgroup $\hat{E}^\pm(\mathfrak{m}_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p\subseteq H^1(k_n,V/T)$.

DEFINITION 4.5.4. *Let $\Phi_n(X)=\sum_{i=0}^{p-1}X^{p^{n-1}i}$ be the p^n-th cyclotomic polynomial and $\Phi_0(X)=1$. We put*

$$\omega_n(X)=(X+1)^{p^n}-1=X\prod_{0\le m\le n,}\Phi_m(X+1),$$

$$\widetilde{\omega}^+_n(X)=\prod_{0\le m\le n,\ m:even}\Phi_m(X+1),\quad \omega^+_n(X)=X\ \widetilde{\omega}^+_n(X),$$

$$\widetilde{\omega}^-_n(X)=\prod_{0\le m\le n,\ m:odd}\Phi_m(X+1),\quad \omega^-_n(X)=X\ \widetilde{\omega}^-_n(X).$$

We use the notation in Section 1 of Chapter 2. For $n\ge 1$, we identify $\Lambda_n=\mathbb{Z}_p[\mathcal{G}_n]=\mathbb{Z}_p[\Delta][\mathcal{G}^1_{n-1}]$ with $\mathbb{Z}_p[\Delta][X]/(\omega_{n-1}(X))$ by sending γ_{n-1} to $1+X$.

PROPOSITION 4.5.5. i) *The kernel of $P^\pm_n$ is $H^1_\pm(k_n,T)$.*
ii) *The image of $P^\pm_n$ is contained in $\widetilde{\omega}^\pm_{n-1}(X)\,\Lambda_n$.*

PROOF. i) follows directly from the definition of $P^\pm_n$ and Proposition 4.4.5 i). We prove ii) for P^+_n. The proposition for P^-_n is proved similarly. We consider a morphism

$$\mathbb{Z}_p[\Delta][X]/(\omega_{n-1}(X))=\mathbb{Z}_p[\mathcal{G}_n]\ \xrightarrow{\Pi\,\psi}\ \textstyle\prod_\psi\ \overline{\mathbb{Q}_p},$$

where $\psi:\mathcal{G}_n\to\overline{\mathbb{Q}_p}^\times$ ranges over all characters of $\mathcal{G}_n$ of conductor p^m with odd m, $1\le m\le n$ (ψ is naturally extended to $\mathbb{Z}_p[\mathcal{G}_n]\to\overline{\mathbb{Q}_p}$). Since $\psi(\gamma_{n-1})$ is a primitive p^{m-1}-th root of unity, the kernel of the above morphism is generated by $\widetilde{\omega}^+_{n-1}(X)$. Hence to prove the Lemma, it suffices to show that $\psi\circ P^+_n=0$ for any character ψ of conductor p^m with odd m.

By Lemma 4.4.1 and Lemma 4.5.1, up to p-power, we have $\psi\circ P^\pm_n=\psi\circ P^\pm_m\circ \mathrm{Cor}_{n/m}$ where $\mathrm{Cor}_{n/m}$ is the corestriction map. Therefore we may assume that $m=n$. Then

$$\psi\circ P^+_n=\sum_{\sigma\in\mathcal{G}_n}(\mathrm{c}^\sigma_{n-1},z)_n\ \psi(\sigma)=\sum_{\sigma\in\mathcal{G}_{n-1}}(\mathrm{c}^\sigma_{n-1},z)_n\sum_{\tau\in\mathcal{G}_n,\,\overline{\tau}\equiv\sigma}\psi(\tau)=0$$

where $\overline{\tau}$ is the image of τ by the natural projection $\mathcal{G}_n\to\mathcal{G}_{n-1}$. □

Since $\omega_{n-1}(X)=\widetilde{\omega}^\pm_{n-1}(X)\ \omega^\mp_{n-1}(X)$, the multiplication by $\widetilde{\omega}^\pm_{n-1}(X)$ induces an isomorphism

$$\Lambda^\mp_n:=\mathbb{Z}_p[\Delta][X]/(\omega^\mp_{n-1}(X))\ \xrightarrow{\simeq}\ \widetilde{\omega}^\pm_{n-1}(X)\,\Lambda_n. \tag{4.5.3}$$

Hence by Proposition 4.5.5, we have

COROLLARY 4.5.6. *There exists a unique morphism $P^{\pm}_{\Lambda,n}$ which makes the following diagram commutative.*

$$\begin{array}{ccc} H^1(k_n,T) & \xrightarrow{P^{\pm}_{\Lambda,n}} & \Lambda_n^{\mp} \\ \downarrow & & \downarrow \times\widetilde{\omega}^{\pm}_{n-1} \\ \dfrac{H^1(k_n,T)}{H^1_{\pm}(k_n,T)} & \xrightarrow{P^{\pm}_n} & \Lambda_n \end{array}$$

DEFINITION 4.5.7. *We call the above $P^{\pm}_{\Lambda,n}$ the n-th plus (minus) Perrin-Riou map.*

PROPOSITION 4.5.8. *The plus (minus) Perrin-Riou maps are compatible for $n \geq 1$:*

$$\begin{array}{ccc} H^1(k_{n+1},T) & \xrightarrow{P^{\pm}_{\Lambda,n+1}} & \Lambda_{n+1}^{\mp} \\ \downarrow & & \downarrow \\ H^1(k_n,T) & \xrightarrow{P^{\pm}_{\Lambda,n}} & \Lambda_n^{\mp} \end{array}$$

where the vertical maps are the corestriction and the projection.

PROOF. We prove the proposition for P^+_n. The proposition for P^-_n is proved similarly. For an odd n, we consider a diagram

$$\begin{array}{ccccc} H^1(k_{n+1},T) & \xrightarrow{P^+_{n+1}} & \widetilde{\omega}^+_n(X)\,\Lambda_{n+1} & \xrightarrow{\simeq} & \Lambda^-_{n+1} \\ \downarrow & & \downarrow \mathrm{proj} & & \downarrow \\ H^1(k_n,T) & \xrightarrow{P^+_n} & \widetilde{\omega}^+_{n-1}(X)\,\Lambda_n & \xrightarrow{\simeq} & \Lambda^-_n \end{array} \tag{4.5.4}$$

where the vertical maps are the corestriction and the projection. By Lemma 4.4.1, Lemma 4.5.1 and $\widetilde{\omega}^+_n(X) = \widetilde{\omega}^+_{n-1}(X)$, the diagram (4.5.4) is commutative. For an even $n \geq 2$, we consider a diagram

$$\begin{array}{ccccc} H^1(k_{n+1},T) & \xrightarrow{P^+_{n+1}} & \widetilde{\omega}^+_n(X)\,\Lambda_{n+1} & \xrightarrow{\simeq} & \Lambda^-_{n+1} \\ \downarrow & & \downarrow \times\frac{1}{p} & & \downarrow \\ H^1(k_n,T) & \xrightarrow{P^+_n} & \widetilde{\omega}^+_{n-1}(X)\,\Lambda_n & \xrightarrow{\simeq} & \Lambda^-_n \end{array} \tag{4.5.5}$$

where the left vertical map is the corestriction and the right vertical map is the projection. Since $\Phi_n(X+1) = \sum_{i=0}^{p-1}(X+1)^{p^{n-1}i} \equiv p$ modulo $\omega_{n-1}(X)$, we have $\widetilde{\omega}^+_n(X) = p\,\widetilde{\omega}^+_{n-1}(X)$ in Λ_n. The commutativity of the right square in the

diagram (4.5.5) follows from this fact. The commutativity of the left square follows from $\mathrm{c}_{n+1}^{+} = \mathrm{c}_n^{+} = \mathrm{c}_n$ and Lemma 4.5.1. □

Let $\mathbf{H}^1_{\mathrm{Iw}}(T) = \varprojlim_n H^1(k_n, T)$, where the limit is taken with respect to the corestrictions. We have $\varprojlim_n \Lambda_n^{\mp} = \varprojlim_n \mathbb{Z}_p[\Delta][X]/(\omega_{n-1}^{\mp}(X)) = \mathbb{Z}_p[\Delta][[X]] = \Lambda$.

Definition 4.5.9. *We define the plus (minus) Perrin-Riou map*

$$P_\Lambda^{\pm} : \mathbf{H}^1_{\mathrm{Iw}}(T) \longrightarrow \Lambda$$

as the limit of the n-th plus (minus) Perrin-Riou map $P^{\pm}_{\Lambda,n} : H^1(k_n, T) \to \Lambda_n^{\mp}$.

Proposition 4.5.10. *The minus Perrin-Riou maps* $P^{-}_{\Lambda,n}$ *and* P^{-}_{Λ} *are surjective.*

Proof. We first show that the transition (corestriction) maps $H^1(k_m, T) \to H^1(k_n, T)$ are surjective for all $m \geq n$. By the Tate duality, it suffices to show the kernel of the restriction map $H^1(k_n, V/T) \to H^1(k_m, V/T)$ is zero. By the restriction-inflation sequence, the kernel is $H^1(G, H^0(k_m, V/T))$, where $G = \mathrm{Gal}(k_m/k_n)$. This group is zero by Proposition 4.3.2.

Next we show that the first minus Perrin-Riou map $P^{-}_{\Lambda,1} = P_1^{-} : H^1(k_1, T) \to \mathbb{Z}_p[\Delta]$ is surjective. Then, by Nakayama's lemma, $P^{-}_{\Lambda,n}$ and P^{-}_{Λ} are surjective.

Since $\log_{\mathscr{F}_{ss}}$ induces a group isomorphism $\mathscr{F}_{ss}(\mathfrak{m}_1) \cong \hat{\mathbb{G}}_a(\mathfrak{m}_1)$, the elements $(\mathrm{c}_1^{\sigma})_{\sigma\in\Delta}$ become a basis of $\mathscr{F}_{ss}(\mathfrak{m}_1)$ as $\mathbb{Z}_p$-module. Then P_1^{-} is described as

$$H^1(k_1, T) \to \mathrm{Hom}(\mathscr{F}_{ss}(\mathfrak{m}_1), \mathbb{Z}_p) \cong \mathbb{Z}_p[\Delta]$$

where the first map is induced by the pairing (4.5.1) and the last identification is $f \mapsto \sum_{\sigma\in\Delta} f(\mathrm{c}_1^{\sigma})\,\sigma$.

Since the cup product induces a non-degenerate pairing

$$(\ ,\ )_{\mathbb{F}_p} : H^1(k_1, E[p]) \times H^1(k_1, E[p]) \to \mathbb{F}_p,$$

the isomorphism $\mathscr{F}_{ss}(\mathfrak{m}_1) \cong \hat{E}(\mathfrak{m}_1)$ and the Kummer map $\hat{E}(\mathfrak{m}_1)/p\hat{E}(\mathfrak{m}_1) \hookrightarrow H^1(k_1, E[p])$ induces a surjection

$$H^1(k_1, E[p]) \to \mathrm{Hom}_{\mathbb{F}_p}(\mathscr{F}_{ss}(\mathfrak{m}_1)/p\mathscr{F}_{ss}(\mathfrak{m}_1), \mathbb{F}_p).$$

Therefore, by Nakayama's lemma, the pairing (4.5.1) induces a surjection

$$H^1(k_1, T) \to \mathrm{Hom}_{\mathbb{Z}_p}(\mathscr{F}_{ss}(\mathfrak{m}_1), \mathbb{Z}_p).$$

□

For the plus Perrin-Riou maps, the situation is different. The reason is the trivial zero phenomena (3.1.4). For characters $\eta : \Delta \to \mathbb{Z}_p^{\times}$, we decompose the plus Perrin-Riou maps to the η-components

$$\epsilon_\eta P^{+}_{\Lambda,n} : H^1(k_n, T)^{\eta} \longrightarrow \epsilon_\eta \Lambda_n^{-}.$$

Let I_n be the augmentation ideal of $\mathbb{Z}_p[\mathcal{G}_n] = \mathbb{Z}_p[\Delta][\mathcal{G}_n^1]$:

$$I_n = \mathrm{Ker}\,(\ \mathbb{Z}_p[\Delta][\mathcal{G}_n^1] \longrightarrow \mathbb{Z}_p[\Delta]\ )$$

where the map is induced by $\mathcal{G}_n^1 \to \{1\}$. We put $I = \varprojlim_n I_n$ and $I_n^{\pm} := I_n\Lambda_n^{\pm} = \mathrm{Ker}\,(\ \Lambda_n^{\pm} \to \mathbb{Z}_p[\Delta],\ X \mapsto 0\ )$.

Proposition 4.5.11. *For the trivial η, the plus Perrin-Riou maps $\epsilon_\eta P^+_{\Lambda,n}$ and $\epsilon_\eta P^+_{\Lambda}$ are surjective. For a non-trivial character η, the image of the Perrin-Riou map $\epsilon_\eta P^+_{\Lambda,n}$ is the augmentation ideal $(I_n^-)^\eta$. The image of $\epsilon_\eta P^+_{\Lambda}$ is I^η.*

Proof. The proof is similar to that of Proposition 4.5.10. The difference is, for the component of a non-trivial η, we have to prove surjectivity of the second Perrin-Riou map

$$\epsilon_\eta P^+_{\Lambda,2} : H^1(k_2, T)^\eta \longrightarrow (\Lambda_2^-)^\eta$$

to the augmentation ideal. It is easy to see that $\Lambda_2^- = \Lambda_2$ and $P^+_{\Lambda,2} = P_2^+$.

We put $d_\sigma = \epsilon_\eta\, \mathrm{c}_2^\sigma$. Then $d_{\sigma\tau} = \eta(\tau)\, d_\sigma$ for $\tau \in \Delta$ and $\sum_{\sigma\in\mathcal{G}_1^1} d_\sigma = 0$ by Lemma 4.4.1. Therefore by Proposition 4.4.5 i) and Proposition 4.4.6 i), $(d_\sigma)_{\sigma\in\mathcal{G}_1^1,\,\sigma\neq 1}$ becomes a basis of $\mathscr{C}_{ss}(\mathfrak{m}_2)^\eta$. Hence we have an isomorphism

$$\mathrm{Hom}(\mathscr{C}_{ss}(\mathfrak{m}_2)^\eta, \mathbb{Z}_p) \cong I_2^\eta, \quad f \mapsto \sum_{\sigma\in\mathcal{G}_1^1} f(d_\sigma)\,\sigma.$$

Then the morphism $\epsilon_\eta P^+_{\Lambda,2} = \epsilon_\eta P_{2,\,\mathrm{c}_2}$ is described as

$$H^1(k_2, T)^\eta \to \mathrm{Hom}(\mathscr{F}_{ss}(\mathfrak{m}_2)^\eta, \mathbb{Z}_p) \to \mathrm{Hom}(\mathscr{C}_{ss}(\mathfrak{m}_2)^\eta, \mathbb{Z}_p) \cong I_2^\eta$$

where the first map is induced by the pairing (4.5.1) and the second map is the projection induced by the decomposition $\mathscr{F}_{ss}(\mathfrak{m}_2)^\eta = \mathscr{C}_{ss}(\mathfrak{m}_2)^\eta \oplus \mathscr{C}_{ss}(\mathfrak{m}_1)^\eta$ (cf. Proposition 4.4.5). The surjectivity of $H^1(k_2, T)^\eta \to \mathrm{Hom}(\mathscr{F}_{ss}(\mathfrak{m}_2)^\eta, \mathbb{Z}_p)$ is proved as in the proof of Proposition 4.5.10. □

Hence, by Proposition 4.5.5, Proposition 4.5.10 and Proposition 4.5.11, we have

Theorem 4.5.12. *The plus (minus) Perrin-Riou maps induce isomorphisms*

$$P^-_{\Lambda,n} : H^1(k_n, T)/H^1_-(k_n, T) \cong \Lambda_n^+, \tag{4.5.6}$$

$$\epsilon_1 P^+_{\Lambda,n} : H^1(k_n, T)^\Delta/H^1_+(k_n, T)^\Delta \cong (\Lambda_n^-)^\Delta, \tag{4.5.7}$$

$$\epsilon_\eta P^+_{\Lambda,n} : H^1(k_n, T)^\eta/H^1_+(k_n, T)^\eta \cong (I_n^-)^\eta \quad \textit{for } \eta \neq 1. \tag{4.5.8}$$

If we put $\mathbf{H}^1_{\mathrm{Iw},\pm}(T) = \varprojlim_n H^1_\pm(k_n, T)$, then the above isomorphisms induce isomorphisms

$$P^-_{\Lambda} : \mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},-}(T) \cong \Lambda, \tag{4.5.9}$$

$$\epsilon_1 P^+_\Lambda : \mathbf{H}^1_{\mathrm{Iw}}(T)^\Delta/\mathbf{H}^1_{\mathrm{Iw},+}(T)^\Delta \cong \Lambda^\Delta, \tag{4.5.10}$$

$$\epsilon_\eta P^+_\Lambda : \mathbf{H}^1_{\mathrm{Iw}}(T)^\eta/\mathbf{H}^1_{\mathrm{Iw},+}(T)^\eta \cong I^\eta \quad \textit{for } \eta \neq 1. \tag{4.5.11}$$

6. Perrin-Riou maps in terms of the dual exponential maps

In the next chapter (Theorem 5.2.5), we compute the image of Kato's zeta element by the plus (minus) Perrin-Riou map. For this purpose, we give a description of Perrin-Riou maps in terms of the dual exponential map of E. Then it turns out that our Perrin-Riou maps are similar objects with the explicit Coleman map in the appendix in Rubin [**24**]. It also turns out that our $P_{n,\,x}$ is Kurihara's $z \mapsto p^n P_n(x,z)$ (Kurihara [**10**], Section 3).

We first fix notations, and recall the dual exponential map and its basic properties. We follow Rubin [**24**, Section 5].

For every n let $\tan(E/k_n)$ denote the tangent space of E/k_n at the origin and consider the Lie group exponential map

$$\exp_E : \tan(E/k_n) \to E(k_n) \otimes \mathbb{Q}_p.$$

Fix a minimal Weierstrass model of E and let ω_E denote the Néron differential. Then the cotangent space $\mathrm{cotan}(E/k_n)$ is $k_n\omega_E$, and we let ω_E^* be the corresponding dual basis of $\tan(E/k_n)$. We have a commutative diagram

$$\begin{array}{ccccc}
\log_{\mathscr{F}_{ss}}(\mathfrak{m}_n) & \xleftarrow{\log_{\mathscr{F}_{ss}}} & \mathscr{F}_{ss}(\mathfrak{m}_n) & & \\
\| & & \downarrow{\scriptstyle \exp_{\hat{E}}\circ\log_{\mathscr{F}_{ss}}} & & \\
\log_{\hat{E}}(\mathfrak{m}_n) & \xleftarrow{\log_{\hat{E}}} & \hat{E}(\mathfrak{m}_n) & \longrightarrow & E_1(k_n) \\
{\scriptstyle \cdot\omega_E^*}\downarrow & & & & \downarrow \\
\tan(E/k_n) & & \xrightarrow{\exp_E} & & E(k_n)\otimes\mathbb{Q}_p
\end{array} \tag{4.6.1}$$

There is a dual exponential map

$$\exp^*_E : H^1(k_n, V) \longrightarrow \mathrm{cotan}(E/k_n) = k_n\,\omega_E$$

which has a property

$$(x,z)_n = \mathrm{Tr}_{k_n/\mathbb{Q}_p}\, \log_{\hat{E}}(x)\, \exp^*_{\omega_E}(z) \tag{4.6.2}$$

for every $x \in \hat{E}(\mathfrak{m}_n)$ and $z \in H^1(k_n, V)$. Here $(\ ,\ )_n$ is the local Tate pairing and $\exp^*_{\omega_E} = \omega_E^* \circ \exp^*_E$. (cf. Formula (2) in Rubin [**24**, Section 5].)

PROPOSITION 4.6.1. *The map $P_{n,x}$ in Section 5 is described in terms of the dual exponential map as follows.*

$$\begin{aligned} P_{n,x}(z) &= \sum_{\sigma\in\mathcal{G}_n} (x^\sigma, z)_n\, \sigma \\ &= \sum_{\sigma\in\mathcal{G}_n} (\,\mathrm{Tr}_{k_n/\mathbb{Q}_p} \log_{\mathscr{F}_{ss}}(x^\sigma)\, \exp^*_{\omega_E}(z)\,)\,\sigma \\ &= (\sum_{\sigma\in\mathcal{G}_n} \log_{\mathscr{F}_{ss}}(x^\sigma)\,\sigma)\,(\sum_{\sigma\in\mathcal{G}_n} \exp^*_{\omega_E}(z^\sigma)\,\sigma^{-1}). \end{aligned}$$

PROOF. The formula follows from the diagram (4.6.1) and the formula (4.6.2). See also the appendix of Rubin [**24**]. □

PROPOSITION 4.6.2. *Let ψ be a character of $\mathcal{G}_n$ of conductor p^m. Then for $n \geq 1$, we have*

$$\frac{1}{p^{[\frac{n-1}{2}]}} \sum_{\sigma\in\mathcal{G}_n} \log_{\mathscr{F}_{ss}}(\mathrm{c}_n^+)^\sigma\, \psi(\sigma) = \begin{cases} (-1)^{\frac{m}{2}} p^{-[\frac{m-1}{2}]}\, \tau(\psi) & \text{if } m \text{ is even} > 0, \\ 0 & \text{if } m \text{ is odd}, \\ \frac{p(p-1)}{p+1} & \text{if } \psi = 1. \end{cases}$$

Similarly,

$$\frac{1}{p^{[\frac{n}{2}]}} \sum_{\sigma\in\mathcal{G}_n} \log_{\mathscr{F}_{ss}}(\mathrm{c}_n^-)^\sigma\, \psi(\sigma) = \begin{cases} (-1)^{\frac{m+1}{2}} p^{-[\frac{m}{2}]}\, \tau(\psi) & \text{if } m \text{ is odd}, \\ 0 & \text{if } m \text{ is even} > 0, \\ \frac{2p}{p+1} & \text{if } \psi = 1. \end{cases}$$

where $\tau(\psi)$ is the Gauss sum $\sum_{\sigma\in\mathcal{G}_n} \psi(\sigma)\, \zeta_{p^m}^\sigma$.

PROOF. If $m \geq 1$, by the norm compatibility of $p^{-[\frac{n-1}{2}]} \log_{\mathscr{F}_{ss}}(\mathrm{c}_n^+)$ and $p^{-[\frac{n}{2}]} \log_{\mathscr{F}_{ss}}(\mathrm{c}_n^-)$, we may assume that $m = n$. Then the formula is obtained by direct calculations as in the proof of Lemma 4.4.1 and Proposition 4.5.5. If $\psi = 1$, we may assume that $n = 1$. Then we have $\sum_{\sigma\in\mathcal{G}_1} \log_{\mathscr{F}_{ss}}(\mathrm{c}_0) = \frac{p(p-1)}{p+1}$ and $\sum_{\sigma\in\mathcal{G}_1} \log_{\mathscr{F}_{ss}}(\mathrm{c}_1)^\sigma = \log_{\mathscr{F}_{ss}}(\mathrm{c}_{-1}) = \frac{2p}{p+1}$ by Lemma 4.4.1. □

CHAPTER 5

The plus (minus) Selmer group

We define the plus (minus) Selmer group. This Selmer group is Λ-cotorsion and has a certain control theorem. The characteristic ideal of the Pontryagin dual of this Selmer group is conjectured to be generated by Pollack's p-adic L-function (main conjecture). By using Kato's Euler system, we prove a half of this conjecture, that is, the characteristic ideal contains Pollack's p-adic L-function.

In this chapter, if not otherwise specified, we assume that p is odd and E is an elliptic curve over $\mathbb{Q}$ with good reduction at p and $a_p = 0$.

1. The definition of $\mathrm{Sel}^+(E/K_n)$ and $\mathrm{Sel}^-(E/K_n)$

We use the notation in Chapter 2, Section 1.

Definition 5.1.1. *We define the Selmer group by*

$$\mathrm{Sel}(E/K_n) := \mathrm{Ker}\left(H^1(K_n, E[p^\infty]) \longrightarrow \prod_v \frac{H^1(K_{n,v}, E[p^\infty])}{E(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

where v ranges over all places of K_n and the map is induced by the restrictions of the Galois cohomology groups. Let $\mathrm{Sel}(E/K_\infty) := \varinjlim_n \mathrm{Sel}(E/K_n)$.

Definition 5.1.2. *We define the n-th plus (minus) norm subgroup by*

$$E^+(K_{n,v}) = \{P \in E(K_{n,v}) \mid \mathrm{Tr}_{n/m} P \in E(K_{m-1,v}) \text{ for odd } m \leq n\},$$
$$E^-(K_{n,v}) = \{P \in E(K_{n,v}) \mid \mathrm{Tr}_{n/m} P \in E(K_{m-1,v}) \text{ for even } m \leq n\}.$$

where $\mathrm{Tr}_{n/m} : E(K_{n,v}) \to E(K_{m,v})$ is the trace map.

(cf. Definition 4.5.2.)

Definition 5.1.3. *We define the plus (minus) Selmer group by*

$$\mathrm{Sel}^\pm(E/K_n) := \mathrm{Ker}\left(H^1(K_n, E[p^\infty]) \longrightarrow \prod_v \frac{H^1(K_{n,v}, E[p^\infty])}{E^\pm(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right).$$

We remark that $E(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = E^\pm(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ if $v \nmid p$.

Let

$$\mathrm{Sel}^+(E/K_\infty) := \varinjlim_n \mathrm{Sel}^+(E/K_n),$$
$$\mathrm{Sel}^-(E/K_\infty) := \varinjlim_n \mathrm{Sel}^-(E/K_n).$$

Following Kurihara [**10**], we define the zero Selmer group.

Definition 5.1.4. *We define the zero Selmer group by*

$$\mathrm{Sel}_0(E/K_n) := \mathrm{Ker}\left(H^1(K_n, E[p^\infty]) \longrightarrow \prod_v H^1(K_{n,v}, E[p^\infty]) \right).$$

Let $\mathrm{Sel}_0(E/K_\infty) := \varinjlim_n \mathrm{Sel}_0(E/K_n)$.

We denote the Pontryagin dual of Selmer groups by "$\mathscr{X}$". For example, $\mathscr{X}(E/K_n)$ is the dual of $\mathrm{Sel}(E/K_n)$ and $\mathscr{X}^\pm(E/K_\infty)$ is the dual of $\mathrm{Sel}^\pm(E/K_\infty)$.

2. Λ-cotorsionness of the plus (minus) Selmer group

We first fix notations. Let T be the p-adic Tate module of E and $V = T \otimes \mathbb{Q}$. Let S be a finite set of primes containing all bad primes of E and the archimedean places. We denote the integral closure of $\mathbb{Z}[1/S]$ in K_n by $O_{K_n}[1/S]$, and we put $G_{K_n,S} = \mathrm{Gal}(K_{n,S}/K_n)$ where $K_{n,S}$ is the maximal unramified extension of K_n outside S. Let $H^q(O_{K_n}[1/S], T)$ be the étale cohomology group or equivalently, the Galois cohomology group $H^q(G_{K_n,S}, T)$.

We define

$$\mathbf{H}^q_S(T) := \varprojlim_n H^q(O_{K_n}[1/S], T)$$

where the limit is taken with respect to the corestrictions.

We define

$$\mathbf{H}^q_{\mathrm{Iw},v}(T) := \varprojlim_n H^q(K_{n,v}, T)$$

and

$$\mathbf{H}^q_{\mathrm{Iw},S}(T) := \oplus_{v\in S} \mathbf{H}^q_{\mathrm{Iw},v}(T),$$

where the limit is taken with respect to the corestrictions and the sum is taken over the places of K_∞ over S. For the place v over p, we put $\mathbf{H}^q_{\mathrm{Iw},v}(T) = \mathbf{H}^q_{\mathrm{Iw}}(T)$.

We consider the Tate-Poitou exact sequence of O_{K_n}-modules

$$H^1(O_{K_n}[1/S], T) \to \oplus_{v\in S} H^1(K_{n,v}, T) \to H^1(O_{K_n}[1/S],\, V/T)^\vee$$
$$\to H^2(O_{K_n}[1/S], T) \to \oplus_{v\in S} H^2(K_{n,v}, T).$$

(cf. Perrin-Riou [**19**], Appendix A.3.)

We have $E(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ for the places v not lying above p. The exact annihilator of $E(k_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ with respect to the local Tate pairing is $E(k_n)$.

The exact annihilator of $E^{\pm}(k_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is $H^1_{\pm}(k_n, T)$ (cf. Definition 4.5.3). Hence from the Tate-Poitou exact sequence, we deduce three exact sequences

$$0 \to \mathscr{X}_0(E/K_n) \to H^2(O_{K_n}[1/S], T) \to \oplus_{v \in S} H^2(K_{n,v}, T), \tag{5.2.1}$$

(5.2.2)
$$H^1(O_{K_n}[1/S], T) \to H^1(k_n, T)/H^1_{\pm}(k_n, T) \to \mathscr{X}^{\pm}(E/K_n) \to \mathscr{X}_0(E/K_n) \to 0,$$

(5.2.3)
$$H^1(O_{K_n}[1/S], T) \to H^1(k_n, T)/E(k_n) \to \mathscr{X}(E/K_n) \to \mathscr{X}_0(E/K_n) \to 0.$$

(cf. Kurihara [**10**] or Perrin-Riou [**19**], Appendix A.3.2.)

Taking the limit of the above three exact sequences, we get

$$0 \to \mathscr{X}_0(E/K_\infty) \to \mathbf{H}^2_S(T) \to \mathbf{H}^2_{\mathrm{Iw},S}(T), \tag{5.2.4}$$

$$\mathbf{H}^1_S(T) \to \mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},\pm}(T) \to \mathscr{X}^{\pm}(E/K_\infty) \to \mathscr{X}_0(E/K_\infty) \to 0, \tag{5.2.5}$$

$$\mathbf{H}^1_S(T) \to \mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},f}(T) \to \mathscr{X}(E/K_\infty) \to \mathscr{X}_0(E/K_\infty) \to 0, \tag{5.2.6}$$

where $\mathbf{H}^1_{\mathrm{Iw},\pm}(T) = \varprojlim_n H^1_{\pm}(k_n, T)$ and $\mathbf{H}^1_{\mathrm{Iw},f}(T) = \varprojlim_n E(k_n)$.

The most crucial difference between the good ordinary case and the good supersingular case is the structure of the universal norm group $\mathbf{H}^1_{\mathrm{Iw},f}(T)$. In the good ordinary case, $\mathbf{H}^1_{\mathrm{Iw},f}(T)$ has Λ-rank 1, and by the Perrin-Riou map or so called the Coleman map, $\mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},f}(T)$ is pseudo-isomorphic to Λ. On the other hand, in the good supersingular case, the universal norm group is equal to zero, and $\mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},f}(T) = \mathbf{H}^1_{\mathrm{Iw}}(T)$ has Λ-rank 2. This is the reason that the usual Selmer group is not Λ-cotorsion (Λ-rank 1). Since our plus (minus) Selmer group is constructed to have the property that $\mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},\pm}(T)$ is isomorphic to Λ (or its augmentation ideal) by the plus (minus) Perrin-Riou map, we can treat the good supersingular case as in the good ordinary case.

Now we recall Kato's result (the CM case is essentially due to Rubin). Here we do not need to assume anything about the reduction type of E at p. (For simplicity, in Theorem 5.2.2 iii), we assume that E has good reduction at p.)

Let j be the natural inclusion $\operatorname{Spec} O_{K_n}[1/S] \to \operatorname{Spec} O_{K_n}[1/p]$. We put

$$\mathbf{H}^q_p(T) = \varprojlim_n H^q(\operatorname{Spec} O_{K_n}[1/p], j_*T)$$

where $H^q(\operatorname{Spec} O_{K_n}[1/p], j_*T)$ is the étale cohomology group.

THEOREM 5.2.1 (Kato [**8**], Theorem 12.4). i) $\mathbf{H}^2_p(T)$ *is a torsion* Λ*-module.*
ii) $\mathbf{H}^1_p(T)$ *is a torsion free* Λ*-module, and* $\mathbf{H}^1_p(V) := \mathbf{H}^1_p(T) \otimes \mathbb{Q}$ *is a free* $\Lambda \otimes \mathbb{Q}$*-module of rank* 1*.*
iii) *If* $p \neq 2$ *and if* T/pT *is irreducible as a two dimensional representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *over* $\mathbb{F}_p$*, then* $\mathbf{H}^1_p(T)$ *is a free* Λ*-module of rank* 1*.*

THEOREM 5.2.2 (Kato [**8**], Theorem 12.5). i) *There exist two systems of elements,*

$$\mathbf{z}^{\pm} = (z_n^{\pm})_n \in \mathbf{H}^1_p(V), \;\; z_n^{\pm} \in H^1(O_{K_n}[1/p], T) \otimes \mathbb{Q}$$

such that for a character ψ *of* $\mathcal{G}_n$ *of conductor* p^n*, we have*

$$\sum_{\sigma \in \mathcal{G}_n} \psi(\sigma) \exp^*_{\omega_E}(\sigma(z_n^{\pm})) = \delta \left(1 - a_p \, \psi(p) \, p^{-1} + \psi(p)^2 \, p^{-1}\right) \frac{L(E, \psi, 1)}{\Omega_E^{\pm}}$$

where $\delta = 1$ *if* $\psi(-1)$ *is equal to the sign of* $z_n^{\pm}$ *and otherwise* $\delta = 0$*.*
ii) *Let* $\mathbf{Z}_p(V)$ *be the* $\Lambda \otimes \mathbb{Q}$*-submodule of* $\mathbf{H}^1_p(V)$ *generated by* $\mathbf{z}^+$ *and* $\mathbf{z}^-$*. Then* $\mathbf{H}^1_p(V)/\mathbf{Z}_p(V)$ *is a torsion* $\Lambda \otimes \mathbb{Q}$*-module.*
iii) *Let* $\eta : \Delta \to \mathbb{Z}_p^{\times}$ *be a character. Suppose that* E *has good reduction at* p*. Then*

$$\mathrm{Char}\left(\mathbf{H}^2_p(V)^{\eta}\right) \supseteq \mathrm{Char}\left(\mathbf{H}^1_p(V)^{\eta}/\mathbf{Z}_p(V)^{\eta}\right).$$

iv) *Let* $\mathbf{Z}_p(T)$ *be the* Λ*-submodule of* $\mathbf{H}^1(V)$ *generated by* $\mathbf{z}^+$ *and* $\mathbf{z}^-$*. Suppose that* $p \neq 2$ *and* T/pT *is irreducible as a two dimensional representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *over* $\mathbb{F}_p$*. Then*

$$\mathbf{Z}_p(T) \subseteq \mathbf{H}^1_p(T) \quad \textit{in} \quad \mathbf{H}^1_p(T) \otimes \mathbb{Q}.$$

v) *Suppose that* $p \neq 2$ *and that the homomorphism*

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_{\mathbb{Z}_p}(T)$$

is surjective. Then,

$$\mathrm{Char}\left(\mathbf{H}^2_p(T)^{\eta}\right) \supseteq \mathrm{Char}\left(\mathbf{H}^1_p(T)^{\eta}/\mathbf{Z}_p(T)^{\eta}\right).$$

REMARK 2.1. i) Since we assume that E has supersingular reduction at p, the condition in Theorem 5.2.1 iii) and Theorem 5.2.2 iv) is satisfied.
ii) The signs in Theorem 5.2.2 i) are related with the action of the complex conjugate on the homology group of E, and there are no connections with the signs of plus (minus) Selmer groups or Perrin-Riou maps.
iii) In Theorem 5.2.2 iv), we have to fix a good modular parametrization. Then Theorem 5.2.2 iv) follows from Kato [**8**], Theorem 12.6. See also Section 13.14 of [**8**]. We remark that if $p \neq 2$ and T/pT is irreducible, T and $V_{\mathbb{Z}_p}(f)$ (cf. [**8**, Section 8.3]) differ by an element of $\mathbb{Z}_p^{\times}$. We also use the fact that the Manin constant for an optimal parametrization is a p-adic unit (cf. Greenberg-Vatsal [**4**]).

iv) If E has no complex multiplication, then by the result of Serre [**25**], the condition in Theorem 5.2.2 v) is satisfied for almost all p.

PROPOSITION 5.2.3 (Kurihara). i) $\mathbf{H}^1_S(T)$ *is isomorphic to* $\mathbf{H}^1_p(T)$.
ii) $\mathbf{H}^2_p(T)$ *is isomorphic to* $\mathscr{X}_0(E/K_\infty)$ *as* Λ*-module.*

PROOF. The proposition is due to Kurihara [**10**]. We recall his proof. We put $S' = S \setminus \{p\}$, and denote by S'_n the primes of K_n lying over S'. From the localization sequence of étale cohomology groups, we have an exact sequence

$$\begin{aligned} 0 \to & H^1(O_{K_n}[1/p], j_*T) \to H^1(O_{K_n}[1/S], T) \to \oplus_{v\in S'_n} H^0(k(v), H^1(I_{n,v}, T)) \\ & \to H^2(O_{K_n}[1/p], j_*T) \to H^2(O_{K_n}[1/S], T) \to \oplus_{v\in S'_n} H^2(K_{n,v}, T) \end{aligned}$$

where $k(v)$ is the residue field of v and $I_{n,v}$ is the inertia subgroup of the Galois group $\mathrm{Gal}(\overline{K_{n,v}}/K_{n,v})$. Since $\varprojlim_n H^0(k(v), H^1(I_{n,v}, T)) = 0$, we have the assertion i) and

$$0 \to \mathbf{H}^2_p(T) \to \mathbf{H}^2_S(T) \to \mathbf{H}^2_{\mathrm{Iw}, S-\{p\}}(T).$$

Hence, by the exact sequence (5.2.4), we have an injection $\mathbf{H}^2_p(T)/\mathscr{X}_0(E/K_\infty) \hookrightarrow \mathbf{H}^2_{\mathrm{Iw}}(T)$. However, since $E(k_\infty)_{p^\infty} = 0$ by Proposition 4.3.2, we have $\mathbf{H}^2_{\mathrm{Iw}}(T) = 0$ by the local Tate duality. □

COROLLARY 5.2.4. $\mathscr{X}_0(E/K_\infty)$ *is a torsion* Λ*-module.*

PROOF. This follows Theorem 5.2.1 and Proposition 5.2.3. □

By Proposition 5.2.3 i), we put $\mathbf{H}^1(T) = \mathbf{H}^1_S(T) = \mathbf{H}^1_p(T)$.

THEOREM 5.2.5. *Let* $\eta : \Delta \to \mathbb{Z}_p^\times$ *be a character. Let* $\mathbf{z}^\pm \in \mathbf{H}^1(T)$ *be Kato's zeta element in Theorem 5.2.2. By the localization map, we regard* $\mathbf{z}^\pm$ *as an element of* $\mathbf{H}^1_{\mathrm{Iw}}(T)$. *Then, the image of the zeta element by the plus (minus) Perrin-Riou map is Pollack's plus (minus) p-adic L-function*:

$$\epsilon_\eta \, P^\pm_\Lambda (\, \mathbf{z}^{\eta(-1)} \,) \; = \; \eta(-1) \, \mathscr{L}^\pm_p(E, \eta, X).$$

PROOF. Since the both power series in the theorem have the coefficients in $\mathbb{Z}_p$, it suffices to show that the power series in the left hand side have the same interpolation properties (3.1.1) and (3.1.2) of Pollack's plus (minus) p-adic L-function.

Let $\chi : \mathcal{G}_n \to \mu_{p^\infty}$ be a Dirichlet character of conductor $p^n \neq 1$. We put $\psi = \eta\chi$. Suppose n is even. Then by the construction, we have $\psi \circ P^+_n = \widetilde{\omega}^+_{n-1}(\zeta - 1) \, \pi_\psi \circ P^+_{\Lambda,n}$ where $\chi(\gamma_{n-1}) = \zeta$ and $\pi_\psi : \Lambda^\mp_n \to \overline{\mathbb{Q}_p}$, $X \mapsto \zeta$. Hence by the description of P^+_n in terms of the dual exponential map (Proposition 4.6.1 and Proposition 4.6.2) and by Kato's result Theorem 5.2.2, $\epsilon_\eta \, P^+_\Lambda (\, \mathbf{z}^{\eta(-1)} \,)$ has the same interpolation properties as the Pollack's plus p-adic L-function. We remark that $\tau(\psi) \, \tau(\overline{\psi}) = \psi(-1) \, p^n$. The formula for the minus Perrin-Riou map is shown similarly by considering odd n. □

The above theorem gives another construction of Pollack's (and the usual) p-adic L-function of E.

THEOREM 5.2.6. i) *we have an exact sequence*

(5.2.7)
$$0 \to \mathbf{H}^1(T) \to \mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},\pm}(T) \to \mathscr{X}^{\pm}(E/K_\infty) \to \mathscr{X}_0(E/K_\infty) \to 0.$$

ii) *The plus (minus) Selmer group* $\mathrm{Sel}^{\pm}(E/K_\infty)$ *is* Λ*-cotorsion.*

PROOF. The exact sequence is the exact sequence (5.2.5) except the injectivity of $\mathbf{H}^1(T) \to \mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},\pm}(T)$. Since $\mathbf{H}^1(T)$ is a free Λ-module of rank 1 by Theorem 5.2.1 iii) and $\mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},\pm}(T) \hookrightarrow \Lambda$ by Theorem 4.5.12, the morphism $\mathbf{H}^1(T) \to \mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},\pm}(T)$ is injective if and only if this is non-zero map. However, the image of the zeta elements in $\mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},\pm}(T) \hookrightarrow \Lambda$ is non-zero by Theorem 5.2.5 and Rohrlich's theorem [**22**].

For ii), by Theorem 5.2.5, the η-component of the cokernel of the morphism $\mathbf{H}^1(T) \to \mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},\pm}(T)$ is killed by Pollack's p-adic L-function $\mathscr{L}_p^{\pm}(E,\eta,X)$. Since $\mathscr{L}_p^{\pm}(E,\eta,X) \neq 0$ by Rohrlich's theorem, the cokernel is Λ-torsion. Since $\mathscr{X}_0(E/K_\infty)$ is Λ-torsion by Corollary 5.2.4, ii) follows from the exact sequence (5.2.7). □

3. Main conjecture

In the classical Iwasawa theory, there are two types of formulations of Iwasawa main conjecture. Roughly speaking, one is that the characteristic ideal of the minus part of the ideal class group is generated by the Kubota-Leopoldt p-adic L-function. We call this type of the formulation the first type. The other is that the characteristic ideal of the plus part of the ideal class group is equal to the characteristic ideal of the group of the global units modulo the cyclotomic units. In [**7**] (Section 3.2 of Chapter 1), Kato generalized the second type of the formulation to main conjecture of motives (see also Perrin-Riou [**19**], 4.4). For elliptic curves, his conjecture is specified to the following (Kato [**8**], 12.9).

CONJECTURE (Kato's main conjecture). *Let* $\eta : \Delta \to \mathbb{Z}_p^{\times}$ *be a character. Then,* $\mathbf{Z}_p(T)^{\eta} \subseteq \mathbf{H}^1_p(T)^{\eta}$ *and*

$$\mathrm{Char}\,(\,\mathbf{H}^2_p(T)^{\eta}\,) \;=\; \mathrm{Char}\,(\,\mathbf{H}^1_p(T)^{\eta}/\mathbf{Z}_p(T)^{\eta}\,).$$

A half of the conjecture is proved in Theorem 5.2.2 v). Kurihara formulate main conjecture by replacing the left hand side of Kato's main conjecture by $\mathrm{Char}\,(\mathscr{X}_0(E/K_\infty)^{\eta})$ (cf. Proposition 5.2.3).

For elliptic curves with good ordinary reduction at p, Mazur formulated main conjecture of the first type similarly as in the classical case (cf. Chapter 2). Perrin-Riou [**17**] formulated main conjecture of the first type for elliptic

curves with good supersingular reduction at p, and generalized it to motives ([**19**], 4.2). However, in general, if they existed, p-adic L-functions would have huge denominators and would be no longer in Λ, and Selmer groups would be also no longer Λ-cotorsion. Hence, the formulation of the first type should be complicated even in the case of the elliptic curves with good supersingular reduction. In fact, Perrin-Riou's formulation is not just like the form as in the classical case or Mazur's formulation.

However, in the case of $a_p = 0$, we can propose another formulation of main conjecture of the first type using Pollack's p-adic L-function and the plus (minus) Selmer group. This formulation goes along with the classical case or Mazur's formulation in the good ordinary case.

Conjecture (Plus main conjecture). *Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character. For the trivial η, we have*

$$\mathrm{Char}\,(\mathscr{X}^+(E/K_\infty)^\Delta) \;=\; (\,\mathscr{L}_p^+(E,X)\,).$$

For a non-trivial η, we have

$$\mathrm{Char}\,(\mathscr{X}^+(E/K_\infty)^\eta) \;=\; (\,\frac{1}{X}\mathscr{L}_p^+(E,\eta,X)\,).$$

We remark that for a non-trivial η, Pollack's p-adic L-function $\mathscr{L}_p^+(E,\eta,X)$ has a trivial zero at "$X = 0$" (cf. Chapter 3).

Conjecture (Minus main conjecture). *Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character. We have*

$$\mathrm{Char}\,(\mathscr{X}^-(E/K_\infty)^\eta) \;=\; (\,\mathscr{L}_p^-(E,\eta,X)\,).$$

We study the relation with our conjectures and Kato's main conjecture.

Theorem 5.3.1. *The three conjectures, Kato's main conjecture, the plus main conjecture and the minus main conjecture are equivalent.*

Proof. By Theorem 4.5.12, Theorem 5.2.5 and the exact sequence (5.2.7), we have three exact sequences

$$0 \to \mathbf{H}^1_p(T)^\Delta/\mathbf{Z}_p(T)^\Delta \to \Lambda^\Delta/(\mathscr{L}_p^+(E,X)) \to \mathscr{X}^+(E/K_\infty)^\Delta \to \mathscr{X}_0(E/K_\infty)^\Delta \to 0,$$

$$0 \to \mathbf{H}^1_p(T)^\eta/\mathbf{Z}_p(T)^\eta \to I^\eta/(\mathscr{L}_p^+(E,\eta,X)) \to \mathscr{X}^+(E/K_\infty)^\eta \to \mathscr{X}_0(E/K_\infty)^\eta \to 0,$$

$$0 \to \mathbf{H}^1_p(T)^\eta/\mathbf{Z}_p(T)^\eta \to \Lambda^\eta/(\mathscr{L}_p^-(E,\eta,X)) \to \mathscr{X}^-(E/K_\infty)^\eta \to \mathscr{X}_0(E/K_\infty)^\eta \to 0.$$

The middle sequence is for a non-trivial η. The theorem follows from the above exact sequences. □

THEOREM 5.3.2. *There exists an integer $n \geq 0$ such that*

$$\begin{aligned}
&\mathrm{Char}\,(\mathscr{X}^+(E/K_\infty)^\Delta) \supseteq (p^n\,\mathscr{L}_p^+(E,X)),\\
&\mathrm{Char}\,(\mathscr{X}^+(E/K_\infty)^\eta) \supseteq (\frac{p^n}{X}\,\mathscr{L}_p^+(E,\eta,X)) \quad \textit{for } \eta \neq 1,\\
&\mathrm{Char}\,(\mathscr{X}^-(E/K_\infty)^\eta) \supseteq (p^n\,\mathscr{L}_p^-(E,\eta,X)).
\end{aligned}$$

If the assumption in Theorem 5.2.2 v) is satisfied, then we can take $n = 0$.

PROOF. The theorem follows from Theorem 5.2.2 and the exact sequences in the proof of Theorem 5.3.1. □

4. The plus (minus) control theorem

In the good supersingular case, the control theorem for the usual Selmer group always breaks. For our plus (minus) Selmer group, considering the local structure at p (cf. in Theorem 4.5.12, the group $\Lambda_n^\pm$ appears instead of Λ_n), we have a weaker control theorem.

PROPOSITION 5.4.1. *The natural maps*

$$\mathrm{Sel}^\pm(E/K_n) \to \mathrm{Sel}^\pm(E/K_\infty)^{\Gamma_n}$$

are injective. Here $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$.

PROOF. By definition, the n-th plus (minus) Selmer group is a subgroup of $H^1(K_n, V/T)$. Hence it suffices to show that $H^1(K_n, V/T) \to H^1(K_\infty, V/T)^{\Gamma_n}$ is injective (in fact, bijective). By the restriction-inflation sequence, the kernel is $H^1(\mathcal{G}_n, E(K_n)_{p^\infty})$ and the cokernel is contained in $H^2(\mathcal{G}_n, E(K_n)_{p^\infty})$. However, $E(K_\infty)_{p^\infty}$ is zero by Proposition 4.3.2. □

In the good ordinary case, to prove the control theorem, the non-triviality of the universal norm group is crucial, which is zero in the good supersingular case. The following proposition says that the universal norm group for our local condition is non-trivial.

PROPOSITION 5.4.2. *The natural maps*

$$\varprojlim_m H^1_\pm(k_m, T) \to H^1_\pm(k_n, T)/\omega_{n-1}^\mp(\gamma)H^1(k_n, T)$$

are surjective.

PROOF. We put $H^1_{\pm,n} = H^1_{\pm}(k_n, T)$ for simplicity. We first remark that $\omega^{\mp}_{n-1}(\gamma)\, H^1(k_n, T) \subset H^1_{\pm,n}$ since $H^1(k_n, T)/H^1_{\pm,n} \hookrightarrow \Lambda/(\omega^{\mp}_{n-1}(X))$ by Theorem 4.5.12. We consider a commutative diagram

$$\begin{array}{ccccccc} & & \dfrac{\varprojlim_m H^1_{\pm,m}}{\omega^{\mp}_{n-1}(\gamma)} & \longrightarrow & \dfrac{\varprojlim_m H^1(k_m,T)}{\omega^{\mp}_{n-1}(\gamma)} & \longrightarrow & \dfrac{\varprojlim_m H^1(k_m,T)/H^1_{\pm,m}}{\omega^{\mp}_{n-1}(\gamma)} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 \longrightarrow & \dfrac{H^1_{\pm,n}}{\omega^{\mp}_{n-1}(\gamma)H^1(k_n,T)} & \longrightarrow & \dfrac{H^1(k_n,T)}{\omega^{\mp}_{n-1}(\gamma)H^1(k_n,T)} & \longrightarrow & \dfrac{H^1(k_n,T)/H^1_{\pm,n}}{\omega^{\mp}_{n-1}(\gamma)}. & \end{array}$$

The rows are exact. By Theorem 4.5.12, the right vertical map is an isomorphism. Since $\varprojlim_m H^1(k_m, T) \to H^1(k_m, T)$ is surjective (cf. the proof of Proposition 4.5.10), the middle vertical map is surjective. Hence the proposition follows from the Snake lemma. □

For a Λ-module M, we put

$$M^{\omega^{\mp}_{n-1}=0} = \{x \in M \mid \omega^{\mp}_{n-1}(\gamma)\, x = 0\}.$$

We also put $\mathcal{H}^{\pm}(K_{n,v}) = H^1(K_{n,v}, V/T)/(E^{\pm}(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$.

COROLLARY 5.4.3. *The morphism*

$$\mathcal{H}^{\pm}(k_n)^{\omega^{\mp}_{n-1}=0} \to \varinjlim_m \mathcal{H}^{\pm}(k_m)$$

is injective.

PROOF. This is the Pontryagin dual of Proposition 5.4.2. □

Let us consider a diagram

$$\begin{array}{ccccccc} 0 \longrightarrow & \mathrm{Sel}^{\pm}(E/K_n)^{\omega^{\mp}_{n-1}=0} & \longrightarrow & H^1(K_n, V/T)^{\omega^{\mp}_{n-1}=0} & \longrightarrow & \Pi_v\, \mathcal{H}^{\pm}(K_{n,v})^{\omega^{\mp}_{n-1}=0} \\ & \downarrow s_n & & \downarrow h_n & & \downarrow g_n \\ 0 \longrightarrow & \mathrm{Sel}^{\pm}(E/K_\infty)^{\omega^{\mp}_{n-1}=0} & \longrightarrow & H^1(K_\infty, V/T)^{\omega^{\mp}_{n-1}=0} & \longrightarrow & \Pi_v\, \mathcal{H}^{\pm}(K_{\infty,v})^{\omega^{\mp}_{n-1}=0} \end{array}$$

We would like to show that s_n has finite kernel and cokernel of bounded order as n varies. We show this by arguments in Greenberg [**3**, Section 3].

If $\omega^{\mp}_{n-1} = 0$ is replaced by $\omega_{n-1} = 0$, then the morphism h_n is bijective as in the proof of Proposition 5.4.1. Hence in fact h_n is bijective. We show that kernel of g_n is finite of bounded order as n varies. By Lemma 3.3 in Greenberg [**3**], for $v \nmid p$, the kernel of $r_v : \mathcal{H}^{\pm}(K_{n,v}) \to \varinjlim_m \mathcal{H}^{\pm}(K_{m,v})$ is finite of bounded order. For $v \mid p$, the kernel of r_v is zero by Corollary 5.4.3.

Hence we have

THEOREM 5.4.4 (The plus (minus) control theorem). *The natural maps*

$$\mathrm{Sel}^{\pm}(E/K_n)^{\omega_{n-1}^{\mp}=0} \to \mathrm{Sel}^{\pm}(E/K_\infty)^{\omega_{n-1}^{\mp}=0}$$

are injective and have finite cokernel of bounded order as n varies.

We write $\mathscr{X}_\infty^{\pm} = \mathscr{X}^{\pm}(E/K_\infty)$ and $\mathscr{X}_n^{\pm} = \mathscr{X}^{\pm}(E/K_n)$ for simplicity. The Pontryagin dual of the plus (minus) control theorem is

THEOREM 5.4.5. *The natural maps*

$$\mathscr{X}_\infty^{\pm}/\omega_{n-1}^{\mp}(\gamma)\mathscr{X}_\infty^{\pm} \to \mathscr{X}_n^{\pm}/\omega_{n-1}^{\mp}(\gamma)\mathscr{X}_n^{\pm}$$

are surjective and have finite kernel of bounded order as n varies.

The following is a half of the p-adic Birch and Swinnerton-Dyer conjecture, which is already proved in Kato [**8**].

THEOREM 5.4.6.

$$\mathrm{ord}_{X=0}\mathscr{L}_p^{\pm}(E,X) \;\geq\; \mathrm{rank}\, E(\mathbb{Q}).$$

In particular, we have

$$\mathrm{ord}_{X=0}\mathscr{L}_p(E,X) \;\geq\; \mathrm{rank}\, E(\mathbb{Q}).$$

PROOF. By Theorem 5.4.5, we have a pseudo-isomorphism

$$\mathscr{X}_\infty^{\pm}/(\gamma-1)\mathscr{X}_\infty^{\pm} \cong \mathscr{X}_1^{\pm}/(\gamma-1)\mathscr{X}_1^{\pm} = \mathscr{X}_1^{\pm} = \mathscr{X}_1.$$

We compare the $\mathbb{Z}_p$-rank of the Δ-fixed parts of the both sides. By the half of the plus (minus) main conjecture, the rank of the left hand side is less than or equal to $\mathrm{ord}_{X=0}\mathscr{L}_p^{\pm}(E,X)$, and the rank of the right hand side is greater than or equal to the rank of $E(\mathbb{Q})$. □

5. The plus (minus) Iwasawa invariants

Since in the good supersingular case, the Selmer group is no longer Λ-cotorsion, the definition of the λ- and μ-invariants were not known. Recently, Perrin-Riou defined λ- and μ-invariants ([**20**]). However, her definition of λ- and μ-invariants are complicated.

We define the λ- and μ-invariants simply by the λ- and μ-invariants of our plus (minus) Selmer group. Arithmetic properties of our λ- and μ-invariants are visible, for example, we easily bound the rank of the Mordell-Weil group over K_∞ by using these λ-invariants as in the good ordinary case.

Recently, Kurihara announced that he obtained an Iwasawa formula for the Tate-Shafarevich group for some rational numbers λ, μ and ν (cf. Chapter 2, Section 5.) Perrin-Riou ([**20**]) also obtained an Iwasawa formula in terms of her λ- and μ-invariants. Iwasawa formula should be also obtained by using our λ- and μ-invariants as in Pollack's analytic Iwasawa formula.

DEFINITION 5.5.1. *Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character. We define $\lambda_\pm^\eta$ and $\mu_\pm^\eta$ as the λ- and the μ-invariants of* $\mathrm{Char}(\mathscr{X}^\pm(E/K_\infty)^\eta)$. *We put $\lambda_\pm = \sum_\eta \lambda_\pm^\eta$ and $\mu_\pm = \sum_\eta \mu_\pm^\eta$*

We define the n-th plus (minus) Mordell-Weil groups by

$$E^+(K_n) = \{P \in E(K_n) \mid \mathrm{Tr}_{n/m} P \in E(K_{m-1}) \text{ for odd } m,\ 1 \le m \le n\},$$
$$E^-(K_n) = \{P \in E(K_n) \mid \mathrm{Tr}_{n/m} P \in E(K_{m-1}) \text{ for even } m,\ 1 \le m \le n\}.$$

PROPOSITION 5.5.2. *We have $E^+(K_n) \otimes \mathbb{Q} \cap E^-(K_n) \otimes \mathbb{Q} = E(\mathbb{Q}) \otimes \mathbb{Q}$ and $E^+(K_n) \otimes \mathbb{Q} + E^-(K_n) \otimes \mathbb{Q} = E(K_n) \otimes \mathbb{Q}$. In other words, we have an exact sequence*

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q} \to (E^+(K_n) \otimes \mathbb{Q}) \oplus (E^-(K_n) \otimes \mathbb{Q}) \to E(K_n) \otimes \mathbb{Q} \to 0$$

where the first map is the diagonal embedding by inclusions and the second map is $(a, b) \mapsto (-1)^n(a - b)$.

PROOF. Suppose $P \in E^+(K_n) \otimes \mathbb{Q} \cap E^-(K_n) \otimes \mathbb{Q}$. If $P \in E(K_m) \backslash E(K_{m-1})$ for $m \ge 1$, then $\mathrm{Tr}_{n/m} P \notin E(K_{m-1})$. Hence we have a contradiction. Let P be an element of $E(K_n) \otimes \mathbb{Q}$. Let $\widetilde{\omega}_{n-1}^\pm(X)$ be as in Definition 4.5.4. Since $\mathrm{Tr}_{k+1/k}$ is given by the p^k-th cyclotomic polynomial $\Phi_k(\gamma)$, the element $\widetilde{\omega}_{n-1}^\mp(\gamma - 1)\, P$ is in $E^\pm(K_n) \otimes \mathbb{Q}$. Since $\widetilde{\omega}_{n-1}^+(X)$ and $\widetilde{\omega}_{n-1}^-(X)$ are mutually prime in $\mathbb{Q}[X]$, there exist $A(X), B(X) \in \mathbb{Q}[X]$ such that $A(X)\, \widetilde{\omega}_{n-1}^-(X) - B(X)\, \widetilde{\omega}_{n-1}^+(X) = (-1)^n$. If we put $P^+ = A(\gamma - 1)\widetilde{\omega}_{n-1}^-(\gamma - 1)\, P$ and $P^- = B(\gamma - 1)\widetilde{\omega}_{n-1}^+(\gamma - 1)\, P$, then $P^\pm \in E^\pm(K_n) \otimes \mathbb{Q}$ and $P = (-1)^n(P^+ - P^-)$. □

The following proposition is an analogue of Corollary 2.4.2 for the good ordinary case.

PROPOSITION 5.5.3. *We have*

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}^\pm(E/K_n)^\eta \ \le\ \lambda_\pm^\eta.$$

In particular, we have $\mathrm{rank}\ E^\pm(K_n)^\eta \le \mathrm{rank}\ E^\pm(K_\infty)^\eta \le \lambda_\pm^\eta$.

PROOF. The proposition follows from Proposition 5.4.1 and the fact that $E^\pm(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is contained in $\mathrm{Sel}^\pm(E/K_n)$. □

COROLLARY 5.5.4. *Let r be the rank of the Mordell-Weil group of $E(\mathbb{Q})$. Then,*

$$\mathrm{rank}\ E(K_\infty)^\eta \le \begin{cases} \lambda_+^\eta + \lambda_-^\eta & \text{if } \eta \ne 1, \\ \lambda_+^\eta + \lambda_-^\eta - r & \text{if } \eta = 1. \end{cases}$$

In particular, we have $\mathrm{rank}\ E(K_\infty) \ \le\ \lambda_+ + \lambda_- - r$.

PROOF. The corollary follows from Proposition 5.5.2 and Proposition 5.5.3. □

By the half of the plus (minus) main conjecture, we have a similar bound as in Corollary 5.5.4 by using the λ-invariants of Pollack's p-adic L-functions. Pollack gave a table of the values of his λ-invariants of elliptic curves of conductor less than 1000 ([**21**]).

THEOREM 5.5.5. *If $p \nmid \frac{L(E,1)}{\Omega_E}$ and the assumption in Theorem 5.2.2 v) is satisfied, then $\lambda^1_\pm = \mu^1_\pm = 0$ and the plus (minus) main conjecture for $\mathbb{Q}_\infty$ (the trivial η-part) holds. In particular, $\mathcal{X}^\pm(E/\mathbb{Q}_\infty)$ and $\mathcal{X}_0(E/\mathbb{Q}_\infty)$ are finite, and $\mathcal{X}^\pm(E/\mathbb{Q}_n)$ and $\mathcal{X}_0(E/\mathbb{Q}_n)$ are finite of bounded order as n varies.*

PROOF. By the interpolation properties of Pollack's p-adic L-function (3.1.1) and (3.1.2), Pollack's $\lambda^1_\pm$ and $\mu^1_\pm$-invariants are zero. Hence the assertion follows from Theorem 5.3.2. □

References

[1] Y. Amice and J. Vélu, Distributions p-adiques associées aux séries de Hecke. (French) JournéesArithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974), pp. 119–131. Asterisque, Nos. 24-25, Soc. Math. France, Paris, 1975.

[2] S. Bloch and K. Kato, L-functions and Tamagawa numbers of motives. The Grothendieck Festschrift, Vol. I, 333–400, Progr. Math., 86, Birkhäuser Boston, Boston, MA, 1990.

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

[4] R. Greenberg and V. Vatsal, On the Iwasawa invariants of elliptic curves. Invent. Math. 142 (2000), no. 1, 17–63.

[5] T. Honda, Formal groups and zeta-functions. Osaka J. Math. 5 1968 199–213.

[6] T. Honda, On the theory of commutative formal groups, J. Math. Soc. Japan 22 1970 213–246.

[7] K. Kato, Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}, Part I, in Arithmetic algebraic geometry (Trento, 1991), 50–163, Springer Lecture Notes in Math 1553 (1993).

[8] K. Kato, P-adic Hodge theory and values of zeta funcions of modular forms, Preprint series, Graduate School of Mathematical Sciences, The University of Tokyo.

[9] H. Knospe, Iwasawa-theory of abelian varieties at primes of non-ordinary reduction. Manuscripta Math. 87 (1995), no. 2, 225–258.

[10] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, preprint.

[11] M. Kurihara, The Iwasawa theory of elliptic curves that have supersingular reduction. Algebraic number theory and related topics (Kyoto, 2000). Surikaisekikenkyusho Kokyuroku No. 1154 (2000), 33–43.

[12] B. Mazur, Rational points of abelian varieties with values in towers of number fields. Invent. Math. 18 (1972), 183–266.

[13] B. Mazur and J. Tate, Refined conjectures of the "Birch and Swinnerton-Dyer type". Duke Math. J. 54 (1987), no. 2, 711–750.

[14] B. Mazur, J. Tate and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. Math. 84 (1986), no. 1, 1–48.

[15] J. Nekovář, On the parity of ranks of Selmer groups. II. C. R. Acad. Sci. Paris Ser. I Math. 332 (2001), no. 2, 99–104.

[16] B. Perrin-Riou, Théorie d'Iwasawa p-adique locale et globale, Invent. Math. 99 (1990), no. 2, 247–292.

[17] B. Perrin-Riou, Fonctions L p-adiques d'une courbe elliptique et points rationnels, Ann. Inst. Fourier (Grenoble) 43 (1993), no. 4, 945–995.

[18] B. Perrin-Riou, Théorie d'Iwasawa des représentations p-adiques sur un corps local, Invent. Math. 115 (1994), no. 1, 81–161.

[19] B. Perrin-Riou, Fonctions L p-adiques des repŕsentations p-adiques, Astérisque No. 229 (1995), 198 pp.
[20] B. Perrin-Riou, Arithmétique des courbes elliptiques à réduction supersinguliére en p, preprint.
[21] R. Pollack, On the p-adic L-function of a modular form at a supersingular prime, preprint.
[22] D. Rohrlich, On L-functions of elliptic curves and cyclotomic towers. Invent. Math. 75 (1984), no. 3, 409–423.
[23] D. Rohrlich, L-functions and division towers. Math. Ann. 281 (1988), no. 4, 611–632.
[24] K. Rubin, Euler systems and modular elliptic curves. Galois representations in arithmetic algebraic geometry (Durham, 1996), 351–367, London Math. Soc. Lecture Note Ser., 254, Cambridge Univ. Press, Cambridge, 1998.
[25] J-P. Serre, Proprietes galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. 15 (1972), no. 4, 259–331.
[26] G. Shimura, Introduction to the arithmetic theory of automorphic functions. Publications of the Mathematical Society of Japan, 11. Kano Memorial Lectures.
[27] G. Stevens, Stickelberger elements and modular parametrizations of elliptic curves. Invent. Math. 98 (1989), no. 1, 75–106.
[28] M. Višik Nonarchimedean measures associated with Dirichlet series. Mat. Sb. (N.S.) 99(141) (1976), no. 2, 248–260, 296.
[29] L. Washington, Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997.

UTMS

2001–27 Takeshi Saito: *Log smooth extension of family of curves and semi-stable reduction.*

2001–28 Takeshi Katsura: *AF-embeddability of crossed products of Cuntz algebras.*

2001–29 Toshio Oshima: *Annihilators of generalized Verma modules of the scalar type for classical Lie algebras.*

2001–30 Kim Sungwhan and Masahiro Yamamoto: *Uniqueness in identification of the support of a source term in an elliptic equation.*

2001–31 Tetsuhiro Moriyama: *The mapping class group action on the homology of the configuration spaces of surfaces.*

2001–32 Takeshi Katsura: *On crossed products of the Cuntz algebra $\mathcal{O}_\infty$ by quasi-free actions of abelian groups.*

2001–33 Yuichi Sugiki: *The category of cosheaves and Laplace transforms.*

2001–34 Hiroshige Kajiura: *Homotopy algebra morphism and geometry of classical string field theories.*

2002–1 Tetsushi Ito: *Stringy Hodge numbers and p-adic Hodge theory.*

2002–2 Yasuyuki Kawahigashi and Roberto Longo: *Classification of local conformal nets. case $c < 1$.*

2002–3 Takashi Taniguchi: *A mean value theorem for orders of degree zero divisor class groups of quadratic extensions over a function field.*

2002–4 Shin-ichi Kobayashi: *Iwasawa theory for elliptic curves at supersingular primes.*

The Graduate School of Mathematical Sciences was established in the University of Tokyo in April, 1992. Formerly there were two departments of mathematics in the University of Tokyo: one in the Faculty of Science and the other in the College of Arts and Sciences. All faculty members of these two departments have moved to the new graduate school, as well as several members of the Department of Pure and Applied Sciences in the College of Arts and Sciences. In January, 1993, the preprint series of the former two departments of mathematics were unified as the Preprint Series of the Graduate School of Mathematical Sciences, The University of Tokyo. For the information about the preprint series, please write to the preprint series office.

ADDRESS:
Graduate School of Mathematical Sciences, The University of Tokyo
3–8–1 Komaba Meguro-ku, Tokyo 153, JAPAN
TEL +81-3-5465-7001 FAX +81-3-5465-7012