Invent. math. 152, 1–36 (2003)
DOI: 10.1007/s00222-002-0265-4

Inventiones mathematicae

Iwasawa theory for elliptic curves at supersingular primes

Shin-ichi Kobayashi

Graduate School of Mathematical Sciences, University of Tokyo, Komaba 3-8-1, Tokyo, 153-8914 Japan (e-mail: koba@ms406ss5.ms.u-tokyo.ac.jp)

Oblatum 17-VI-2002 & 2-IX-2002
Published online: 18 December 2002 – © Springer-Verlag 2002

Abstract. We give a new formulation in Iwasawa theory for elliptic curves at good supersingular primes. This formulation is similar to Mazur's at good ordinary primes. Namely, we define a new Selmer group, and show that it is of Λ-cotorsion. Then we formulate the Iwasawa main conjecture as that the characteristic ideal is generated by Pollack's p-adic L-function. We show that this main conjecture is equivalent to Kato's and Perrin-Riou's main conjectures. We also prove an inequality in the main conjecture by using Kato's Euler system. In terms of the λ- and the μ-invariants of our Selmer group, we specify the numbers λ and μ in the asymptotic formula for the order of the Tate-Shafarevich group by Kurihara and Perrin-Riou.

1. Introduction

Let p be an odd prime. Let $F = \mathbb{Q}$ and F_∞/F the cyclotomic $\mathbb{Z}_p$-extension with n-th layer F_n. We denote $\mathrm{Gal}(F_\infty/F)$ by Γ. We identify $\mathbb{Z}_p[[\Gamma]]$ with the ring of power series $\mathbb{Z}_p[[X]]$.

In 1970's, Mazur formulated the Iwasawa theory for elliptic curves at good ordinary primes. In his formulation, the main conjecture states that the Selmer group over F_∞ is $\mathbb{Z}_p[[\Gamma]]$-cotorsion and the characteristic ideal is generated by the Mazur-Swinnerton-Dyer p-adic L-function. On the contrary, at supersingular primes, the Selmer group is no longer $\mathbb{Z}_p[[\Gamma]]$-cotorsion, and the p-adic L-function is not an element of $\mathbb{Z}_p[[\Gamma]] \otimes \overline{\mathbb{Q}_p}$. Hence, at supersingular primes, in spite of the significant works by Kato and Perrin-Riou, we had no formulation analogue to Mazur's.

The aim of this paper is to consider Iwasawa theory for elliptic curves at good supersingular primes in a way similar with Mazur's at good ordinary primes. More precisely, let E be an elliptic curve over $\mathbb{Q}$ with good

supersingular reduction at p. Suppose $a_p = 0$. This condition is automatically satisfied for a supersingular p greater than 3, however, the condition is crucial for us. Our methods will probably have to be modified quite significantly to treat the excluded cases. Then we define new Selmer groups $\mathrm{Sel}^{\pm}(E/F_n)$ by putting moderately stronger local conditions at p on the definition of the usual (p-primary) Selmer group $\mathrm{Sel}(E/F_n)$.

Definition 1.1. *We define the n-th even (odd) Selmer group by*

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

where $F_{n,p}$ is the completion of F_n at the place over p and

$$E^{+}(F_{n,p}) := \{P \in E(F_{n,p}) \mid \mathrm{Tr}_{n/m+1} P \in E(F_{m,p}) \ \textit{for even } m\ (0 \le m < n)\}$$
$$E^{-}(F_{n,p}) := \{P \in E(F_{n,p}) \mid \mathrm{Tr}_{n/m+1} P \in E(F_{m,p}) \ \textit{for odd } m\ (0 \le m < n)\}$$

where $\mathrm{Tr}_{n/m+1} : E(F_{n,p}) \to E(F_{m+1,p})$ is the trace map.

We remark that the group $E^{\pm}(F_{n,p})$ essentially appeared in Knospe [8] and Perrin-Riou [13]. Let $\mathrm{Sel}^{\pm}(E/F_\infty) := \varinjlim_n \mathrm{Sel}^{\pm}(E/F_n)$. Then $\mathbb{Z}_p[[\Gamma]]$ acts naturally on the Pontryagin dual of $\mathrm{Sel}^{\pm}(E/F_\infty)$.

Theorem 1.2. *The Pontryagin dual of the even (odd) Selmer group $\mathrm{Sel}^{\pm}(E/F_\infty)^\vee$ is a finitely generated torsion $\mathbb{Z}_p[[\Gamma]]$-module.*

We formulate the main conjecture as follows.

Conjecture (Main Conjecture). *Suppose $a_p = 0$ (e.g. $p \ge 5$). Then the characteristic ideal of the Pontryagin dual of $\mathrm{Sel}^{\pm}(E/F_\infty)$ is generated by Pollack's p-adic L-function $\mathcal{L}_p^{\pm}(E, X)$:*

$$\mathrm{Char}\left(\mathrm{Sel}^{\pm}(E/F_\infty)^\vee\right) = \left(\mathcal{L}_p^{\pm}(E, X)\right).$$

Pollack's p-adic L-function [18] is a p-adic function which interpolates special values of the Hasse-Weil L-function similarly to the usual p-adic L-function. However, this p-adic L-function lives in $\mathbb{Z}_p[[\Gamma]]$ (cf. Sect. 3). We will see that our main conjecture is equivalent to Kato's and Perrin-Riou's main conjectures (cf. [6], [7], [14]).

By using Kato's Euler system [7], we show that

Theorem 1.3. *Suppose $E/\mathbb{Q}$ does not have complex multiplication. Then for almost all prime p, we have*

$$\mathrm{Char}\left(\mathrm{Sel}^{\pm}(E/F_\infty)^\vee\right) \supseteq \left(\mathcal{L}_p^{\pm}(E, X)\right).$$

For the more precise statement of the theorem, see Sect. 4. Recently, Pollack and Rubin informed the author that the above main conjecture is true for CM elliptic curves ([19]).

We also obtain an asymptotic formula for the p-adic order of the Tate-Shafarevich group $Ш(E/F_n)$ using the λ- and the μ-invariants of $\mathrm{Sel}^{\pm}(E/F_\infty)^\vee$.

Theorem 1.4. *Assume that $Ш(E/F_n)$ is finite for all n. Let $e_n = \mathrm{ord}_p \sharp Ш(E/F_n)$. Let $\lambda_\pm$ and $\mu_\pm$ be the λ- and the μ-invariants of $\mathrm{Sel}^{\pm}(E/F_\infty)^\vee$. Then for sufficiently large n, we have*

$$e_n = \sum_{m=0}^{[\frac{n-2}{2}]} p^{n-1-2m} - \left[\frac{n}{2}\right] + \left[\frac{n}{2}\right]\lambda_+ + \left[\frac{n+1}{2}\right]\lambda_- - n\, r_\infty + \sum_{m=1}^{[\frac{n}{2}]} \phi\big(p^{2m}\big)\,\mu_+ + \sum_{m=1}^{[\frac{n+1}{2}]} \phi\big(p^{2m-1}\big)\,\mu_- + \nu$$

where $r_\infty = \mathrm{rank}\, E(F_\infty)$, $\phi(p^k) = p^k - p^{k-1}$ and ν is an integer independent of n. Here $[x]$ denotes the largest integer not greater than x.

Similar formulas have been obtained by Kurihara and Perrin-Riou [17] with unspecified rational numbers λ and μ. In the above formula, these λ and μ are specified as $\lambda_\pm$ and $\mu_\pm$ as in Pollack's analytic counterpart. (The sign in the notation of our λ- and μ-invariants are opposite to that of Pollack's.)

The key to our theory is a construction of the even (odd) Coleman maps. These are Λ-valued and send Kato's zeta element to Pollack's p-adic L-function. The group $E^{\pm}(F_{n,p})$ is defined so as to be equal to the exact annihilator with respect to the Tate pairing of the kernel of the n-th even (odd) Coleman map. Once these maps are constructed, the main theorems are proved in the same way as in the good ordinary case (cf. Sect. 7). We construct these Coleman maps by modifying Kurihara's P_n-pairing in [9] with Pollack's idea on the p-adic L-function. We outline the construction.

Let $k_n = \mathbb{Q}_p(\zeta_{p^{n+1}})$. We denote $\Lambda_n = \mathbb{Z}_p[\mathcal{G}_n]$ and $\Lambda = \mathbb{Z}_p[[\mathcal{G}_\infty]]$ where $\mathcal{G}_n = \mathrm{Gal}(k_n/\mathbb{Q})$ and $\mathcal{G}_\infty = \varprojlim \mathcal{G}_n$. Let T be the p-adic Tate module of E and $\mathbf{H}^1_{\mathrm{Iw}}(T) = \varprojlim_n H^1(k_n, T)$. We construct the even (odd) Coleman map $\mathrm{Col}^{\pm} : \mathbf{H}^1_{\mathrm{Iw}}(T) \to \Lambda$ as follows.

Using Honda's theory of formal groups, we construct a canonical system $(\mathrm{c}_n)_n$, $\mathrm{c}_n \in E(k_n) \otimes \mathbb{Z}_p \subseteq H^1(k_n, T)$ satisfying

$$\mathrm{Tr}_{n+1/n}(\mathrm{c}_{n+1}) - a_p\,\mathrm{c}_n + \mathrm{c}_{n-1} = 0. \tag{1.1}$$

(Perrin-Riou [13] also constructed such a system using the theory of norm fields by Fontaine and Wintenberger.) If $a_p = 0$, we have $\mathrm{Tr}_{n+1/n}(\mathrm{c}_{n+1}) =$

$-\mathrm{c}_{n-1}$. Hence, according to the parity of n, the elements $(\mathrm{c}_n)_n$ give kinds of norm compatible systems. Then we consider a morphism

$$P_n : H^1(k_n, T) \longrightarrow \Lambda_n, \quad z \longmapsto (-1)^{[\frac{n+2}{2}]} \sum_{\sigma \in \mathcal{G}_n} \left(\mathrm{c}_n^{\sigma}, z\right)_n \sigma$$

where $(\ ,\ )_n$ is the pairing induced by the cup product. We show that the image of P_n is contained in the ideal generated by a certain product of cyclotomic polynomials. Eliminating the product and using the norm relation of $(\mathrm{c}_n)_n$, we can take the limit of P_n for n of the same parity. Then we get the even (odd) Coleman map

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

Acknowledgements. 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 also thank Ken-ichi Bannai and Seidai Yasuda for discussions and for reading the manuscript carefully. He would like to thank Robert Pollack for showing him the preprint [18]. He is grateful to Kazuya Kato for showing him the preprint [7]. He expresses his sincere gratitude to Masato Kurihara. The author learned a lot of things through the manuscript of the paper [9], including the P_n-pairing and the idea to use Honda's theory.

2. The even (odd) Selmer group

Let p be an odd prime number. We fix a generator (ζ_{p^n}) of $\mathbb{Z}_p(1)$, namely, for each $n \geq 0$, ζ_{p^n} is a primitive p^n-th root of unity such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. We denote $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$, $K_{-1} = \mathbb{Q}$ and $K_\infty = \cup_n K_n$.

Let E be an elliptic curve over $\mathbb{Q}$ with good reduction at p. We assume that $a_p = 0$. When $p \geq 5$, the condition $a_p = 0$ is equivalent to the condition that E has supersingular reduction at p.

The (p-primary) Selmer group is defined by

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

and $\mathrm{Sel}(E/K_\infty) := \varinjlim_n \mathrm{Sel}(E/K_n)$, where v ranges over all places of K_n and $K_{n,v}$ is the completion of K at v. We regard $E(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ as a subgroup of $H^1(K_{n,v}, E[p^\infty])$ by the Kummer map.

We define subgroups $E^{\pm}(K_{n,v})$ of $E(K_{n,v})$ by

$$E^+(K_{n,v}) = \{P \in E(K_{n,v}) \mid \mathrm{Tr}_{n/m+1} P \in E(K_{m,v}) \text{ for even } m\ (0 \leq m < n)\},$$
$$E^-(K_{n,v}) = \{P \in E(K_{n,v}) \mid \mathrm{Tr}_{n/m+1} P \in E(K_{m,v}) \text{ for odd } m\ (-1 \leq m < n)\},$$

where $\mathrm{Tr}_{n/m+1} : E(K_{n,v}) \to E(K_{m+1,v})$ is the trace map.

Definition 2.1. *The even (odd) Selmer group is defined by*

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

and $\mathrm{Sel}^{\pm}(E/K_\infty) := \varinjlim_n \mathrm{Sel}^{\pm}(E/K_n)$.

Following Kurihara [9], we also define the zero Selmer group by

$$\mathrm{Sel}^{0}(E/K_n) := \mathrm{Ker}\left(H^1\big(K_n, E[p^\infty]\big) \longrightarrow \prod_v H^1\big(K_{n,v}, E[p^\infty]\big) \right)$$

and $\mathrm{Sel}^{0}(E/K_\infty) := \varinjlim_n \mathrm{Sel}^{0}(E/K_n)$.

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

Let $\mathcal{G}_n = \mathrm{Gal}(K_n/\mathbb{Q})$ and $\mathcal{G}_\infty = \varprojlim \mathcal{G}_n$. Then $\Lambda_n = \mathbb{Z}_p[\mathcal{G}_n]$ acts naturally on $\mathcal{X}^{\pm}(E/K_n)$ and $\Lambda = \mathbb{Z}_p[[\mathcal{G}_\infty]]$ on $\mathcal{X}^{\pm}(E/K_\infty)$.

Theorem 2.2. *The Pontryagin dual of the even (odd) Selmer group $\mathcal{X}^{\pm}(E/K_\infty)$ is a finitely generated torsion Λ-module.*

Proof. This theorem is proved in Sect. 7 (cf. Theorem 7.3). □

3. Pollack's p-adic L-function

We first recall the classical p-adic L-function of an elliptic curve $E/\mathbb{Q}$ at a good prime p. Let α be a root of the p-Euler factor $X^2 - a_p X + p$ such that $\mathrm{ord}_p(\alpha) < 1$. Let $L = \mathbb{Q}_p(\alpha)$. For an integer $h \geq 1$, we let

$$\mathcal{H}_{h,L} = \left\{ \sum_{n\geq 0} a_n X^n \in L[[X]] \;\middle|\; \lim_{n\to\infty} \frac{|a_n|_p}{n^h} = 0 \right\}$$

where $|\ |_p$ denotes the multiplicative valuation of L normalized by $|p|_p = \frac{1}{p}$. Then $\mathcal{H}_{\infty,L} = \cup_h \mathcal{H}_{h,L}$ is a ring.

Let $\kappa : \mathcal{G}_\infty \xrightarrow{\sim} \mathbb{Z}_p^\times$ be the cyclotomic character. Then we have the decomposition

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

We fix a topological generator $\gamma \in \Gamma$. Then we identify $\mathbb{Z}_p[[\Gamma]]$ with $\mathbb{Z}_p[[X]]$ and Λ with $\mathbb{Z}_p[\Delta][[X]]$ by identifying γ with $1 + X$.

Theorem 3.1 (Amice-Vélu [1], Vishik [23]). *Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character with sign $\delta = \eta(-1)$. We regard η as a character of $\mathcal{G}_\infty$ by taking $\eta(\gamma) = 1$. Let $\Omega_E^\pm$ be the real and imaginary Néron periods. Then there exists a unique element*

$$\mathcal{L}_p(E, \eta, \alpha, X) \in \mathcal{H}_{1,L}$$

having the following interpolation properties. (If $\eta = 1$, we write $\mathcal{L}_p(E, \eta, \alpha, X)$ simply by $\mathcal{L}_p(E, \alpha, X)$.)

Let $\chi : \mathcal{G}_n \to \mu_{p^\infty}$ be a character and let $\chi(\gamma) = \zeta$ and $\psi = \chi\eta$. We denote the Hasse-Weil L-function with the Dirichlet character ψ by $L(E, \psi, s)$.

Then, if the conductor of ψ is $p^{n+1} \neq 1$, we have

$$\mathcal{L}_p(E, \eta, \alpha, \zeta - 1) = \frac{p^{n+1}}{\tau(\overline{\psi})\, \alpha^{n+1}} \frac{L\big(E, \overline{\psi}, 1\big)}{\Omega_E^\delta} \tag{3.2}$$

where $\overline{\psi} = \psi^{-1}$ and $\tau(\psi)$ is the Gauss sum $\sum_{a \in \mathcal{G}_n} \psi(a)\, \zeta_{p^{n+1}}^a$. Here, we identify $\mathcal{G}_n$ with $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$.

If $\psi = 1$, we have

$$\mathcal{L}_p(E, \alpha, 0) = \big(1 - \alpha^{-1}\big)^2 \frac{L(E, 1)}{\Omega_E}. \tag{3.3}$$

We call the power series $\mathcal{L}_p(E, \eta, \alpha, X)$ the p-adic L-function. (Usually, the function $\mathcal{L}_p(E, \eta, \alpha, \kappa(\gamma)^{s-1} - 1)$ of variable $s \in \mathbb{Z}_p$ is called the p-adic L-function.) The p-adic L-function $\mathcal{L}_p(E, \eta, \alpha, X)$ is in $\mathbb{Z}_p[[X]] \otimes L$ if and only if a_p is a unit.

Now we assume that $a_p = 0$. Then the both roots $\alpha, \overline{\alpha}$ of $X^2 - a_p X + p = X^2 + p$ satisfy $\mathrm{ord}_p(\alpha) < 1$, and we have two p-adic L-functions $\mathcal{L}_p(E, \eta, \alpha, X)$ and $\mathcal{L}_p(E, \eta, \overline{\alpha}, X)$. Then by the interpolation property (3.2), we have

$$\mathcal{L}_p(E, \eta, \alpha, X) \pm \mathcal{L}_p(E, \eta, \overline{\alpha}, X) = 0$$

at $X = \zeta - 1$ where ζ is a primitive p^n-th root of unity such that $(-1)^n = \pm 1$.

Pollack compared the sum and the difference of two p-adic L functions with the following two functions $\log_p^+(1 + X)$ and $\log_p^-(1 + X)$, which also have trivial zeros of the form $\zeta - 1$.

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

where $\Phi_n(X) = \sum_{i=0}^{p-1} X^{p^{n-1} i}$ is the p^n-th cyclotomic polynomial. We remark that $\log_p(1 + X) = p^2 X \log_p^+(1 + X) \log_p^-(1 + X)$.

Theorem 3.2 (Pollack). *There exist power series $\mathcal{L}_p^{\pm}(E, \eta, X)$ in $\mathbb{Z}_p[[X]]$ satisfying*

$$\mathcal{L}_p(E, \alpha, \eta, X) = \mathcal{L}_p^-(E, \eta, X)\ \log_p^+(1+X) + \mathcal{L}_p^+(E, \eta, X)\ \log_p^-(1+X)\,\alpha,$$
$$\mathcal{L}_p(E, \overline{\alpha}, \eta, X) = \mathcal{L}_p^-(E, \eta, X)\ \log_p^+(1+X) + \mathcal{L}_p^+(E, \eta, X)\ \log_p^-(1+X)\,\overline{\alpha}.$$

Proof. See Pollack [18], Theorem 6.1 and 6.6. □

We call $\mathcal{L}_p^{\pm}(E, \eta, X)$ Pollack's p-adic L-function. If η is trivial, we simply write $\mathcal{L}_p^{\pm}(E, X)$ for $\mathcal{L}_p^{\pm}(E, \eta, X)$. We remark that our sign of Pollack's p-adic L-function is opposite to that in [18].

Pollack's p-adic L-function is characterized by the following interpolation properties.

Let $\chi : \mathcal{G}_n \to \mu_{p^\infty}$ be a non-trivial character of conductor p^{n+1} and let $\psi = \eta\chi$ and $\chi(\gamma) = \zeta$. For an even n, we have

$$\mathcal{L}_p^+(E, \eta, \zeta - 1) = (-1)^{\frac{n+2}{2}} \frac{p^{n+1}}{\tau(\overline{\psi})} \prod_k \Phi_k(\zeta)^{-1}\ \frac{L\big(E, \overline{\psi}, 1\big)}{\Omega_E^{\delta}} \tag{3.4}$$

where the product is take over odd k $(1 \le k \le n)$.

For an odd n, we have

$$\mathcal{L}_p^-(E, \eta, \zeta - 1) = (-1)^{\frac{n+1}{2}} \frac{p^{n+1}}{\tau(\overline{\psi})} \prod_k \Phi_k(\zeta)^{-1}\ \frac{L\big(E, \overline{\psi}, 1\big)}{\Omega_E^{\delta}} \tag{3.5}$$

where the product is take over even k $(1 \le k \le n)$.

We also have

$$\mathcal{L}_p^+(E, 0) = 2\,\frac{L(E, 1)}{\Omega_E}, \quad \mathcal{L}_p^-(E, 0) = (p-1)\,\frac{L(E, 1)}{\Omega_E} \tag{3.6}$$

and for $\eta \neq 1$

$$\mathcal{L}_p^+(E, \eta, 0) = -\frac{p}{\tau(\overline{\eta})}\ \frac{L(E, \overline{\eta}, 1)}{\Omega_E^{\delta}}, \quad \mathcal{L}_p^-(E, \eta, 0) = 0. \tag{3.7}$$

In Sect. 8, we reconstruct Pollack's p-adic L-function, 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 even (odd) Coleman maps (Theorem 6.3).

4. Main conjecture

Now we formulate the main conjecture when $a_p = 0$.

Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character. For a $\mathbb{Z}_p[\Delta]$-module M, let M^η denote the η-component of M. If we denote $\varepsilon_\eta = \frac{1}{\sharp\Delta}\sum_{\tau\in\Delta}\eta^{-1}(\tau)\ \tau$, M^η is given by $\varepsilon_\eta M$. If η is trivial, we replace the superscript η by Δ. For a finitely generated torsion $\mathbb{Z}_p[[\Gamma]]$-module N, we denote its characteristic ideal by $\mathrm{Char}(N)$.

By Theorem 2.2, $\mathcal{X}^\pm(E/K_\infty)^\eta$ is a torsion $\mathbb{Z}_p[[\Gamma]]$-module.

Conjecture (Even main conjecture). *For every η, we have*

$$\mathrm{Char}\left(\mathcal{X}^+(E/K_\infty)^\eta\right) = \left(\mathcal{L}_p^+(E,\eta,X)\right).$$

Conjecture (Odd main conjecture). *If η is trivial, we have*

$$\mathrm{Char}\left(\mathcal{X}^-(E/K_\infty)^\Delta\right) = \left(\mathcal{L}_p^-(E,X)\right).$$

If η is non-trivial, we have

$$\mathrm{Char}\left(\mathcal{X}^-(E/K_\infty)^\eta\right) = \left(\frac{1}{X}\mathcal{L}_p^-(E,\eta,X)\right).$$

(By (3.7), the p-adic L-function $\mathcal{L}_p^-(E,\eta,X)$ is divisible by X.)

Theorem 4.1. *There exists an integer $n \geq 0$ such that*

$$\mathrm{Char}\left(\mathcal{X}^+(E/K_\infty)^\eta\right) \supseteq \left(p^n\,\mathcal{L}_p^+(E,\eta,X)\right),$$
$$\mathrm{Char}\left(\mathcal{X}^-(E/K_\infty)^\Delta\right) \supseteq \left(p^n\,\mathcal{L}_p^-(E,X)\right),$$
$$\mathrm{Char}\left(\mathcal{X}^-(E/K_\infty)^\eta\right) \supseteq \left(\frac{p^n}{X}\,\mathcal{L}_p^-(E,\eta,X)\right) \quad \textit{for } \eta \neq 1.$$

If the p-adic representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{\mathbb{Z}_p}(T)$ is surjective, then we can take $n = 0$. Here $T = T_pE$ is the p-adic Tate module of E.

Proof. This theorem is proved in Sect. 7. □

5. Kato's main conjecture

We recall Kato's main conjecture and his results for the Euler system. In this section, we do not need to make any assumption on the reduction of E at p. However, for simplicity, we assume that E has good reduction at p.

Let T be the p-adic Tate module of E and $V = T \otimes \mathbb{Q}_p$. Let j be the natural morphism $\mathrm{Spec}\ K_n \to \mathrm{Spec}\ O_{K_n}[1/p]$. We denote

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

where $H^q(\mathrm{Spec}\ O_{K_n}[1/p],\, j_*T)$ is the étale cohomology group. We also write $\mathbf{H}^q(V) = \mathbf{H}^q(T) \otimes \mathbb{Q}$.

Theorem 5.1 (Kato [7]). i) $\mathbf{H}^2(T)$ *is a finitely generated torsion* Λ*-module.*
ii) $\mathbf{H}^1(T)$ *is a torsion free* Λ*-module, and* $\mathbf{H}^1(V)$ *is a free* $\Lambda \otimes \mathbb{Q}$*-module of rank* 1.
iii) *If* T/pT *is irreducible as a two dimensional representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *over* $\mathbb{F}_p$*, then* $\mathbf{H}^1(T)$ *is a free* Λ*-module of rank* 1.

Proof. See Kato [7], Theorem 12.4. □

Theorem 5.2 (Kato [7]). i) *There exist two systems of elements,*

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

such that for a character ψ *of* $\mathcal{G}_n$ *of conductor* p^{n+1}*, we have*

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

where $\exp^*_{\omega_E}$ *is the dual exponential map (cf. Sect. 8.7) and* $\delta = 1$ *if* $\psi(-1)$ *is equal to the sign of* $z_n^{\pm}$*, otherwise,* $\delta = 0$*.*
ii) *Let* $\mathbf{Z}(V)$ *be the* $\Lambda \otimes \mathbb{Q}$*-submodule of* $\mathbf{H}^1(V)$ *generated by* $\mathbf{z}^+$ *and* $\mathbf{z}^-$*. Then* $\mathbf{H}^1(V)/\mathbf{Z}(V)$ *is a torsion* $\Lambda \otimes \mathbb{Q}$*-module.*
iii) *Let* $\eta : \Delta \to \mathbb{Z}_p^{\times}$ *be a character. Then*

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

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

$$\mathbf{Z}(T) \subseteq \mathbf{H}^1(T) \quad \textit{in} \quad \mathbf{H}^1(V).$$

v) *Suppose that the homomorphism*

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

is surjective. Then,

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

Proof. See Kato [7], Theorem 12.5. For iv), we need Theorem 12.6 of Kato [7]. See also the argument in Sect. 13.14 of [7]. We also use the fact that the Néron period differs from the canonical period by a p-adic unit (cf. Greenberg-Vatsal [3]). □

Remark 5.3. i) When E has supersingular reduction at p, the condition in Theorem 5.1 iii) and 5.2 iv) is satisfied.

ii) The signs in Theorem 5.2 i) are related with the action of the complex conjugate on the homology group of E. They are not connected with the signs of even (odd) Selmer groups.

iii) If E has no complex multiplication, then by the result of Serre [22], the condition in Theorem 5.2 v) is satisfied for almost all p.

In [6], Kato formulated the Iwasawa main conjecture for motives. As a special case, his main conjecture can be read as follows (cf. Conjecture 12.10 in [7]).

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

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

We may see that this is a generalization of the classical Iwasawa main conjecture relating the ideal class groups and the groups of the global units modulo the cyclotomic units.

Kato's main conjecture is known to be equivalent to Perrin-Riou's main conjecture [14], [16]. We see that the even and the odd main conjectures are also equivalent to Kato's main conjecture (Theorem 7.4).

6. The even and the odd Coleman maps

We review the even (odd) Coleman maps constructed in Sect. 8.

Let k_n denote $\mathbb{Q}_p(\zeta_{p^{n+1}})$.

Definition 6.1. *We define $H^1_\pm(k_n, T)$ as the exact annihilator with respect to the Tate pairing*

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

of the subgroup $E^\pm(k_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subseteq H^1(k_n, V/T)$.

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

Let $\Phi_n(X) = \sum_{i=0}^{p-1} X^{p^{n-1}i}$ be the p^n-th cyclotomic polynomial. We define $\omega_0^\pm(X) = X$ and

$$\omega_n^+(X) = X \prod_{2\le m\le n,\ m:\text{even}} \Phi_m(1+X), \tag{6.8}$$

$$\omega_n^-(X) = X \prod_{1\le m\le n,\ m:\text{odd}} \Phi_m(1+X). \tag{6.9}$$

We also let $\Lambda_n^{\pm} = \mathbb{Z}_p[\Delta][X]/(\omega_n^{\pm}(X))$, $I_n^{\pm} = X\Lambda_n^{\pm}$ and $I = X\Lambda$.
In Sect. 8, we construct the n-th even (odd) Coleman map

$$\mathrm{Col}_n^{\pm} : H^1(k_n, T)/H_{\pm}^1(k_n, T) \longrightarrow \Lambda_n^{\pm}$$

and its limit the even (odd) Coleman map

$$\mathrm{Col}^{\pm} : \mathbf{H}_{\mathrm{Iw}}^1(T)/\mathbf{H}_{\mathrm{Iw},\pm}^1(T) \longrightarrow \Lambda.$$

They are morphisms of Λ-modules and have the following properties.

Theorem 6.2. *The even (odd) Coleman maps induce isomorphisms*

$$\mathrm{Col}_n^{+} : H^1(k_n, T)/H_{+}^1(k_n, T) \xrightarrow{\simeq} \Lambda_n^{+}, \tag{6.10}$$

$$\mathrm{Col}_n^{-} : H^1(k_n, T)^{\Delta}/H_{-}^1(k_n, T)^{\Delta} \xrightarrow{\simeq} (\Lambda_n^{-})^{\Delta}, \tag{6.11}$$

$$\mathrm{Col}_n^{-} : H^1(k_n, T)^{\eta}/H_{-}^1(k_n, T)^{\eta} \xrightarrow{\simeq} (I_n^{-})^{\eta} \quad \textit{for } \eta \neq 1. \tag{6.12}$$

Taking the limit of the above isomorphisms, we have

$$\mathrm{Col}^{+} : \mathbf{H}_{\mathrm{Iw}}^1(T)/\mathbf{H}_{\mathrm{Iw},+}^1(T) \xrightarrow{\simeq} \Lambda, \tag{6.13}$$

$$\mathrm{Col}^{-} : \mathbf{H}_{\mathrm{Iw}}^1(T)^{\Delta}/\mathbf{H}_{\mathrm{Iw},-}^1(T)^{\Delta} \xrightarrow{\simeq} \Lambda^{\Delta}, \tag{6.14}$$

$$\mathrm{Col}^{-} : \mathbf{H}_{\mathrm{Iw}}^1(T)^{\eta}/\mathbf{H}_{\mathrm{Iw},-}^1(T)^{\eta} \xrightarrow{\simeq} I^{\eta} \quad \textit{for } \eta \neq 1. \tag{6.15}$$

Proof. This theorem is proved in Sect. 8. □

Theorem 6.3. *Let $\mathbf{z}^{\pm} \in \mathbf{H}^1(T)$ be Kato's zeta element in Theorem 5.2. By the localization map, we regard $\mathbf{z}^{\pm}$ as an element of $\mathbf{H}_{\mathrm{Iw}}^1(T)$. Then, the image of Kato's zeta element by the even (odd) Coleman map is Pollack's p-adic L-function*:

$$\mathrm{Col}^{\pm}\left(\mathbf{z}^{\eta(-1)}\right)\varepsilon_{\eta} = \eta(-1)\,\mathcal{L}_p^{\pm}(E, \eta, X)\,\varepsilon_{\eta}.$$

Proof. This theorem is proved in Sect. 8.7. □

Theorem 6.3 gives another construction of Pollack's p-adic L-function.

7. Proofs of main theorems

Admitting Theorem 6.2 and 6.3, we prove Theorem 2.2 and 4.1. We also prove the equivalence of our main conjecture and Kato's main conjecture. The proofs are basically the same as the good ordinary case (cf. Kato [7]).

Let S be a finite set of places of $\mathbb{Q}$ containing p, all bad places of E, and the archimedean place. Let S_n (resp. S_∞) be the set of places of K_n (resp. K_∞) over S. Let $H^q(G_{n,S}, T)$ denote the Galois cohomology group of $G_{n,S} = \mathrm{Gal}(K_{n,S}/K_n)$ where $K_{n,S}$ is the maximal unramified extension of K_n outside S_n. We let

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

where the limit is taken with respect to the corestrictions.

We have $E(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ for the places v not lying above p. By definition, the exact annihilator of $E^{\pm}(k_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ with respect to the local Tate pairing is $H^1_{\pm}(k_n, T)$. The exact annihilator of $E(k_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is $E(k_n) \otimes \mathbb{Z}_p$. Hence from the Tate-Poitou exact sequence, we have

$$0 \to \mathcal{X}^0(E/K_n) \to H^2(G_{n,S}, T) \to \oplus_{v \in S_n} H^2(K_{n,v}, T), \tag{7.16}$$

$$H^1(G_{n,S}, T) \to H^1(k_n, T)/H^1_{\pm}(k_n, T) \to \mathcal{X}^{\pm}(E/K_n) \to \mathcal{X}^0(E/K_n) \to 0, \tag{7.17}$$

$$H^1(G_{n,S}, T) \to H^1(k_n, T)/E(k_n) \otimes \mathbb{Z}_p \to \mathcal{X}(E/K_n) \to \mathcal{X}^0(E/K_n) \to 0. \tag{7.18}$$

(cf. Perrin-Riou [16], Appendix A. 3.2.)

Taking the limit of the above exact sequences, we have

$$0 \to \mathcal{X}^0(E/K_\infty) \to \mathbf{H}^2_{/S}(T) \to \oplus_{v \in S_\infty} \mathbf{H}^2_{\mathrm{Iw},v}(T), \tag{7.19}$$

$$\mathbf{H}^1_{/S}(T) \to \mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},\pm}(T) \to \mathcal{X}^{\pm}(E/K_\infty) \to \mathcal{X}^0(E/K_\infty) \to 0. \tag{7.20}$$

Proposition 7.1 (Kurihara). i) *The canonical mapping* $\mathbf{H}^1(T) \to \mathbf{H}^1_{/S}(T)$ *is an isomorphism.*
ii) $\mathbf{H}^2(T)$ *is isomorphic to* $\mathcal{X}^0(E/K_\infty)$ *as* Λ*-module.*

Proof. The proposition is due to Kurihara [9]. It follows from the localization sequence of étale cohomology groups

$$0 \to H^1(O_{K_n}[1/p], j_*T) \to H^1(O_{K_n}[1/S], T) \to \oplus_v H^0(k(v), H^1(I_{n,v}, T))$$
$$\to H^2(O_{K_n}[1/p], j_*T) \to H^2(O_{K_n}[1/S], T) \to \oplus_v H^2(K_{n,v}, T)$$

where v ranges over the places over $S' = S \setminus \{p\}$, $k(v)$ is the residue field of v and $I_{n,v}$ is the inertia subgroup of the absolute Galois group of $K_{n,v}$. Then we use the fact $\varprojlim_n H^0(k(v), H^1(I_{n,v}, T)) = 0$ and (7.19). We also remark that $H^1(O_{K_n}[1/S], T) = H^1(G_{n,S}, T)$. □

We identify $\mathbf{H}^1(T) = \mathbf{H}^1_{/S}(T)$.

Corollary 7.2. *$\mathcal{X}^0(E/K_\infty)$ is a torsion Λ-module.*

Proof. This follows from Theorem 5.1 and Proposition 7.1. □

Theorem 7.3. i) *We have an exact sequence*

$$0 \to \mathbf{H}^1(T) \to \mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},\pm}(T) \to \mathcal{X}^{\pm}(E/K_\infty) \to \mathcal{X}^0(E/K_\infty) \to 0. \tag{7.21}$$

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

Proof. The exact sequence is nothing but (7.20) except for the injectivity of $\mathbf{H}^1(T) \to \mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},\pm}(T)$. We consider the composition of this map and the even (odd) Coleman map:

$$\mathbf{H}^1(T) \to \mathbf{H}^1_{\mathrm{Iw}}(T)/\mathbf{H}^1_{\mathrm{Iw},\pm}(T) \hookrightarrow \Lambda.$$

(cf. Theorem 6.2.) Since $\mathbf{H}^1(T)$ is a free Λ-module of rank 1 (cf. Theorem 5.1 iii)), this morphism is injective if and only if it is a non-zero map. Hence i) follows from Theorem 6.3 and Rohrlich's theorem [20], which assures $\mathcal{L}_p^{\pm}(E, \eta, X) \neq 0$.

For ii), by Theorem 6.3, 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 $\mathcal{L}_p^{\pm}(E, \eta, X)$. Hence the cokernel is Λ-torsion. Since $\mathcal{X}^0(E/K_\infty)$ is Λ-torsion by Corollary 7.2, ii) follows from the exact sequence (7.21). □

Theorem 7.4. *The three conjectures, namely, Kato's main conjecture (Sect. 5), the even main conjecture and the odd main conjecture (Sect. 4) are equivalent.*

Proof. By Theorem 6.2, 6.3 and (7.21), we have three exact sequences

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

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

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

The last sequence is for a non-trivial η. The theorem follows from these sequences and Proposition 7.1 ii). □

Theorem 4.1 also follows from Theorem 5.2 iii), iv), v) and the exact sequences in the proof of Theorem 7.4.

8. The construction of the even (odd) Coleman maps

8.1. A review of Honda's theory

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 elements $f(X) = \sum_{k=1}^{\infty} a_k X^k$ satisfying $ka_k \in \mathbb{Z}_p$ for all k. Let $\varphi(X) = (1+X)^p - 1$. We define an endomorphism φ of $\mathcal{P}$ by

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

We denote the n-iterated composition of the endomorphism φ of $\mathcal{P}$ by $\varphi^{(n)}$. For $u(t) = \sum_{\ell=0}^{\infty} b_\ell t^\ell \in \mathbb{Z}_p[[t]]$, we define an endomorphism $u(\varphi)$ of $\mathcal{P}$ by

$$u(\varphi)(f)(X) := \sum_{\ell=0}^{\infty} b_\ell f\big(\varphi^{(\ell)}(X)\big).$$

Lemma 8.1. *The action of 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. This follows from the congruence

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

(cf. Honda [4], Lemma 4.) □

Definition 8.2. *For $u(t) \in \mathbb{Z}_p[[t]]$, we say $f \in \mathcal{P}$ is of the Honda type u when $u(\varphi)(f) \equiv u(F)(f) \equiv 0 \mod p\mathbb{Z}_p[[X]]$ and $f'(0) = 1$.*

For a formal group $\mathcal{F}$ over $\mathbb{Z}_p$ of dimension 1, we denote the logarithm by $\log_{\mathcal{F}}$ and the exponential by $\exp_{\mathcal{F}}$. We remark that $\log_{\mathcal{F}}(X) \in \mathcal{P}$. We say a polynomial $u(t) = a_0 + a_1 t + \cdots + a_h t^h \in \mathbb{Z}_p[t]$ is an Eisenstein polynomial if a_h is a unit, $p \mid a_i$ for all $i \neq h$ and $a_0 = p$. Then Honda showed that there is a one-to-one correspondence between the isomorphism classes of commutative formal groups over $\mathbb{Z}_p$ of dimension 1 and Eisenstein polynomials in $\mathbb{Z}_p[t]$. More precisely,

Theorem 8.3 (Honda).

i) *Let $\mathcal{F}$ be a formal group of dimension 1 over $\mathbb{Z}_p$. Then there exists a unique Eisenstein polynomial u such that $\log_{\mathcal{F}}$ is of the Honda type u.*

ii) *Let $\mathcal{F}$ and $\mathcal{G}$ be formal groups over $\mathbb{Z}_p$ of dimension 1 whose logarithms are of the same Honda type u. Then $\exp_{\mathcal{G}} \circ \log_{\mathcal{F}}(X)$ is an element of $\mathbb{Z}_p[[X]]$ and gives an isomorphism $\mathcal{F} \xrightarrow{\sim} \mathcal{G}$.*

iii) *Let u be an Eisenstein polynomial. Then there exist an element of $\mathcal{P}$ of the Honda type u. If $f \in \mathcal{P}$ is of the Honda type u, there exists a formal group over $\mathbb{Z}_p$ with the logarithm f.*

Proof. The theorem is a combination of theorems and propositions in Honda [5]. See Theorem 2 and 4, Proposition 2.6 and 3.5 in Honda [5]. □

8.2. A formal group $\mathcal{F}_{ss}$

We consider the power series

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

This is an element of $\mathcal{P}$ and of the Honda type t^2+p. Hence by Theorem 8.3, there exists a formal group $\mathcal{F}_{ss}$ whose logarithm is given by $\log_{\mathcal{F}_{ss}}(X)$.

Theorem 8.4. *Let E be an elliptic curve over $\mathbb{Q}_p$ with good reduction at p. Let $\hat{E}$ be the formal group of the minimal model of E over $\mathbb{Z}_p$. Then $\log_{\hat{E}}(X)$ is of the Honda type $t^2 - a_p t + p$.*

Proof. See Honda [5], Theorem 9, p. 240. □

Corollary 8.5. *Suppose $a_p = 0$. Then the Artin-Hasse type power series $\exp_{\hat{E}} \circ \log_{\mathcal{F}_{ss}}(X) \in \mathbb{Z}_p[[X]]$ gives an isomorphism $\mathcal{F}_{ss} \to \hat{E}$.*

Proof. This follows from Theorem 8.3 and 8.4. □

Hence the p-adic Tate module of any elliptic curve with $a_p = 0$ is isomorphic to the p-adic Tate module of $\mathcal{F}_{ss}$.

8.3. Torsion subgroups of $\mathcal{F}_{ss}$

Proposition 8.6. *Over the integer ring of the unramified quadratic extension of $\mathbb{Q}_p$, the formal group $\mathcal{F}_{ss}$ is isomorphic to the Lubin-Tate formal group of height two with the parameter $-p$.*

Proof. This is well-known since $\mathcal{F}_{ss}$ is isomorphic to the formal group of an elliptic curve. However, we give another proof. It suffices to show that the multiplication $[-p]$ of $\mathcal{F}_{ss}$ 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. For ii), the multiplication $[-p]$ of $\mathcal{F}_{ss}$ is given by $\exp_{\mathcal{F}_{ss}}(-p \log_{\mathcal{F}_{ss}}(X))$, which is in $\mathbb{Z}_p[[X]]$ by Honda. Since $(\varphi^{(2)} + p) \log_{\mathcal{F}_{ss}}(X) \equiv 0$ modulo $p\,\mathbb{Z}_p[[X]]$, we have $\exp_{\mathcal{F}_{ss}}(-p \log_{\mathcal{F}_{ss}}(X)) \equiv \exp_{\mathcal{F}_{ss}}(\varphi^{(2)} \log_{\mathcal{F}_{ss}}(X)) \equiv \exp_{\mathcal{F}_{ss}}(\log_{\mathcal{F}_{ss}}(\varphi^{(2)}(X)))$ $\equiv \varphi^{(2)}(X)$ mod $p\,\mathbb{Z}_p[[X]]$. (cf. $\exp_{\mathcal{F}_{ss}}(p\mathbb{Z}_p[[X]]) = p\mathbb{Z}_p[[X]]$.) □

Proposition 8.7. *The formal group $\mathcal{F}_{ss}$ 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 F 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 $\mathcal{F}_{ss}$ to F by $F(\mathcal{F}_{ss}[p])$, which is an abelian extension of F of degree p^2-1 by the Lubin-Tate theory. Suppose that there is a p-torsion point in $\mathcal{F}_{ss}(\mathfrak{m}_L)$. Since $F(\mathcal{F}_{ss}[p])/F$ is abelian, all subextensions are normal over F. Therefore L contains all p-torsion points, namely, $L \supseteq F(\mathcal{F}_{ss}[p])$. However, the degree of L/F is $\phi(p^n) = p^n - p^{n-1}$, which is not a multiple of p^2-1. Hence we have a contradiction. □

8.4. Norm subgroups of $\mathcal{F}_{ss}$

Let $\mathfrak{m}_n$ be the maximal ideal of $\mathbb{Z}_p[\zeta_{p^{n+1}}]$ and $\mathfrak{m}_{-1} = p\mathbb{Z}_p$. For $m \geq n$, we denote the trace (norm) map $\mathcal{F}_{ss}(\mathfrak{m}_m) \to \mathcal{F}_{ss}(\mathfrak{m}_n)$ by $\mathrm{Tr}^{ss}_{m/n}$.

Since the logarithm of a formal group over $\mathbb{Z}_p$ is bijective on $p\mathbb{Z}_p$, there exists a unique element $\varepsilon \in p\mathbb{Z}_p$ such that $\log_{\mathcal{F}_{ss}}(\varepsilon) = \frac{p}{p+1}$.

Definition 8.8. *We define*

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

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

Lemma 8.9. *For a non-negative integer n, we have*

$$\mathrm{Tr}^{ss}_{n+1/n}\,(\mathrm{c}_{n+1}) = -\,\mathrm{c}_{n-1}, \quad \mathrm{Tr}^{ss}_{k_0/\mathbb{Q}_p}\,(\mathrm{c}_0) = -\,\mathrm{c}_{-2}.$$

Proof. By Proposition 8.7, $\log_{\mathcal{F}_{ss}}$ is injective on $\mathcal{F}_{ss}(\mathfrak{m}_n)$. Hence it suffices to show that the image of c_n by $\log_{\mathcal{F}_{ss}}$ satisfies the above relation. We have

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

The other case may be proved similarly. □

Definition 8.10. *We define the n-th norm subgroup* $\mathcal{C}_{ss}(\mathfrak{m}_n)$ *by*

$$\left\{P \in \mathcal{F}_{ss}(\mathfrak{m}_n) \;\middle|\; \mathrm{Tr}^{ss}_{n/m+1} P \in \mathcal{F}_{ss}(\mathfrak{m}_m) \text{ for } m\ (-1 \le m < n,\ m \equiv n \bmod 2)\right\}$$

for $n \ge 0$ *and* $\mathcal{C}_{ss}(\mathfrak{m}_{-1}) = \mathcal{F}_{ss}(\mathfrak{m}_{-1})$.

Proposition 8.11. *For* $n \ge 0$, *we have* $\log_{\mathcal{F}_{ss}}(\mathfrak{m}_n) \subseteq \mathfrak{m}_n + k_{n-1}$. *In particular, there exist canonical isomorphisms of* $\mathbb{Z}_p$*-modules*

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

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

Proof. As a set, $\mathcal{F}_{ss}(\mathfrak{m}_n)$ is the maximal ideal $\mathfrak{m}_n$, and we write $x \in \mathcal{F}_{ss}(\mathfrak{m}_n)$ of the form $x = \sum_i a_i\, \zeta_{p^{n+1}}^i$, $a_i \in \mathbb{Z}_p$. Then $x^{p^k} \equiv \sum_i a_i\, \zeta_{p^{n+1}}^{ip^k} \bmod p\mathbb{Z}_p[\zeta_{p^{n+1}}]$ and $y_k := \sum_i a_i\, \zeta_{p^{n+1}}^{ip^k} \in \mathfrak{m}_{n-1}$ for $k \ge 1$. Therefore by the congruence in the proof of Lemma 8.1, we have

$$\frac{(x+1)^{p^{2k}} - 1}{p^k} \equiv \frac{\left(x^{p^k}+1\right)^{p^k} - 1}{p^k} \equiv \frac{(y_k+1)^{p^k} - 1}{p^k} \mod \mathfrak{m}_n.$$

Hence we have $\frac{(x+1)^{p^{2k}}-1}{p^k} \in \mathfrak{m}_n + k_{n-1}$. For sufficiently large k_0, we have $\sum_{k=k_0}^{\infty} \frac{(x+1)^{p^{2k}}-1}{p^k} \in \mathfrak{m}_n$, and $\log_{\mathcal{F}_{ss}}(x) \in \mathfrak{m}_n + k_{n-1}$.

Since $\log_{\mathcal{F}_{ss}}$ is injective on $\mathcal{F}_{ss}(\mathfrak{m}_n)$ (cf. Proposition 8.7) and is compatible with the Galois action, we have $\log_{\mathcal{F}_{ss}} \mathfrak{m}_n \cap k_{n-1} = \log_{\mathcal{F}_{ss}} \mathfrak{m}_{n-1}$. Therefore we have an injection

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

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

Proposition 8.12. i) *The n-th norm subgroup* $\mathcal{C}_{ss}(\mathfrak{m}_n)$ *is generated by* $(\mathrm{c}_n^\sigma)_{\sigma \in \mathcal{G}_n}$ *as* $\mathbb{Z}_p$*-module.*
ii) *For a non-negative integer n, we have* $\mathcal{C}_{ss}(\mathfrak{m}_n) \cap \mathcal{C}_{ss}(\mathfrak{m}_{n-1}) = \mathcal{F}_{ss}(\mathfrak{m}_{-1})$ *and* $\mathcal{F}_{ss}(\mathfrak{m}_n) = \mathcal{C}_{ss}(\mathfrak{m}_n) + \mathcal{C}_{ss}(\mathfrak{m}_{n-1})$. *In other words, we have an exact sequence*

$$0 \to \mathcal{F}_{ss}(\mathfrak{m}_{-1}) \to \mathcal{C}_{ss}(\mathfrak{m}_n) \oplus \mathcal{C}_{ss}(\mathfrak{m}_{n-1}) \to \mathcal{F}_{ss}(\mathfrak{m}_n) \to 0 \qquad (8.22)$$

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

Proof. We first show that $\mathcal{C}_{ss}(\mathfrak{m}_n) \cap \mathcal{C}_{ss}(\mathfrak{m}_{n-1}) = \mathcal{F}_{ss}(\mathfrak{m}_{-1})$. Let $P \in \mathcal{C}_{ss}(\mathfrak{m}_n) \cap \mathcal{C}_{ss}(\mathfrak{m}_{n-1})$. We show that if $P \in \mathcal{F}_{ss}(\mathfrak{m}_m)$ then $P \in \mathcal{F}_{ss}(\mathfrak{m}_{m-1})$. Suppose that $n \equiv m-1 \mod 2$. Then by the definition of $\mathcal{C}_{ss}(\mathfrak{m}_n)$, we have $p^{n-m}\, P = \mathrm{Tr}^{ss}_{n/m}\, P \in \mathcal{F}_{ss}(\mathfrak{m}_{m-1})$. Therefore for $\sigma \in \mathrm{Gal}(k_m/k_{m-1})$, we have $p^{n-m}(P^\sigma - P) = 0$. Hence, by Proposition 8.7, $P \in \mathcal{F}_{ss}(\mathfrak{m}_{m-1})$. The case $n \equiv m \mod 2$ is shown similarly by considering $n-1$ instead of n in the above argument.

For the moment, let $\mathcal{C}'_{ss}(\mathfrak{m}_n)$ be the $\mathbb{Z}_p$-submodule generated by $(\mathrm{c}_n^\sigma)_{\sigma \in \mathcal{G}_n}$. We prove $\mathcal{C}_{ss}(\mathfrak{m}_n) = \mathcal{C}'_{ss}(\mathfrak{m}_n)$ and $\mathcal{F}_{ss}(\mathfrak{m}_n) = \mathcal{C}_{ss}(\mathfrak{m}_n) + \mathcal{C}_{ss}(\mathfrak{m}_{n-1})$ by induction. Suppose they are true for $n-1$. Then by the inductive hypothesis and Lemma 8.9, we have $\mathcal{F}_{ss}(\mathfrak{m}_{n-1}) = \mathcal{C}_{ss}(\mathfrak{m}_{n-1}) + \mathcal{C}_{ss}(\mathfrak{m}_{n-2})$ and

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

Therefore, by Proposition 8.11, we have

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

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

Corollary 8.13. *Let* $q_n = \sum_{k=0}^{n} (-1)^{n-k} p^k$ *and let* $\eta : \Delta \to \mathbb{Z}_p^\times$ *a character. Then* $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{C}_{ss}(\mathfrak{m}_n)^\eta = q_n + \delta$ *where* $\delta = 1$ *if* $\eta = 1$ *and* n *is odd, otherwise,* $\delta = 0$.

Proof. Since the $\mathbb{Z}_p$-rank of $\mathcal{F}_{ss}(\mathfrak{m}_n)^\eta$ is p^n, the corollary follows from Proposition 8.12 ii) by induction. □

Remark 8.14. Let $N = \mathrm{Tr}^{ss}_{n+1/n}$. By Lemma 8.9 and Proposition 8.12, we can also show that

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

8.5. The construction of Coleman maps

Let $E/\mathbb{Q}_p$ be an elliptic curve with good reduction and $a_p = 0$. Let T be the Tate module of E and $V = T \otimes \mathbb{Q}_p$. Then by Corollary 8.5, the Artin-Hasse type power series $\exp_{\hat{E}} \circ \log_{\mathcal{F}_{ss}}(X)$ induces an isomorphism $i : \mathcal{F}_{ss} \to \hat{E}$. We regard $\mathcal{F}_{ss}(\mathfrak{m}_n) \subseteq H^1(k_n, T)$ by the composition of i and the Kummer map. Then the cup product induces a pairing

$$(\ ,\ )_n : \mathcal{F}_{ss}(\mathfrak{m}_n) \times H^1(k_n, T) \to H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p. \tag{8.23}$$

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

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

This morphism is compatible with the natural Galois action.

Lemma 8.15. *The morphisms $P_{n,x}$ are compatible*:

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

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 $(\mathrm{c}_n^+)_{n\geq 0}$, $(\mathrm{c}_n^-)_{n\geq 0}$, $\mathrm{c}_n^+, \mathrm{c}_n^- \in \mathcal{F}_{ss}(\mathfrak{m}_n)$, by

$$\mathrm{c}_n^+ : -\mathrm{c}_0,\ -\mathrm{c}_0,\ \mathrm{c}_2,\ \mathrm{c}_2,\ -\mathrm{c}_4,\ \ldots, \quad \mathrm{c}_n^- : \mathrm{c}_{-1},\ -\mathrm{c}_1,\ -\mathrm{c}_1,\ \mathrm{c}_3,\ \mathrm{c}_3,\ \ldots.$$

Namely,

$$\mathrm{c}_n^+ = \begin{cases} (-1)^{\frac{n+2}{2}}\,\mathrm{c}_n & \text{if } n \text{ is even,} \\ (-1)^{\frac{n+1}{2}}\,\mathrm{c}_{n-1} & \text{if } n \text{ is odd,} \end{cases} \qquad \mathrm{c}_n^- = \begin{cases} (-1)^{\frac{n+1}{2}}\,\mathrm{c}_n & \text{if } n \text{ is odd,} \\ (-1)^{\frac{n}{2}}\,\mathrm{c}_{n-1} & \text{if } n \text{ is even.} \end{cases}$$

(cf. Definition 8.8.)

Definition 8.16. *We define the n-th norm subgroup and the n-th even norm subgroup and the n-th odd norm subgroup of $\hat{E}(\mathfrak{m}_n)$ by*

$$\mathcal{C}_{\hat{E}}(\mathfrak{m}_n) = \{P \in \hat{E}(\mathfrak{m}_n) \mid \mathrm{Tr}_{n/m+1} P \in \hat{E}(\mathfrak{m}_m) \quad \textit{for } m\ (-1 \leq m < n,\ m \equiv n \bmod 2)\},$$
$$\hat{E}^+(\mathfrak{m}_n) = \{P \in \hat{E}(\mathfrak{m}_n) \mid \mathrm{Tr}_{n/m+1} P \in \hat{E}(\mathfrak{m}_m) \quad \textit{for even } m\ (0 \leq m < n)\},$$
$$\hat{E}^-(\mathfrak{m}_n) = \{P \in \hat{E}(\mathfrak{m}_n) \mid \mathrm{Tr}_{n/m+1} P \in \hat{E}(\mathfrak{m}_m) \quad \textit{for odd } m\ (-1 \leq m < n)\},$$

where $\mathrm{Tr}_{n/m+1} : \hat{E}(\mathfrak{m}_n) \to \hat{E}(\mathfrak{m}_{m+1})$ *is the trace map of* $\hat{E}$.

The relations between these groups are

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

By Proposition 8.12 i), the group $\hat{E}^{\pm}(\mathfrak{m}_n)$ is generated by the image of $\mathrm{c}_n^{\pm}$ by i as $\mathbb{Z}_p[\mathcal{G}_n]$-module.

Lemma 8.17. *The Kummer map induces an injection* $\hat{E}^{\pm}(\mathfrak{m}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(k_n, V/T)$.

Proof. It suffices to show that the natural map $\hat{E}^{\pm}(\mathfrak{m}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \hat{E}(\mathfrak{m}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is injective. Suppose we have $P = p^k Q$ where $P \in \hat{E}^{\pm}(\mathfrak{m}_n)$ and $Q \in \hat{E}(\mathfrak{m}_n)$. Let $R = \mathrm{Tr}_{n/m+1} Q$. Then if $(-1)^m = \pm 1$, we have $p^k(R^\sigma - R) = 0$ for all $\sigma \in \mathrm{Gal}(k_{m+1}/k_m)$. Hence by Proposition 8.7, we have $R \in \hat{E}(\mathfrak{m}_m)$ and $Q \in \hat{E}^{\pm}(\mathfrak{m}_n)$. □

Let $H^1_\pm(k_n, T)$ be the exact annihilator with respect to the Tate pairing

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

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

We define $P_n^\pm = P_{n,\, \mathrm{c}_n^\pm}$.

Proposition 8.18. *The kernel of $P_n^\pm$ is $H^1_\pm(k_n, T)$.*

Proof. By the definition of $P_n^\pm$, we have an exact sequence

$$0 \to \mathrm{Ker}\, P_n^\pm \to H^1(k_n, T) \to \mathrm{Hom}(\hat{E}^\pm(\mathfrak{m}_n),\ \mathbb{Z}_p)$$

where the last morphism is induced by the cup product. Taking the Pontryagin dual of this sequence and by Lemma 8.17, we have

$$0 \to \hat{E}^\pm(\mathfrak{m}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(k_n, V/T) \to \left(\mathrm{Ker}\, P_n^\pm\right)^\vee \to 0.$$

The proposition follows from this sequence. □

Next we study the image of $P_n^\pm$.

Let $\Phi_n(X)$ be the p^n-th cyclotomic polynomial. We let $\omega_n(X) = (1+X)^{p^n} - 1$, $\widetilde{\omega}_0^\pm(X) = 1$ and

$$\widetilde{\omega}_n^+(X) = \prod_{2 \le m \le n,\ m:\text{even}} \Phi_m(1+X), \quad \widetilde{\omega}_n^-(X) = \prod_{1 \le m \le n,\ m:\text{odd}} \Phi_m(1+X). \tag{8.24}$$

(cf. (6.8) and (6.9).)

We identify $\Lambda_n = \mathbb{Z}_p[\mathcal{G}_n]$ with $\mathbb{Z}_p[\Delta][X]/(\omega_n(X))$ by sending γ_n to $1+X$, where γ_n is the image of γ in Λ_n.

Proposition 8.19. *The image of $P_n^\pm$ is contained in $\widetilde{\omega}_n^\mp(X)\ \Lambda_n$.*

Proof. We prove the proposition for P_n^+. The other case is proved similarly. We consider a morphism

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

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

By Lemma 8.9 and 8.15, we have $p^{-[\frac{n+1}{2}]}\psi \circ P_n^+ = p^{-[\frac{m+1}{2}]}\psi \circ P_m^+ \circ \mathrm{Cor}_{n/m}$ where $\mathrm{Cor}_{n/m}$ is the corestriction map. Therefore we may assume that $m = n$. Then

$$\begin{aligned}\psi \circ P_n^+(z) &= (-1)^{\frac{n+1}{2}} \sum_{\sigma \in \mathcal{G}_n} \left(\mathrm{c}_{n-1}^{\sigma}, z\right)_n \psi(\sigma) \\ &= (-1)^{\frac{n+1}{2}} \sum_{\tau \in \mathcal{G}_{n-1}} \left(\mathrm{c}_{n-1}^{\tau}, z\right)_n \sum_{\sigma \in \mathcal{G}_n,\, \overline{\sigma} \equiv \tau} \psi(\sigma) = 0\end{aligned}$$

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

Since $\omega_n(X) = \widetilde{\omega}_n^{\mp}(X)\, \omega_n^{\pm}(X)$, the multiplication by $\widetilde{\omega}_n^{\mp}(X)$ induces an isomorphism

$$\Lambda_n^{\pm} := \mathbb{Z}_p[\Delta][X]/\left(\omega_n^{\pm}(X)\right) \xrightarrow{\simeq} \widetilde{\omega}_n^{\mp}(X)\, \Lambda_n. \tag{8.25}$$

Corollary 8.20. *There exists a unique morphism* $\mathrm{Col}_n^{\pm}$ *which makes the following diagram commutative.*

$$\begin{array}{ccc} H^1(k_n, T) & \xrightarrow{\mathrm{Col}_n^{\pm}} & \Lambda_n^{\pm} \\ \downarrow & & \downarrow \times \widetilde{\omega}_n^{\mp} \\ \dfrac{H^1(k_n, T)}{H^1_{\pm}(k_n, T)} & \xrightarrow{P_n^{\pm}} & \Lambda_n. \end{array}$$

Proof. This follows from Proposition 8.18, 8.19 and (8.25). □

We call $\mathrm{Col}_n^{\pm}$ the n-th even (odd) Coleman map.

Proposition 8.21. *The even (odd) Coleman maps are compatible*:

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

where the vertical maps are the corestriction and the projection.

Proof. We prove the proposition for Col_n^{+}. The compatibility for Col_n^{-} is proved similarly. For an odd n, we consider a diagram

$$\begin{array}{ccccc} H^1(k_{n+1}, T) & \xrightarrow{P_{n+1}^{+}} & \widetilde{\omega}_{n+1}^{-}(X)\, \Lambda_{n+1} & \xrightarrow{\simeq} & \Lambda_{n+1}^{+} \\ \downarrow & & \downarrow \mathrm{proj} & & \downarrow \\ H^1(k_n, T) & \xrightarrow{P_n^{+}} & \widetilde{\omega}_n^{-}(X)\, \Lambda_n & \xrightarrow{\simeq} & \Lambda_n^{+} \end{array} \tag{8.26}$$

where the vertical maps are the corestriction and the projection. By Lemma 8.9, 8.15 and $\widetilde{\omega}^{-}_{n+1}(X) = \widetilde{\omega}^{-}_{n}(X)$, the diagram (8.26) is commutative. For an even n, we consider a diagram

$$\begin{array}{ccccc} H^1(k_{n+1}, T) & \xrightarrow{P^+_{n+1}} & \widetilde{\omega}^{-}_{n+1}(X)\, \Lambda_{n+1} & \xrightarrow{\simeq} & \Lambda^+_{n+1} \\ \downarrow & & \downarrow{\scriptstyle \times \frac{1}{p}} & & \downarrow \\ H^1(k_n, T) & \xrightarrow{P^+_n} & \widetilde{\omega}^{-}_{n}(X)\, \Lambda_{n} & \xrightarrow{\simeq} & \Lambda^+_{n} \end{array} \tag{8.27}$$

where the left vertical map is the corestriction and the right vertical map is the projection. Since $\Phi_{n+1}(1+X) = \sum_{i=0}^{p-1} (1+X)^{p^n i} \equiv p \bmod \omega_n(X)$, we have $\widetilde{\omega}^{-}_{n+1}(X) = p\, \widetilde{\omega}^{-}_{n}(X)$ in Λ_n. The commutativity of the right square in (8.27) follows from this fact. The commutativity of the left square follows from the fact $\mathrm{c}^+_{n+1} = \mathrm{c}^+_n$ and Lemma 8.15. □

Definition 8.22. *We define the even (odd) Coleman map*

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

as the limit of the even (odd) Coleman map $\mathrm{Col}^{\pm}_n : H^1(k_n, T) \to \Lambda^{\pm}_n$.

We remark that

$$\varprojlim_n \Lambda^{\pm}_n = \varprojlim_n \mathbb{Z}_p[\Delta][X]/\big(\omega^{\pm}_n(X)\big) = \mathbb{Z}_p[\Delta][[X]] = \Lambda.$$

8.6. The image of the even (odd) Coleman map

Proposition 8.23. *The Coleman maps* Col^+_n *and* Col^+ *are surjective.*

Proof. We first show that the 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 that the kernel of the restriction map $H^1(k_n, V/T) \to H^1(k_m, V/T)$ is zero. By the inflation-restriction sequence, the kernel is equal to $H^1(\mathrm{Gal}(k_m/k_n), H^0(k_m, V/T))$, and $H^0(k_m, V/T) = 0$ by Proposition 8.7.

Next we show that the 0-th even Coleman map $\mathrm{Col}^+_0 = P^+_0 : H^1(k_0, T) \to \mathbb{Z}_p[\Delta]$ is surjective. Then, by Nakayama's lemma, Col^+_n and Col^+ are surjective.

By Proposition 8.12 i) and Corollary 8.13, the elements $(\mathrm{c}^{\sigma}_0)_{\sigma\in\Delta}$ become a basis of $\mathcal{F}_{ss}(\mathfrak{m}_0)$ as $\mathbb{Z}_p$-module. Then P^+_0 is described as

$$H^1(k_0, T) \to \mathrm{Hom}(\mathcal{F}_{ss}(\mathfrak{m}_0), \mathbb{Z}_p) \cong \mathbb{Z}_p[\Delta]$$

where the first map is induced by the pairing (8.23) and the last identification is $f \mapsto -\sum_{\sigma\in\Delta} f(\mathrm{c}^{\sigma}_0)\, \sigma$. The morphism $H^1(k_0, T) \to \mathrm{Hom}(\mathcal{F}_{ss}(\mathfrak{m}_0), \mathbb{Z}_p)$ is a surjection since its Pontryagin dual is the injection $\mathcal{F}_{ss}(\mathfrak{m}_0) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(k_0, V/T)$. □

For characters $\eta : \Delta \to \mathbb{Z}_p^\times$, we decompose the odd Coleman maps to the η-components

$$\varepsilon_\eta \mathrm{Col}_n^- : H^1(k_n, T)^\eta \longrightarrow \varepsilon_\eta \Lambda_n^-.$$

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

$$I_n = \mathrm{Ker}\,(\ \mathbb{Z}_p[\Delta][\Gamma_n] \longrightarrow \mathbb{Z}_p[\Delta]\ )$$

where Γ_n is the quotient of Γ isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$ and the map is induced by $\Gamma_n \to \{1\}$. We denote $I := \varprojlim_n I_n = X\Lambda$ and $I_n^\pm := X\Lambda_n^\pm$.

Proposition 8.24. *If η is trivial, then $\varepsilon_\eta \mathrm{Col}_n^-$ and $\varepsilon_\eta \mathrm{Col}^-$ are surjective. If η is non-trivial, the image of $\varepsilon_\eta \mathrm{Col}_n^-$ is the augmentation ideal $(I_n^-)^\eta$ and the image of $\varepsilon_\eta \mathrm{Col}^-$ is I^η.*

Proof. The proof is similar to that of Proposition 8.23. The difference is, for the component of a non-trivial η, we have to prove the surjectivity of the first Coleman map

$$\varepsilon_\eta \mathrm{Col}_1^- : H^1(k_1, T)^\eta \longrightarrow (\Lambda_1^-)^\eta$$

to the augmentation ideal. We have $\Lambda_1^- = \Lambda_1$ and $\mathrm{Col}_1^- = P_1^-$.

For $\sigma \in \mathcal{G}_1$, let $d^\sigma = \varepsilon_\eta \mathrm{c}_1^\sigma$. Then $d^{\sigma\tau} = \eta(\tau)\, d^\sigma$ for $\tau \in \Delta$ and by Lemma 8.9, $\sum_{\sigma \in \Gamma_1} d^\sigma = \varepsilon_\eta\, \mathrm{c}_{-1} = 0$. Therefore by Proposition 8.12 i) and Corollary 8.13, $(d^\sigma)_{\sigma \in \Gamma_1,\, \sigma \neq 1}$ becomes a basis of $\mathcal{C}_{ss}(\mathfrak{m}_1)^\eta$. Hence we have an isomorphism

$$\mathrm{Hom}\big(\mathcal{C}_{ss}(\mathfrak{m}_1)^\eta, \mathbb{Z}_p\big) \cong I_1^\eta, \quad f \mapsto -\varepsilon_\eta \sum_{\sigma \in \Gamma_1} f(d^\sigma)\, \sigma.$$

Then the morphism $\varepsilon_\eta \mathrm{Col}_1^- = -\varepsilon_\eta P_{1,\,\mathrm{c}_1}$ is described as

$$H^1(k_1, T)^\eta \to \mathrm{Hom}\big(\mathcal{F}_{ss}(\mathfrak{m}_1)^\eta, \mathbb{Z}_p\big) \to \mathrm{Hom}\big(\mathcal{C}_{ss}(\mathfrak{m}_1)^\eta, \mathbb{Z}_p\big) \cong I_1^\eta$$

where the first map is induced by the pairing (8.23) and the second map is the projection by the decomposition $\mathcal{F}_{ss}(\mathfrak{m}_1)^\eta = \mathcal{C}_{ss}(\mathfrak{m}_1)^\eta \oplus \mathcal{C}_{ss}(\mathfrak{m}_0)^\eta$ (cf. Proposition 8.12). The surjectivity of $H^1(k_1, T)^\eta \to \mathrm{Hom}(\mathcal{F}_{ss}(\mathfrak{m}_1)^\eta, \mathbb{Z}_p)$ is proved as in the proof of Proposition 8.23. □

Now Theorem 6.2 follows from Proposition 8.18, 8.23 and 8.24.

8.7. Coleman maps in terms of the dual exponential maps

We give a description of Coleman maps in terms of the dual exponential maps. Then it turns out that our Coleman maps are similar to the explicit Coleman map in the appendix in Rubin [21]. It also turns out that $P_{n,x}$ in Sect. 8.5 is obtained by Kurihara's P_n-pairing (Kurihara [9], Sect. 3).

We recall the dual exponential maps following Rubin [21]. 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 $\operatorname{cotan}(E/k_n)$ is $k_n\,\omega_E$, and we let ω_E^* be the corresponding dual basis of $\tan(E/k_n)$. Then we have a commutative diagram

$$\begin{array}{ccccc}
\log_{\mathcal{F}_{ss}}(\mathfrak{m}_n) & \xleftarrow{\log_{\mathcal{F}_{ss}}} & \mathcal{F}_{ss}(\mathfrak{m}_n) & & \\
\| & & \downarrow{\scriptstyle \exp_{\hat{E}}\circ\log_{\mathcal{F}_{ss}}} & & \\
\log_{\hat{E}}(\mathfrak{m}_n) & \xleftarrow{\log_{\hat{E}}} & \hat{E}(\mathfrak{m}_n) & \longrightarrow & E_1(k_n) \\
{\scriptstyle \cdot\omega_E^*}\downarrow & & & & \downarrow \\
\tan(E/k_n) & & \xrightarrow{\exp_E} & & E(k_n)\otimes\mathbb{Q}_p
\end{array} \tag{8.28}$$

There is a dual exponential map

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

which has a property

$$(x, z)_n = \operatorname{Tr}_{k_n/\mathbb{Q}_p} \log_{\hat{E}}(x)\ \exp^*_{\omega_E}(z) \tag{8.29}$$

for every $x \in \hat{E}(\mathfrak{m}_n)$ and $z \in H^1(k_n, V)$. Here $(\ ,\ )_n$ is the Tate pairing and $\exp^*_{\omega_E} = \omega_E^* \circ \exp_E^*$. (See formula (2) in Sect. 5 of Rubin [21].)

Proposition 8.25. *The morphism $P_{n,x}$ in Sect. 8.5 is described in terms of the dual exponential map as follows.*

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

Proof. The formula follows from the diagram (8.28) and the formula (8.29). See also the appendix of Rubin [21]. □

Proposition 8.26. *Let ψ be a character of $\mathcal{G}_n$ of conductor p^{m+1}. Then we have*

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

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

Here $\tau(\psi)$ is the Gauss sum $\sum_{\sigma\in\mathcal{G}_m} \psi(\sigma)\, \zeta_{p^{m+1}}^\sigma$.

Proof. Since $p^{-[\frac{n+1}{2}]} \log_{\mathcal{F}_{ss}}(\mathrm{c}_n^+)$ and $p^{-[\frac{n}{2}]} \log_{\mathcal{F}_{ss}}(\mathrm{c}_n^-)$ are norm compatible, we may assume that $m = n$. Then the formula is obtained by direct calculations as in the proof of Lemma 8.9. □

Now we prove Theorem 6.3.

Proof of Theorem 6.3. It suffices to show that $\mathrm{Col}^\pm(\mathbf{z}^{\eta(-1)})\,\varepsilon_\eta$ has interpolation properties (3.4) and (3.5).

Let $\chi : \mathcal{G}_n \to \mu_{p^\infty}$ be a Dirichlet character of conductor p^{n+1}. Let $\psi = \eta\chi$. Suppose n is even. Then by Corollary 8.20, we have $\psi \circ P_n^+ = \widetilde{\omega}_n^-(\zeta - 1)\, \pi_\psi \circ \mathrm{Col}_n^+$ where $\chi(\gamma_n) = \zeta$ and $\pi_\psi : \Lambda_n^+ \to \overline{\mathbb{Q}_p}$, $X \mapsto \zeta - 1$. Hence by Proposition 8.25, 8.26 and Theorem 5.2, $\varepsilon_\eta\, \mathrm{Col}_n^+(\mathbf{z}^{\eta(-1)})$ has the properties (3.4) and (3.5). We remark that $\tau(\psi)\,\tau(\overline{\psi}) = \psi(-1)\, p^{n+1}$. The other case is shown similarly by considering odd n. □

9. A control theorem for the even (odd) Selmer group

Lemma 9.1. *The morphisms $\mathrm{Sel}^\pm(E/K_n) \to \mathrm{Sel}^\pm(E/K_\infty)$ are injective.*

Proof. The lemma follows from the inflation-restriction sequence for $H^1(K_n, V/T) \to H^1(K_\infty, V/T)$ and the fact that $E(K_\infty)_{p^\infty} = 0$ (cf. Proposition 8.7). □

Proposition 9.2. *Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character. The natural maps*

$$\varprojlim_m H_+^1(k_m, T) \to H_+^1(k_n, T)/\omega_n^+(\gamma - 1)H^1(k_n, T) \tag{9.30}$$

$$\varprojlim_m H_-^1(k_m, T)^\Delta \to H_-^1(k_n, T)^\Delta/\omega_n^-(\gamma - 1)H^1(k_n, T)^\Delta \tag{9.31}$$

$$\varprojlim_m H_-^1(k_m, T)^\eta \to H_-^1(k_n, T)^\eta/\widetilde{\omega}_n^-(\gamma - 1)H^1(k_n, T)^\eta \tag{9.32}$$

are surjective. The last morphism is for a non-trivial η.

Proof. We prove the surjectivity for (9.30). The other cases may be proved similarly.

Since $H^1(k_n, T)/H^1_+(k_n, T) \cong \Lambda/(\omega_n^+(X))$ by Theorem 6.2, we have

$$\omega_n^+(\gamma - 1)\, H^1(k_n, T) \subset H^1_+(k_n, T).$$

For simplicity, we write $H^1_{+,n} = H^1_+(k_n, T)$, and consider a commutative diagram

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

By Theorem 6.2, the right vertical map is an isomorphism. Since $\varprojlim_m H^1(k_m, T) \to H^1(k_n, T)$ is surjective by Proposition 8.7, the middle vertical map is surjective. Hence the proposition follows from the snake lemma. □

For simplicity, we write $\mathcal{X}^{\pm}_{\infty} = \mathcal{X}^{\pm}(E/K_{\infty})$ and $\mathcal{X}_n = \mathcal{X}(E/K_n)$. We also abbreviate $\omega_n^{\pm}(\gamma - 1)$ to $\omega_n^{\pm}$, and similarly for $\widetilde{\omega}_n^{\pm}$.

Theorem 9.3. *The natural maps*

$$\begin{aligned} \mathcal{X}^{+}_{\infty}/\omega_n^{+}\mathcal{X}^{+}_{\infty} &\longrightarrow \mathcal{X}^{+}_{n}/\omega_n^{+}\mathcal{X}^{+}_{n}, \\ \mathcal{X}^{-,\Delta}_{\infty}/\omega_n^{-}\mathcal{X}^{-,\Delta}_{\infty} &\longrightarrow \mathcal{X}^{-,\Delta}_{n}/\omega_n^{-}\mathcal{X}^{-,\Delta}_{n}, \\ \mathcal{X}^{-,\eta}_{\infty}/\widetilde{\omega}_n^{-}\mathcal{X}^{-,\eta}_{\infty} &\longrightarrow \mathcal{X}^{-,\eta}_{n}/\widetilde{\omega}_n^{-}\mathcal{X}^{-,\eta}_{n} \quad \textit{for } \eta \neq 1 \end{aligned}$$

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

Proof. We prove the theorem for the even Selmer groups. The other cases may be proved similary. We prove the Pontryagin dual of the theorem by similar arguments as in Greenberg [2, Sect. 3]. For a Λ-module M, we let

$$M^{\omega_n^+=0} = \left\{ x \in M \;\middle|\; \omega_n^+(\gamma - 1)\, x = 0 \right\}.$$

We also let $\mathcal{H}^+(K_{n,v}) = H^1(K_{n,v}, V/T)^{\omega_n^+=0}/(E^+(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$. Then, taking the dual of Proposition 9.2, the morphism

$$\mathcal{H}^+(k_n) \to \varinjlim_m \mathcal{H}^+(k_m) \tag{9.33}$$

is injective. Let us consider a diagram

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

The morphism s_n is injective by Lemma 9.1. If the superscript $\omega_n^+ = 0$ is replaced by $\omega_n = 0$, then the morphism h_n is bijective by the inflation-restriction sequence. Hence a posteriori, h_n is bijective. By Lemma 3.3 in Greenberg [2], for $v \not| p$, the kernel of $r_v : \mathcal{H}^+(K_{n,v}) \to \varinjlim_m \mathcal{H}^+(K_{m,v})$ is finite of bounded order. For $v \mid p$, the kernel of r_v is zero by (9.33). Hence the kernel of g_n is finite of bounded order as n varies. The theorem follows from the snake lemma. □

The following is half of the p-adic Birch and Swinnerton-Dyer conjecture, which is already proved in Kato [7].

Theorem 9.4.

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

In particular, we have

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

Proof. By Theorem 9.3, we have a pseudo-isomorphism

$$\mathcal{X}_\infty^{\pm,\Delta}/(\gamma-1)\mathcal{X}_\infty^{\pm,\Delta} \cong \mathcal{X}_0^{\pm,\Delta}/(\gamma-1)\mathcal{X}_0^{\pm,\Delta} = \mathcal{X}_0^{\pm,\Delta} = \mathcal{X}_0^{\Delta}.$$

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

10. An asymptotic formula for the order of $Ш(E/K_n)$

We give an asymptotic formula for the p-adic order of the Tate-Shafarevich group $Ш(E/K_n)$ in terms of the λ- and μ-invariants of the even and the odd Selmer groups. Similar formulas have been obtained by Kurihara and Perrin-Riou [17] for unspecified rational numbers λ and μ.

10.1. The even (odd) λ- and μ-invariants

Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character. We denote the λ- and the μ-invariants of $\mathcal{X}^\pm(E/K_\infty)^\eta$ by $\lambda_\pm^\eta$ and $\mu_\pm^\eta$. As in the good ordinary case, we can bound the corank of the Selmer groups by these invariants.

Let $\mathrm{Sel}^1(E/K_n) := \mathrm{Ker}\left(\mathrm{Sel}(E/K_n) \longrightarrow \dfrac{H^1(k_n, E[p^\infty])}{E(\mathbb{Q}_p)\otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)$.

By (8.22), we have an exact sequence

$$0 \to \mathrm{Sel}^1(E/K_n) \xrightarrow{i} \mathrm{Sel}^+(E/K_n) \oplus \mathrm{Sel}^-(E/K_n) \xrightarrow{j} \mathrm{Sel}(E/K_n)$$

where i is the diagonal embedding and j is $(x, y) \mapsto x - y$.

Proposition 10.1. *The cokernel of j is finite.*

Proof. Since $\mathrm{Sel}(E/K_n)^\vee$ is a finitely generated $\mathbb{Z}_p$-module, it suffices to show that the image of the morphism j contains the p-divisible part of $\mathrm{Sel}(E/K_n)$. Since $\mathrm{Tr}_{k/k-1}$ is given by the p^k-th cyclotomic polynomial $\Phi_k(\gamma)$, we have $\widetilde{\omega}_n^-(\gamma - 1)\, Q \in \mathrm{Sel}^+(E/K_n)$ for every $Q \in \mathrm{Sel}(E/K_n)$. Similarly, $\omega_n^+(\gamma - 1)\, Q \in \mathrm{Sel}^-(E/K_n)$ for every $Q \in \mathrm{Sel}(E/K_n)$. Since $\omega_n^+(X)$ and $\widetilde{\omega}_n^-(X)$ are mutually prime in $\mathbb{Q}_p[X]$, there exist $A(X), B(X) \in \mathbb{Z}_p[X]$ such that $A(X)\,\widetilde{\omega}_n^-(X) - B(X)\,\omega_n^+(X) = p^m$ for some integer m. Let P be a p-divisible element of $\mathrm{Sel}(E/K_n)$ and let $Q \in \mathrm{Sel}(E/K_n)$ be such that $P = p^m Q$. We put $P^+ = A(\gamma - 1)\,\widetilde{\omega}_n^-(\gamma - 1)\, Q$ and $P^- = B(\gamma - 1)\,\omega_n^+(\gamma - 1)\, Q$. Then $P^\pm \in \mathrm{Sel}^\pm(E/K_n)$ and $P = (P^+ - P^-)$. □

Corollary 10.2. *For every n, we have*

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

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

Proof. This follows from Lemma 9.1, Proposition 10.1 and the facts that $\mathrm{Sel}^1(E/K_n) \supseteq \mathrm{Sel}(E/\mathbb{Q})$ and $\mathrm{Sel}(E/K_n) \supseteq E(K_n)\otimes \mathbb{Q}_p/\mathbb{Z}_p$. □

10.2. An asymptotic formula

The (p-primary) Tate-Shafarevich group is defined by

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

By definition, we have an exact sequence

$$0 \to E(K_n)\otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}(E/K_n) \to Ш(E/K_n) \to 0. \qquad (10.34)$$

In the following, we always assume that $Ш_n := Ш(E/K_n)$ is finite for all n. We first show elementary lemmas.

Lemma 10.3. *For an exact sequence of Λ-modules $0 \to A \to B \to C \to 0$, we have*

$$0 \to A^{\Gamma_n} \to B^{\Gamma_n} \to C^{\Gamma_n} \to A_{\Gamma_n} \to B_{\Gamma_n} \to C_{\Gamma_n} \to 0.$$

Proof. For a generater $\gamma_n \in \Gamma_n$, we consider a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \times(\gamma_n-1)} & & \downarrow{\scriptstyle \times(\gamma_n-1)} & & \downarrow{\scriptstyle \times(\gamma_n-1)} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0. \end{array}$$

The lemma follows from the snake lemma. □

Let $(M_n)_{n=1,2,\ldots}$ be a projective system of finitely generated $\mathbb{Z}_p$-modules. If $\pi_n : M_n \to M_{n-1}$ has finite kernel and cokernel, then we define

$$\nabla M_n := \mathrm{length}_{\mathbb{Z}_p}(\mathrm{Ker}\,\pi_n) - \mathrm{length}_{\mathbb{Z}_p}(\mathrm{Coker}\,\pi_n) + \dim_{\mathbb{Q}_p} M_{n-1} \otimes \mathbb{Q}_p.$$

Lemma 10.4. i) *Suppose we have an exact sequence $0 \to (M'_n) \to (M_n) \to (M''_n) \to 0$. If two of ∇M_n, $\nabla M'_n$, $\nabla M''_n$ are defined, then the other is also defined and $\nabla M_n = \nabla M'_n + \nabla M''_n$.*

ii) *Suppose that M_n are constant. If M_n is finite or the transition map $M_n \to M_{n-1}$ is given by the multiplication by p, then $\nabla M_n = 0$.*

Proof. This is straightforward. □

We write $\omega_n(X) = (1+X)^{p^n} - 1$ simply by ω_n.

Lemma 10.5. i) *For $f \in R := \mathbb{Z}_p[[X]]$, we let $R_{f,n} = R/(f, \omega_n)$. We consider a natural projective system $(R_{f,n})_n$. If $f(\zeta_{p^n} - 1) \neq 0$, then the number $\nabla R_{f,n}$ is defined and*

$$\nabla R_{f,n} = \mathrm{ord}_{\zeta_{p^n}-1} f(\zeta_{p^n} - 1).$$

ii) *Let M be a finitely generated torsion R-module with the characteristic polynomial f, and let $M_n = M/\omega_n M$. We consider a natural projective system $(M_n)_n$. Then for sufficiently large n, ∇M_n is defined and*

$$\nabla M_n = \mathrm{ord}_{\zeta_{p^n}-1} f(\zeta_{p^n} - 1) = \lambda(M) + \phi(p^n)\mu(M),$$

where $\lambda(M)$ and $\mu(M)$ are the λ- and the μ-invariants of M.

Proof. Let h be the common divisor of f and ω_{n-1}, and we write $f = gh$. Then $R_{f,n-1} \otimes \mathbb{Q}_p = \oplus_{m \leq n-1} R \otimes \mathbb{Q}_p / (f, \Phi_m)$ and

$$\dim_{\mathbb{Q}_p} R_{f,n-1} \otimes \mathbb{Q}_p = \sum_{\Phi_m | h} \phi(p^m) = \deg h = \mathrm{ord}_{\zeta_{p^n}-1} h(\zeta_{p^n} - 1).$$

On the other hand, by direct computation, the kernel of the projection $\pi_n : R_{f,n} \to R_{f,n-1}$ is isomorphic to $R/(g, \Phi_n)$ and

$$\text{length}_{\mathbb{Z}_p} \text{Ker}\, \pi_n = \text{length}_{\mathbb{Z}_p} R/(g, \Phi_n) = \text{ord}_{\zeta_{p^n}-1} g(\zeta_{p^n} - 1).$$

Hence we have

$$\nabla R_{f,n} = \text{length}_{\mathbb{Z}_p} \text{Ker}\, \pi_n + \dim_{\mathbb{Q}_p} R_{f,n-1} \otimes \mathbb{Q}_p = \text{ord}_{\zeta_{p^n}-1} f(\zeta_{p^n} - 1).$$

Let us prove ii). By the structure theorem, we have a pseudo-isomorphism

$$0 \to A \to M \xrightarrow{\varrho} \oplus_i R/f_i \to B \to 0$$

where A and B are finite groups. Then by Lemma 10.3, we have

$$(\oplus_i R/f_i)^{\Gamma_n} \to B^{\Gamma_n} \to (\text{Im}\, \varrho)_{\Gamma_n} \to \oplus_i R/(f_i, \omega_n) \to B_{\Gamma_n} \to 0,$$

$$(\text{Im}\, \varrho)^{\Gamma_n} \to A_{\Gamma_n} \to M_n \to (\text{Im}\, \varrho)_{\Gamma_n} \to 0.$$

The groups A_{Γ_n}, B_{Γ_n} and B^{Γ_n} stabilize for sufficiently large n. By the noetherian property, $(\oplus_i R/f_i)^{\Gamma_n}$ and $(\text{Im}\, \varrho)^{\Gamma_n}$ also stabilize. Hence for sufficiently large n, by Lemma 10.4, we have

$$\nabla(\oplus_i R/(f_i, \omega_n)) = \nabla((\text{Im}\, \varrho)_{\Gamma_n}) = \nabla M_n.$$

Then ii) follows from i) in this lemma. □

We consider a projective system $(\mathcal{X}(E/K_n)^\eta)_n$, which is the dual of the inductive system $(\text{Sel}(E/K_n)^\eta)_n$ by the restrictions. For sufficiently large n, the Mordell-Weil group over K_n stabilize (e.g. Corollary 10.2) and by (10.34) we have

$$\nabla \mathcal{X}(E/K_n)^\eta = \text{length}_{\mathbb{Z}_p} \left(Ш_n^\eta / Ш_{n-1}^\eta \right) + \text{rank}_{\mathbb{Z}_p} E(K_\infty)^\eta.$$

We let

$$\mathcal{Y}(E/K_n) = \text{Coker} \left(H^1(G_{n,S}, T) \to H^1(k_n, T)/E(k_n) \otimes \mathbb{Z}_p \right).$$

Then by (7.18), we have an exact sequence

$$0 \to \mathcal{Y}(E/K_n) \to \mathcal{X}(E/K_n) \to \mathcal{X}^0(E/K_n) \to 0. \tag{10.35}$$

Let us determine the numbers $\nabla \mathcal{Y}(E/K_n)^\eta$ and $\nabla \mathcal{X}^0(E/K_n)^\eta$.
We let

$$\mathcal{Y}'(E/K_n) = \text{Coker} \left(\mathbf{H}^1(T)_{\Gamma_n} \to H^1(k_n, T)/E(k_n) \otimes \mathbb{Z}_p \right),$$

$$\mathcal{Z}_n = \text{Im} \left(H^1(G_{n,S}, T) \to H^1(k_n, T)/E(k_n) \otimes \mathbb{Z}_p \right).$$

Then we have a commutative diagram

$$\begin{array}{ccccccc}
\mathbf{H}^1(T)_{\Gamma_n} & \longrightarrow & H^1(k_n, T)/E(k_n)\otimes\mathbb{Z}_p & \longrightarrow & \mathcal{Y}'(E/K_n) & \longrightarrow & 0 \\
\downarrow{\scriptstyle g_n} & & \| & & \downarrow & & \\
0 \longrightarrow \mathcal{Z}_n & \longrightarrow & H^1(k_n, T)/E(k_n)\otimes\mathbb{Z}_p & \longrightarrow & \mathcal{Y}(E/K_n) & \longrightarrow & 0.
\end{array} \tag{10.36}$$

We consider projective systems $(\mathcal{Y}(E/K_n)^\eta)_n$, $(\mathcal{Y}'(E/K_n)^\eta)_n$ and $(\mathrm{Coker}\, g_n)_n$ by the corestrictions.

Proposition 10.6. i) $\nabla\,(\mathrm{Coker}\, g_n)^\eta = 0$ *for* $n \gg 0$. *In particular,*

$$\nabla\,\mathcal{Y}(E/K_n)^\eta = \nabla\,\mathcal{Y}'(E/K_n)^\eta.$$

ii) *Let* f_0^η *be the characteristic polynomial of* $\mathcal{X}^0(E/K_\infty)^\eta$. *Then for sufficiently large* n, *we have*

$$\nabla\mathcal{X}^0(E/K_n)^\eta = \mathrm{ord}_{\zeta_{p^n-1}} f_0^\eta(\zeta_{p^n} - 1).$$

Proof. Let $\mathcal{Z}'_n = \mathrm{Im}\,(\,H^1(G_{n,S}, T) \to \oplus_v H^1(K_{n,v}, T)\,)$ where v ranges over all places over S. By the Tate-Poitou sequence, we have a commutative diagram

$$\begin{array}{ccccccccc}
\mathbf{H}^1(T) & \longrightarrow & \oplus_v \mathbf{H}^1_{\mathrm{Iw},v}(T) & \xrightarrow{f_\infty} & H^1(G_{\infty,S}, V/T)^\vee & \longrightarrow & \mathcal{X}^0(E/K_\infty) & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 \longrightarrow \mathcal{Z}'_n & \longrightarrow & \oplus_v H^1(K_{n,v}, T) & \xrightarrow{f_n} & H^1(G_{n,S}, V/T)^\vee & \longrightarrow & \mathcal{X}^0(E/K_n) & \longrightarrow & 0.
\end{array}$$

Here v ranges over the places over S. From the above, we have diagrams

$$\begin{array}{ccccccc}
\mathbf{H}^1(T)_{\Gamma_n} & \longrightarrow & \oplus_v \mathbf{H}^1_{\mathrm{Iw},v}(T)_{\Gamma_n} & \longrightarrow & (\mathrm{Im} f_\infty)_{\Gamma_n} & \longrightarrow & 0 \\
\downarrow{\scriptstyle g'_n} & & \downarrow{\scriptstyle h_n} & & \downarrow{\scriptstyle i_n} & & \\
0 \longrightarrow \mathcal{Z}'_n & \longrightarrow & \oplus_v H^1(K_{n,v}, T) & \longrightarrow & \mathrm{Im} f_n & \longrightarrow & 0,
\end{array}$$

$$\begin{array}{ccccccc}
(\mathrm{Im} f_\infty)_{\Gamma_n} & \longrightarrow & (H^1(G_{\infty,S}, V/T)^\vee)_{\Gamma_n} & \longrightarrow & \mathcal{X}^0(E/K_\infty)_{\Gamma_n} & \longrightarrow & 0 \\
\downarrow{\scriptstyle i_n} & & \downarrow{\scriptstyle j_n} & & \downarrow{\scriptstyle s_n} & & \\
0 \longrightarrow \mathrm{Im} f_n & \longrightarrow & H^1(G_{n,S}, V/T)^\vee & \longrightarrow & \mathcal{X}^0(E/K_n) & \longrightarrow & 0.
\end{array}$$

By Lemma (10.3), we also have an exact sequence

$$(H^1(G_{\infty,S}, V/T)^\vee)^{\Gamma_n} \xrightarrow{t_n} \mathcal{X}^0(E/K_\infty)^{\Gamma_n} \longrightarrow (\mathrm{Im} f_\infty)_{\Gamma_n} \longrightarrow (H^1(G_{\infty,S}, V/T)^\vee)_{\Gamma_n}.$$

We consider the dual of h_n and the inflation-restriction sequence. Then since Γ_n has cohomological dimension 1, the morphism h_n is injective. Similarly, since $E(K_\infty)_{p^\infty} = 0$ by Proposition 8.7, we see that j_n is bijective. Hence we have

$$0 \longrightarrow \mathrm{Coker}\, t_n \longrightarrow \mathrm{Coker}\, g'_n \longrightarrow \mathrm{Coker}\, h_n \longrightarrow \mathrm{Ker}\, s_n \longrightarrow 0.$$

We consider a commutative diagram

$$\begin{array}{ccc} \mathbf{H}^1(T)_{\Gamma_n} & \xrightarrow{1+\gamma_n+\cdots+\gamma_n^{p-1}} & \mathbf{H}^1(T)_{\Gamma_{n+1}} \\ \downarrow{\scriptstyle g'_n} & & \downarrow{\scriptstyle g'_{n+1}} \\ \mathcal{Z}'_n & \xrightarrow{\mathrm{Res}} & \mathcal{Z}'_{n+1}. \end{array}$$

Then the restriction induces a morphism $\mathrm{Coker}\, g'_n \to \mathrm{Coker}\, g'_{n+1}$. Similarly, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Coker}\, t_n & \longrightarrow & \mathrm{Coker}\, g'_n & \longrightarrow & \mathrm{Coker}\, h_n & \longrightarrow & \mathrm{Ker}\, s_n \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Coker}\, t_{n+1} & \longrightarrow & \mathrm{Coker}\, g'_{n+1} & \longrightarrow & \mathrm{Coker}\, h_{n+1} & \longrightarrow & \mathrm{Ker}\, s_{n+1} \longrightarrow 0, \end{array} \tag{10.37}$$

where the vertical maps are induced by restrictions.

We show that for sufficiently large n, all vertical maps in (10.37) are isomorphisms. Since diagram (10.37) consists of finitely generated $\mathbb{Z}_p$-modules, it suffices to show that the vertical maps on $\mathrm{Coker}\, t_n$ and $\mathrm{Coker}\, h_n$ are isomorphisms for $n \gg 0$. By the noetherian property, the groups $(H^1(G_{\infty,S}, V/T)^\vee)^{\Gamma_n}$ and $\mathcal{X}^0(E/K_\infty)^{\Gamma_n}$ stabilize. Therefore for large n the restriction map $\mathrm{Coker}\, t_n \to \mathrm{Coker}\, t_{n+1}$ is an isomorphism. The dual of $\mathrm{Coker}\, h_n$ is $\oplus_v (E(K_{\infty,v})_{p^\infty})_{\Gamma_n}$, which is finite of bounded order as n varies (cf. Greenberg [2], Lemma 3.3) and the projection $(\mathrm{Coker}\, h_{n+1})^\vee \to (\mathrm{Coker}\, h_n)^\vee$ is surjective. Hence for large n the restriction $\mathrm{Coker}\, h_n \to \mathrm{Coker}\, h_{n+1}$ is an isomorphism.

By definition, there is a canonical projection $\mathcal{Z}'_n \to \mathcal{Z}_n$. This induces a surjection $\mathrm{Coker}\, g'_n \to \mathrm{Coker}\, g_n$. Since $\mathrm{Coker}\, g'_n$ is a finitely generated $\mathbb{Z}_p$-module and stabilize for large n, $\mathrm{Coker}\, g_n$ also stabilize and the restriction $\mathrm{Coker}\, g_n \to \mathrm{Coker}\, g_{n+1}$ is an isomorphism for $n \gg 0$. We consider the composition $\mathrm{Cor} \circ \mathrm{Res} : \mathrm{Coker}\, g_{n-1} \cong \mathrm{Coker}\, g_n \to \mathrm{Coker}\, g_{n-1}$, which is the multiplication by p. Then by Lemma 10.4 ii), we have $\nabla(\mathrm{Coker}\, g_n)^\eta = 0$

and $\nabla\mathcal{Y}(E/K_n)^\eta = \nabla\mathcal{Y}'(E/K_n)^\eta$ by (10.36). We have already seen that $\mathrm{Ker}\, s_n$ is finite and stabilize for large n. In particular, $\nabla\mathrm{Ker}\, s_n = 0$. Hence by Lemma 10.5 ii), we have

$$\nabla\mathcal{X}^0(E/K_n)^\eta = \nabla\big(\mathcal{X}^0(E/K_\infty)^\eta{}_{\Gamma_n}\big) = \mathrm{ord}_{\zeta_{p^n}-1} f_0^\eta(\zeta_{p^n}-1). \qquad \square$$

Next we compute $\nabla\mathcal{Y}'(E/K_n)^\eta$. Let $\mathcal{Y}''(E/K_n)$ be the cokernel of

$$\mathbf{H}^1(T)_{\Gamma_n} \longrightarrow \frac{H^1(k_n,T)}{H^1_+(k_n,T)} \oplus \frac{H^1(k_n,T)}{H^1_-(k_n,T)} \tag{10.38}$$

where the map is the diagonal by localization.

By taking the Pontryagin dual of (8.22) after tensoring with $\otimes\mathbb{Q}_p/\mathbb{Z}_p$, we have an exact sequence

$$0 \to \frac{H^1(k_n,T)}{E(k_n)\otimes\mathbb{Z}_p} \to \frac{H^1(k_n,T)}{H^1_+(k_n,T)} \oplus \frac{H^1(k_n,T)}{H^1_-(k_n,T)} \to \frac{H^1(\mathbb{Q}_p,T)}{E(\mathbb{Q}_p)\otimes\mathbb{Z}_p} \to 0.$$

Thus we have

$$0 \to \mathcal{Y}'(E/K_n) \to \mathcal{Y}''(E/K_n) \to H^1(\mathbb{Q}_p,T)/E(\mathbb{Q}_p)\otimes\mathbb{Z}_p \to 0. \tag{10.39}$$

Since $H^1(\mathbb{Q}_p,T)/E(\mathbb{Q}_p)\otimes\mathbb{Z}_p \cong \mathbb{Z}_p$, we have

$$\nabla\mathcal{Y}'(E/K_n)^\eta = \begin{cases} \nabla\mathcal{Y}''(E/K_n)^\Delta - 1 & \text{if } \eta = 1, \\ \nabla\mathcal{Y}''(E/K_n)^\eta & \text{if } \eta \neq 1. \end{cases} \tag{10.40}$$

Using the even and the odd Coleman maps, we identify

$$H^1(k_n,T)/H^1_+(k_n,T) \cong \Lambda_n^+,$$

$$H^1(k_n,T)^\Delta/H^1_-(k_n,T)^\Delta \cong \Lambda_n^{-,\Delta}, \quad H^1(k_n,T)^\eta/H^1_-(k_n,T)^\eta \cong I_n^{-,\eta}.$$

The last identification is for a non-trivial η.

We consider commutative diagrams with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_p & \xrightarrow{G} & \Lambda_n^{+,\Delta} \oplus \Lambda_n^{-,\Delta} & \xrightarrow{F} & \Lambda_n^\Delta & \longrightarrow & \Lambda_n^\Delta/\big(\widetilde{\omega}_n^+, \widetilde{\omega}_n^-\big) \longrightarrow 0 \\ & & \| & & \downarrow \mathrm{proj} & & \downarrow \mathrm{proj} & & \downarrow \mathrm{proj} \\ 0 & \longrightarrow & \mathbb{Z}_p & \xrightarrow{G} & \Lambda_{n-1}^{+,\Delta} \oplus \Lambda_{n-1}^{-,\Delta} & \xrightarrow{F} & \Lambda_{n-1}^\Delta & \longrightarrow & \Lambda_{n-1}^\Delta/\big(\widetilde{\omega}_n^+, \widetilde{\omega}_n^-\big) \longrightarrow 0, \end{array} \tag{10.41}$$

and for $\eta \neq 1$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda_n^{+,\eta} \oplus I_n^{-,\eta} & \xrightarrow{F} & \Lambda_n^\eta & \longrightarrow & \Lambda_n^\eta/\big(\omega_n^+, \widetilde{\omega}_n^-\big) & \longrightarrow & 0 \\ & & \downarrow \mathrm{proj} & & \downarrow \mathrm{proj} & & \downarrow \mathrm{proj} & & \\ 0 & \longrightarrow & \Lambda_{n-1}^{+,\eta} \oplus I_{n-1}^{-,\eta} & \xrightarrow{F} & \Lambda_{n-1}^\eta & \longrightarrow & \Lambda_{n-1}^\eta/\big(\omega_n^+, \widetilde{\omega}_n^-\big) & \longrightarrow & 0. \end{array} \tag{10.42}$$

Here

$$F : (f, g) \mapsto \widetilde{\omega}_n^- f + \widetilde{\omega}_n^+ g, \quad G : a \mapsto \big(\widetilde{\omega}_n^+ a, -\widetilde{\omega}_n^- a\big).$$

Lemma 10.7. i) *The projections* $\Lambda_n/(\widetilde{\omega}_n^+, \widetilde{\omega}_n^-) \to \Lambda_{n-1}/(\widetilde{\omega}_n^+, \widetilde{\omega}_n^-)$ *and* $\Lambda_n/(\omega_n^+, \widetilde{\omega}_n^-) \to \Lambda_{n-1}/(\omega_n^+, \widetilde{\omega}_n^-)$ *are bijective.*

ii) *Let* $u_n : \mathbf{H}^1(T)^\Delta \to \Lambda_n^{+,\Delta} \oplus \Lambda_n^{-,\Delta}$ *be the morphism induced by (10.38). Then* $\operatorname{Im} u_n \cap \operatorname{Im} G = \operatorname{Im} u_{n-1} \cap \operatorname{Im} G = 0$.

Proof. i) follows from the fact that ω_{n-1} is a multiple of ω_n^+ or ω_n^-. Let $\boldsymbol{v} = (v_m)_m$ be an element $\mathbf{H}^1(T)^\Delta$ and let $u_{n-1}(\boldsymbol{v}) = (v^+, v^-) \in \Lambda_{n-1}^{+,\Delta} \oplus \Lambda_{n-1}^{-,\Delta}$. Then by the definition and the compatibility of the odd Coleman map, we have

$$v^- \equiv \varepsilon_\Delta \sum_{\sigma \in \mathcal{G}_0} \big(\mathrm{c}_{-1}^\sigma, v_0\big)_0 \equiv \varepsilon_\Delta\, (p-1) \times (\varepsilon, v_0)_0 \mod X.$$

Similarly, we have $v^+ \equiv 2\,\varepsilon_\Delta\, (\varepsilon, v_0)_0 \bmod X$. Hence $(p-1)\, v^+ \equiv 2\, v^-$. Suppose that $u_{n-1}(\boldsymbol{v}) \in \operatorname{Im} G$. We write $(v^+, v^-) = (\widetilde{\omega}_n^+ a, -\widetilde{\omega}_n^- a)$ for $a \in \mathbb{Z}_p$. Then $(p-1)v^+ \equiv 2\, v^- \bmod X$ if and only if $a = 0$. □

Let $\mathbf{e}$ be a basis of the free Λ-module $\mathbf{H}^1(T)$ of rank 1. We put $f_+^\eta := \varepsilon_\eta \mathrm{Col}^+(\mathbf{e})$, $f_-^\eta := \varepsilon_\eta \mathrm{Col}^-(\mathbf{e})$ and

$$M_n^\eta := \frac{\Lambda_n^\eta}{\big(\widetilde{\omega}_n^- f_+^\eta + \widetilde{\omega}_n^+ f_-^\eta\big)}, \quad M_{n-1}^\eta := \frac{\Lambda_{n-1}^\eta}{\big(\widetilde{\omega}_n^- f_+^\eta + \widetilde{\omega}_n^+ f_-^\eta\big)}.$$

(If η is trivial, we replace the superscript η by Δ.) Then by (10.41), (10.42) and Lemma 10.7, we have

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}_p & \longrightarrow & \mathcal{Y}''(E/K_n)^\Delta & \longrightarrow & M_n^\Delta & \longrightarrow & \Lambda_n^\Delta/\big(\widetilde{\omega}_n^+, \widetilde{\omega}_n^-\big) \longrightarrow 0 \\
 & & \| & & \downarrow & & \downarrow & & \| \\
0 & \longrightarrow & \mathbb{Z}_p & \longrightarrow & \mathcal{Y}''(E/K_{n-1})^\Delta & \longrightarrow & M_{n-1}^\Delta & \longrightarrow & \Lambda_{n-1}^\Delta/\big(\widetilde{\omega}_n^+, \widetilde{\omega}_n^-\big) \longrightarrow 0,
\end{array} \tag{10.43}$$

and for $\eta \neq 1$

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathcal{Y}''(E/K_n)^\eta & \longrightarrow & M_n^\eta & \longrightarrow & \Lambda_n^\eta/\big(\omega_n^+, \widetilde{\omega}_n^-\big) \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \| \\
0 & \longrightarrow & \mathcal{Y}''(E/K_{n-1})^\eta & \longrightarrow & M_{n-1}^\eta & \longrightarrow & \Lambda_{n-1}^\eta/\big(\omega_n^+, \widetilde{\omega}_n^-\big) \longrightarrow 0.
\end{array} \tag{10.44}$$

Hence together with (10.40), we have $\nabla \mathcal{Y}'(E/K_n)^\eta = \nabla M_n^\eta$ for every η.

Proposition 10.8. *For sufficiently large n, we have*

$$\nabla \mathcal{X}(E/K_n)^\eta = \begin{cases} \deg \widetilde{\omega}_n^- + \lambda_+^\eta + \phi(p^n)\mu_+^\eta & \text{if } n \text{ is even,} \\ \deg \widetilde{\omega}_n^+ + \lambda_-^\eta + \phi(p^n)\mu_-^\eta + \xi^\eta & \text{if } n \text{ is odd} \end{cases}$$

where $\xi^\eta = 1$ if $\eta \neq 1$, otherwise, $\xi^\eta = 0$.

Proof. By Lemma 10.5 i), we have

$$\nabla M_n^\eta = \deg \widetilde{\omega}_n^{\mp} + \operatorname{ord}_{\zeta_{p^n}-1} f_\pm^\eta(\zeta_{p^n} - 1).$$

Here the signs are taken according to the parity of n. On the other hand, we have $\operatorname{Char}(\mathcal{X}^-(E/K_\infty)^\eta) = (f_0^\eta(X)\, f_-^\eta(X)/X)$ if $\eta \neq 1$, otherwise, $\operatorname{Char}(\mathcal{X}^\pm(E/K_\infty)^\eta) = (f_0^\eta(X)\, f_\pm^\eta(X))$. Hence the proposition follows from (10.35), Proposition 10.6 and $\nabla \mathcal{Y}'(E/K_n)^\eta \cong \nabla M_n^\eta$. □

By summing up the formula

$$\nabla \mathcal{X}(E/K_m)^\eta = \operatorname{length}_{\mathbb{Z}_p}\left(Ш_m^\eta / Ш_{m-1}^\eta\right) + \operatorname{rank} E(K_\infty)^\eta$$

for m $(0 \leq m \leq n)$, we have the following.

Theorem 10.9. *Assume that $Ш(E/K_n)$ are finite for all n. Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character and let*

$$e_n^\eta = \operatorname{ord}_p(\sharp Ш(E/K_n)^\eta).$$

Then, for sufficiently large n, we have

$$e_n = \sum_{m=0}^{[\frac{n-2}{2}]} p^{n-1-2m} - \left[\frac{n}{2}\right] + \left[\frac{n}{2}\right]\lambda_+^\eta + \left[\frac{n+1}{2}\right]\left(\lambda_-^\eta + \xi^\eta\right) - n\, r_\infty^\eta + \sum_{m=1}^{[\frac{n}{2}]} \phi\left(p^{2m}\right)\mu_+^\eta + \sum_{m=1}^{[\frac{n+1}{2}]} \phi\left(p^{2m-1}\right)\mu_-^\eta + \nu^\eta$$

where ν^η is an integer independent of n, $r_\infty^\eta = \operatorname{rank} E(K_\infty)^\eta$, and $\xi^\eta = 1$ if $\eta \neq 1$, otherwise, $\xi^\eta = 0$.

By comparing with Greenberg's conjecture in the good ordinary case and by numerical data, Pollack conjectured that his analytic μ-invariants are always equal to zero. By the even (odd) main conjecture, our μ_+^η and μ_-^η would be also equal to zero.

Corollary 10.10. *Assume that $\mu_+^\eta = \mu_-^\eta = 0$. Then for sufficiently large n, we have*

$$e_n^\eta = \begin{cases} \left[\lambda^\eta n + \mu p^n + \nu_+^\eta\right] & \text{if } n \text{ is even,} \\ \left[\lambda^\eta n + \mu p^n + \nu_-^\eta\right] & \text{if } n \text{ is odd} \end{cases}$$

where $\lambda^\eta = \frac{\lambda_+^\eta + \lambda_-^\eta + \xi^\eta - 1}{2} - r_\infty^\eta$, $\mu = \frac{p}{p^2-1}$ *and* ν_+^η, ν_-^η *are some rational constants.*

The above formula was conjectured by Kurihara in [10].

References

1. Amice, Y., Vélu, J.: Distributions p-adiques associées aux séries de Hecke. Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974), pp. 119–131. Asterisque, Nos. 24–25, Soc. Math. France, Paris 1975
2. Greenberg, R.: Iwasawa theory for elliptic curves. Arithmetic theory of elliptic curves. (Cetraro, 1997), 51–144, Lect. Notes Math. **1716**, Springer, Berlin 1999
3. Greenberg, R., Vatsal, V.: On the Iwasawa invariants of elliptic curves. Invent. Math. **142**, 17–63 (2000)
4. Honda, T.: Formal groups and zeta-functions. Osaka J. Math. **5**, 199–213 (1968)
5. Honda, T.: On the theory of commutative formal groups. J. Math. Soc. Japan **22**, 213–246 (1970)
6. Kato, K.: 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 Lect. Notes Math. **1553**, 1993
7. Kato, K.: P-adic Hodge theory and values of zeta funcions of modular forms. Preprint series, Graduate School of Mathematical Sciences, The University of Tokyo
8. Knospe, H.: Iwasawa-theory of abelian varieties at primes of non-ordinary reduction. Manuscr. Math. **87**, 225–258 (1995)
9. Kurihara, M.: On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I. Invent. math. **149**, 195-224 (2002)
10. Kurihara, M.: The Iwasawa theory of elliptic curves that have supersingular reduction. Algebraic number theory and related topics (Kyoto, 2000). Surikaisekikenkyusho Kokyuroku **1154**, 33–43 (2000)
11. Mazur, B.: Rational points of abelian varieties with values in towers of number fields. Invent. Math. **18**, 183–266 (1972)
12. Mazur, B., Tate, J., Teitelbaum, J.: On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. Invent. Math. **84**, 1–48 (1986)
13. Perrin-Riou, B.: Théorie d'Iwasawa p-adique locale et globale. Invent. Math. **99**, 247–292 (1990)
14. Perrin-Riou, B.: Fonctions L p-adiques d'une courbe elliptique et points rationnels. Ann. Inst. Fourier **43**, 945–995 (1993)
15. Perrin-Riou, B.: Théorie d'Iwasawa des représentations p-adiques sur un corps local. Invent. Math. **115**, 81–161 (1994)
16. Perrin-Riou, B.: Fonctions L p-adiques des représentations p-adiques, Astérisque **229** (1995), 198 pp.
17. Perrin-Riou, B.: Arithmétique des courbes elliptiques à réduction supersingulière en p. Preprint
18. Pollack, R.: On the p-adic L-function of a modular form at a supersingular prime. Preprint
19. Pollack, R., Rubin, K.: The main conjecture for CM elliptic curves at supersingular primes. Preprint
20. Rohrlich, D.: On L-functions of elliptic curves and cyclotomic towers. Invent. Math. **75**, 409–423 (1984)
21. Rubin, K.: Euler systems and modular elliptic curves. Galois representations in arithmetic algebraic geometry (Durham, 1996), 351–367. London Math. Soc. Lect. Note Ser. 254, Cambridge Univ. Press, Cambridge 1998
22. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**, 259–331 (1972)
23. Višik, M.: Nonarchimedean measures associated with Dirichlet series. Mat. Sb. **99**(141), 248–260, 296 (1976)