Canad. J. Math. Vol. **66** (4), 2014 pp. 826–843
http://dx.doi.org/10.4153/CJM-2013-043-2

Signed-Selmer Groups over the $\mathbb{Z}_p^2$-extension of an Imaginary Quadratic Field

Byoung Du (B. D.) Kim

Abstract. Let E be an elliptic curve over $\mathbb{Q}$ that has good supersingular reduction at $p > 3$. We construct what we call the $\pm/\pm$-Selmer groups of E over the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field K when the prime p splits completely over $K/\mathbb{Q}$, and prove that they enjoy a property analogous to Mazur's control theorem.

Furthermore, we propose a conjectural connection between the $\pm/\pm$-Selmer groups and Loeffler's two-variable $\pm/\pm$-p-adic L-functions of elliptic curves.

1 Introduction

This paper is the algebraic counterpart to the author's previous paper [4]. In this paper, we construct certain Selmer groups $\mathrm{sel}_p^{\pm/\pm}(E/K_\infty)$ (which we call the $\pm/\pm$-Selmer groups) of an elliptic curve E/K where K is an imaginary quadratic field, and K_∞ is its $\mathbb{Z}_p^2$-extension, and then study their control theorem (and by so doing, we argue that these Selmer groups are useful). In addition, we make a conjecture analogous to the classical main conjecture of Iwasawa Theory that connects our $\pm/\pm$-Selmer groups to Loeffler's two-variable $\pm/\pm -p$-adic L-functions [10].

Readers acquainted with the plus/minus Iwasawa theory will recognize that we try to generalize the $\pm$-Selmer groups of S. Kobayashi [5]. However, in this paper we are working with the $\mathbb{Z}_p^2$-extensions of imaginary quadratic fields rather than with $\mathbb{Z}_p$-extensions, which results in many differences.

To understand the context of this work, it is helpful to understand not only Kobayashi and Pollack's work that initiated the current plus/minus Iwasawa Theory [5,14], but also more recent developments in this area by A. Lei, D. Loeffler, F. Sprung, S. Zerbes, *et. al.* [7–9, 16], though this is hardly an exhaustive list). Also see Kurihara, Rubin, and Perrin-Riou's papers on the topic that predate the current theory [6, 13, 15].

First, we introduce our $\pm/\pm$-Selmer groups.

Let $\mathfrak{f}$ be an integral ideal of K prime to p. One crucial assumption of this paper is that $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Also, we assume that E is defined over K, and

$$a_{\mathfrak{p}}(E) = 1 + N_{K/\mathbb{Q}}\mathfrak{p} - \#E(\mathcal{O}_K/\mathfrak{p}) = a_{\overline{\mathfrak{p}}}(E) = 0.$$

Received by the editors October 30, 2012; revised August 13, 2013.
Published electronically November 14, 2013.
AMS subject classification: **11Gxx**.
Keywords: elliptic curves, Iwasawa theory.

(This last assumption is automatically true if E is defined over $\mathbb{Q}$, E has good supersingular reduction at p, and $p > 3$.) Then $\mathfrak{p}$ is unramified over $K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty})/K$ and totally ramified over $K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})/K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty})$, so we can apply the plus/minus technique to $K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})_{\mathfrak{q}}/K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty})_{\mathfrak{q}}$, where $\mathfrak{q}$ is any prime above $\mathfrak{p}$. This is a natural extension of [3, Section 3.2], which is itself a natural extension of [2]. We can apply the same idea to $K(\mathfrak{f}\mathfrak{p}^{\infty}\overline{\mathfrak{p}}^{\infty})_{\bar{\mathfrak{q}}}/K(\mathfrak{f}\mathfrak{p}^{\infty})_{\bar{\mathfrak{q}}}$, and combining these two, we obtain $\pm/\pm$-local conditions that define $\mathrm{sel}_p^{\pm/\pm}(E/K_{\infty})$. (See Section 2.3.)

Second, we prove a theorem analogous to Mazur's Control Theorem [12] for the Δ_1-parts of these Selmer groups where $\Delta_1 = \mathrm{Gal}(K(\mathfrak{f}p)/K(\mathfrak{f}))$.

Theorem 1.1 (Proposition 2.19) *We assume $p > 2$. We also assume that $4 \nmid [K(\mathfrak{f})_{\mathfrak{P}} : \mathbb{Q}_p]$ for every prime $\mathfrak{P}$ above p except in the case of the $\mathrm{sel}_p^{-/-}$ group. For $m, n \geq 0$, the natural homomorphism*

$$\mathrm{sel}_p^{\pm/\pm}\big(E/K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})\big)^{\Delta_1} \longrightarrow \mathrm{sel}_p^{\pm/\pm}\big(E/K(\mathfrak{f}\mathfrak{p}^{\infty}\overline{\mathfrak{p}}^{\infty})\big)^{\Delta_1}\big[\omega_n^{\pm}(S)\big]\big[\omega_m^{\pm}(T)\big]$$

has bounded kernel and cokernel as n and m vary.

Initially, we erroneously thought we could prove this only for the $\mathrm{sel}_p^{-/-}$ groups, but the referee pointed out that a more general claim can be proven. We owe Theorem 2.8 to the referee.

Remark 1.2 Proving a more general statement

$$\mathrm{sel}_p^{\pm/\pm}(E/K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})) \to \mathrm{sel}_p^{\pm/\pm}(E/K(\mathfrak{f}\mathfrak{p}^{\infty}\overline{\mathfrak{p}}^{\infty}))[\omega_n^{\pm}(S)][\omega_m^{\pm}(T)]$$

was initially our goal, which we hope to achieve some day.

In Iwasawa Theory, we usually believe that there is an analytic theory that matches every algebraic theory. Such a theory in our case must be a theory of four integral two-variable power series $L_p^{\pm,\pm}(X, Y)$ so that

$$L_p^{\pm,\pm}(\zeta_{p^n} - 1, \zeta_{p^m} - 1) = \frac{L(\pi_E, \omega, 1)}{*}$$

(where n and m are even or odd depending on the signs $\{\pm,\pm\}$ and ω is a finite character of K determined by ζ_{p^n}, ζ_{p^m}), where $L(\pi_E, \omega, s)$ is an L-function (in a certain way) attached E/K twisted by ω, and $*$ is some term that possibly contains periods, the Gauss sums, π, i, etc. The existence of such p-adic L-functions was already predicted by D. Loeffler and S. Zerbes [11].

The answer can be found in Loeffler's remarkable recent work [10] in which he constructed such p-adic L-functions based on a clever application of S. Haran's generalized Mazur-Tate elements for GL_2 [1]. We include a brief sketch of Loeffler's work in Section 3, but an interested reader should read the full account described in [10].

Finally, we conjecture the following.

Conjecture 1.3 (See Conjecture 3.1)

$$(L_p^{\pm,\pm}) = \mathrm{char}(X^{\pm/\pm}) \subset \mathbb{Z}_p[[\mathrm{Gal}(K(\mathfrak{f}p^{\infty})/K)]]$$

where $X^{\pm/\pm}$ is the Pontryagin dual $\mathrm{Hom}(\mathrm{sel}_p^{\pm/\pm}(E/K(\mathfrak{f}p^{\infty})), \mathbb{Q}_p/\mathbb{Z}_p)$.

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

2 $\pm/\pm$-Selmer Groups

In this section, we construct the $\pm/\pm$-Selmer groups, and prove a control theorem for them.

2.1 Plus/minus Norms Group Decomposition

In this section, we slightly generalize Kobayashi's construction [5] of what we call the plus/minus norm points. The construction presented in this paper is the same as the one given in [3], but, the situation of this paper is yet different from [3], because we only deal with the cyclotomic extension of an arbitrary unramified field k for a reason that will become clear in Section 2.3. Because of this particular situation, we do need all the ideas for the construction of [3], yet the presentation is more elegant and illustrative because of the properties of the cyclotomic fields.

Many results in [3, Section 3.1] were proved only for the minus groups. In this paper, we will deal with both the plus groups and the minus groups. In the case of the plus groups, we may assume some mild conditions.

In this section, we assume the following:

(a) the elliptic curve $E/\mathbb{Q}_p$ has good reduction;
(b) if $\tilde{E}$ is the reduced curve of E over $\mathbb{Z}/p\mathbb{Z}$, then $a_p = 1 + p - |\tilde{E}(\mathbb{Z}/p\mathbb{Z})|$ is 0.

Let k be a finite unramified extension of $\mathbb{Q}_p$ of degree d and let $\mathcal{O}_k$ be its ring of integers.

For a fuller explanation of the following construction, see [3, Section 3.2]. We will explain this briefly, and only point out the differences that matter to us. For a local field k', we let $\widehat{E}(k')$ denote $\widehat{E}(\mathfrak{m}_{k'})$ for convenience.

Definition 2.1 (Kobayashi) For $n \geq -1$, we define

$$\widehat{E}^{+}\big(k(\mu_{p^{n+1}})\big) = \Big\{ x \in \widehat{E}\big(k(\mu_{p^{n+1}})\big) \;\Big|\; \mathrm{Tr}_{k(\mu_{p^{n+1}})/k(\mu_{p^{l+2}})}(x) \in \widehat{E}\big(k(\mu_{p^{l+1}})\big) \text{ for } 0 \leq l < n, 2 \mid l \Big\},$$

$$\widehat{E}^{-}\big(k(\mu_{p^{n+1}})\big) = \Big\{ x \in \widehat{E}\big(k(\mu_{p^{n+1}})\big) \;\Big|\; \mathrm{Tr}_{k(\mu_{p^{n+1}})/k(\mu_{p^{l+2}})}(x) \in \widehat{E}\big(k(\mu_{p^{l+1}})\big) \text{ for } -1 \leq l < n, 2 \nmid l \Big\}.$$

Remark 2.2 We can plausibly argue that it is more natural to define $\widehat{E}^{\pm}$ inductively as follows:

First we let $\widehat{E}^{+}(k(\mu_{p^0})) = \widehat{E}(k)$. Then for every even number $n \geq 0$, we let $\widehat{E}^{+}(k(\mu_{p^{n+1}}))$ be the set of points $x \in \widehat{E}(k(\mu_{p^{n+1}}))$ such that $\mathrm{Tr}_{k(\mu_{p^{n+1}})/k(\mu_{p^n})}(x) \in \widehat{E}^{+}(k(\mu_{p^n}))$, and for every odd number $n \geq -1$, we let

$$\widehat{E}^{+}\big(k(\mu_{p^{n+1}})\big) \stackrel{\text{def}}{=} \widehat{E}^{+}\big(k(\mu_{p^n})\big)$$

inductively.

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

(For $\widehat{E}^-$, switch the roles of odd and even.)

Notation 2.3 Let $\Phi_n(X)$ be the minimal polynomial ("the cyclotomic polynomial") of the p^n-th primitive root of unity ζ_{p^n} for every integer $n \geq 0$. (Then, of course, $\Phi_n(X+1)$ is the minimal polynomial of $\zeta_{p^n} - 1$.) And, for every $n \geq 0$, we define

$$\omega_n(X) = (X+1)^{p^n} - 1,$$
$$\omega_n^+(X) = \prod_{\substack{0 \leq m \leq n, \\ m \text{ even}}} \Phi_m(X+1),$$
$$\omega_n^-(X) = \Phi_0(X+1) \prod_{\substack{0 \leq m \leq n, \\ m \text{ odd}}} \Phi_m(X+1).$$

Remark 2.4 By examining Definition 2.1, we can easily see that

$$\operatorname{rank}_{\mathbb{Z}_p} \widehat{E}^-(k(\mu_{p^{n+1}}))^\eta = \begin{cases} d \cdot (\deg(\omega_n^-) - 1) & \text{if } \eta \neq 1 \text{ and } n \text{ is odd,} \\ d \cdot (\deg(\omega_{n-1}^-) - 1) & \text{if } \eta \neq 1 \text{ and } n \text{ is even,} \\ d \cdot \deg(\omega_n^-) & \text{if } n \text{ is odd,} \\ d \cdot \deg(\omega_{n-1}^-) & \text{if } n \text{ is even,} \end{cases}$$

$$\operatorname{rank}_{\mathbb{Z}_p} \widehat{E}^+(k(\mu_{p^{n+1}}))^\eta = \begin{cases} d \cdot \deg(\omega_n^+) & \text{if } n \text{ is even,} \\ d \cdot \deg(\omega_{n-1}^+) & \text{if } n \text{ is odd.} \end{cases}$$

Now we construct points $c_{n+1} \in E(k(\mu_{p^{n+1}}))$ satisfying

$$\operatorname{Tr}_{k(\mu_{p^{n+1}})/k(\mu_{p^n})} c_{n+1} = -c_{n-1}.$$

It is not hard to see that $c_{n+1} \in E^+(k(\mu_{p^{n+1}}))$ if n is even, and $c_{n+1} \in E^-(k(\mu_{p^{n+1}}))$ if n is odd.

Let φ denote the p-th Frobenius map of k, and for a unit $z \in \mathcal{O}_k^\times$, we let

$$f_z(X) = (X+z)^p - z^p, \qquad \log_{f_z}(X) = \sum_{n=0}^{\infty} (-1)^n \frac{f_z^{(2n)}(X)}{p^n},$$

where $f^{(n)}(X)$ denote $f^{\varphi^{n-1}} \circ f^{\varphi^{n-2}} \circ \cdots \circ f(X)$. Fix a logarithm $\log_{\widehat{E}}$ of the formal group $\widehat{E}$ associated with the minimal model of E over $\mathbb{Z}_p$ and a primitive p^n-th root of unity ζ_{p^n} for each $n \geq 0$. (We may assume $\zeta_{p^n}^p = \zeta_{p^{n-1}}$ for each $n > 0$.) As in [3, Section 3.2], we can construct a point $c_{n,z}$ such that

$$\log_{\widehat{E}}(c_{n,z}) = \left[\sum_{i=1}^{\infty} (-1)^{i-1} z^{\varphi^{-(n+2i)}} \cdot p^i \right] + \log_{f_z^{\varphi^{-n}}} \left(z^{\varphi^{-n}} \cdot (\zeta_{p^n} - 1) \right). \tag{2.1}$$

Because $\log_{\widehat{E}}$ is injective on $\widehat{E}(k(\mu_{p^{n+1}}))$ (which follows from [3, Proposition 3.1], a slight but necessary generalization of [5, Proposition 8.7]), from (2.1) we can see that $\operatorname{Tr}_{k(\mu_{p^{n+1}})/k(\mu_{p^n})} c_{n+1} = -c_{n-1}$ for every $n > 0$.

Fix $\zeta \in \mathcal{O}_k^\times$ such that $\{1, \zeta, \ldots, \zeta^{d-1}\}$ linearly generates $\mathcal{O}_k/p\mathcal{O}_k$ over $\mathbb{Z}/p\mathbb{Z}$. With the points $\{c_{n,1}, c_{n,\zeta}, \ldots, c_{n,\zeta^{d-1}}\}$, we study the following.

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

Notation 2.5 For an even number $n \geq 0$, let C_{n+1}^{+} be the subgroup of $\widehat{E}^{+}(k(\mu_{p^{n+1}}))$ generated by $\{c_{n+1,\zeta^i}\}_{i=0,\dots,d-1}$ over $\mathbb{Z}_p[\mathrm{Gal}(k(\mu_{p^{n+1}})/k)]$, and for an odd number $n > 0$, let $C_{n+1}^{+} = C_n^{+}$.

On the other hand, for an odd number $n \geq -1$, let C_{n+1}^{-} be the subgroup of $\widehat{E}^{-}(k(\mu_{p^{n+1}}))$ generated by $\{c_{n+1,\zeta^i}\}_{i=0,\dots,d-1}$ over $\mathbb{Z}_p[\mathrm{Gal}(k(\mu_{p^{n+1}})/k)]$, and for an even number $n \geq 0$, let $C_{n+1}^{-} = C_n^{-}$.

Proposition 2.6 *For every $n \geq -1$, we have*

$$\widehat{E}\big(k(\mu_{p^{n+1}})\big) = \widehat{E}^{+}\big(k(\mu_{p^{n+1}})\big) + \widehat{E}^{-}\big(k(\mu_{p^{n+1}})\big).$$

In fact, we can prove a slightly stronger claim that $C_{n+1}^{+} + C_{n+1}^{-} = \widehat{E}(k(\mu_{p^{n+1}}))$.

Proof We only need to generalize [5, Proposition 8.11] slightly.

First, the same argument used in [5, Proposition 8.11] shows that for any $n \geq 0$, $\log_{\widehat{E}}(x) \in \mathfrak{m}_{k(\mu_{p^n})} + k(\mu_{p^{n-1}})$ for $x \in \widehat{E}(\mathfrak{m}_{k(\mu_{p^n})})$. This gives us the following injection

$$\log_{\widehat{E}}\big(\widehat{E}(k(\mu_{p^n}))\big) / \log_{\widehat{E}}\big(\widehat{E}(k(\mu_{p^{n-1}}))\big) \longrightarrow \big(\mathfrak{m}_{k(\mu_{p^n})} + k(\mu_{p^{n-1}})\big)/k(\mu_{p^{n-1}}) \cong \mathfrak{m}_{k(\mu_{p^n})}/\mathfrak{m}_{k(\mu_{p^{n-1}})}.$$

From (2.1), it is not difficult to see that

$$\log_{\widehat{E}}(c_{n,\zeta^i}) \equiv (\zeta^i)^{\varphi^{-n}} \cdot (\zeta_{p^n} - 1) \pmod{k(\mu_{p^{n-1}})}.$$

We will prove that $\{\zeta^i \cdot (\zeta_{p^n} - 1)\}_{i=0,1,\dots,d-1}$ generates $\mathfrak{m}_{k(\mu_{p^n})}/\mathfrak{m}_{k(\mu_{p^{n-1}})}$ over $\mathbb{Z}_p[\mathrm{Gal}(k(\mu_{p^n})/k)]$.

It is clear that $\mathfrak{m}_{k(\mu_{p^n})}$ is generated (over $\mathbb{Z}_p$) by $\zeta^i(\zeta_{p^n} - 1)^j$ for $i = 0, \dots, d-1$ and $j = 1, 2, \dots$. Now, we observe that $(\zeta_{p^n} - 1)^j$ can be written as a combination of $(\zeta_{p^n} - 1), (\zeta_{p^n}^2 - 1), \dots, (\zeta_{p^n}^j - 1)$, so we can see that $\zeta^i \cdot (\zeta_{p^n} - 1)^j$ can be written as a linear combination of $\zeta^i \cdot (\zeta_{p^n} - 1), \zeta^i \cdot (\zeta_{p^n}^2 - 1), \dots, \zeta^i \cdot (\zeta_{p^n}^j - 1)$. On the other hand, if $p \mid l$, we have $\zeta_{p^n}^l - 1 \in \mathfrak{m}_{k(\mu_{p^{n-1}})}$. Since $\zeta_{p^n}^l - 1$ for any other l is the image of $\zeta_{p^n} - 1$ under some element of $\mathrm{Gal}(k(\mu_{p^n})/k)$, our claim follows.

Thus, $\{\log_{\widehat{E}}(c_{n,\zeta^i})\}_{i=0,\dots,d-1}$ generates $\log_{\widehat{E}}(\widehat{E}(k(\mu_{p^n})))/\log_{\widehat{E}}(\widehat{E}(k(\mu_{p^{n-1}})))$ over $\mathbb{Z}_p[\mathrm{Gal}(k(\mu_{p^n})/k)]$ for every $n \geq 0$, which in turn implies that $\{c_{n,\zeta^i}\}_{i=0,\dots,d-1}$ generates $\widehat{E}(k(\mu_{p^n}))/\widehat{E}(k(\mu_{p^{n-1}}))$ over $\mathbb{Z}_p[\mathrm{Gal}(k(\mu_{p^n})/k)]$ because, as mentioned before, $\log_{\widehat{E}}$ is injective on $\widehat{E}(k(\mu_{p^n}))$.

The rest of the proof is a simple induction argument. Our argument also shows that $C_{n+1}^{+} + C_{n+1}^{-} = \widehat{E}(k(\mu_{p^{n+1}}))$. ∎

Next, we prove

$$\big(\widehat{E}^{\pm}\big(k(\mu_{p^\infty})\big)^{\Delta} \otimes \mathbb{Q}_p/\mathbb{Z}_p\big)^{\vee} \overset{\mathrm{def}}{=} \mathrm{Hom}\big(\widehat{E}^{\pm}(k(\mu_{p^\infty}))^{\Delta} \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p\big) \cong \Lambda_{\mathrm{cyc}}^{d},$$

where

$$\Lambda_{\mathrm{cyc}} = \mathbb{Z}_p[[\mathrm{Gal}(k(\mu_{p^\infty})/k(\mu_p))]] (\cong \mathbb{Z}_p[[X]]), \quad \Delta = \mathrm{Gal}(k(\mu_p)/k)$$

(there will be additional conditions in the case of the plus group).

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

Theorem 2.7 *Recall that $d = [k:\mathbb{Q}_p]$. We have*

$$\left(\widehat{E}^{-}(k(\mu_{p^\infty}))^{\Delta} \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{\vee} \cong \Lambda_{\mathrm{cyc}}^{d}.$$

Proof As in [5] (see also [3, Proposition 3.13] that explains the reason for the switch from Λ_{cyc} to $\Lambda_{\mathrm{cyc}}^{d}$), we construct

$$\mathrm{Col}_n^{\pm}\colon H^1\left(k(\mu_{p^{n+1}}), T_E\right)^{\Delta}/H_{\pm}^1(k(\mu_{p^{n+1}}), T_E)^{\Delta} \longrightarrow (\Lambda_n^{\pm})^d,$$

where $H_{\pm}^1(k(\mu_{p^{n+1}}), T_E)^{\Delta}$ is the exact annihilator of $(C_{n+1}^{\pm})^{\Delta}$ with respect to the local Tate pairing, and $\Lambda_n^{\pm}$ is $\Lambda_{\mathrm{cyc}}/(\omega_n^{\pm})$. These maps are constructed in such a way that the following diagram is commutative for any $m \geq n$:

$$\begin{array}{ccc} H^1(k(\mu_{p^{m+1}}), T_E)^{\Delta} & \longrightarrow & (\Lambda_m^{\pm})^d \\ \downarrow & & \downarrow \\ H^1(k(\mu_{p^{n+1}}), T_E)^{\Delta} & \longrightarrow & (\Lambda_n^{\pm})^d \end{array}$$

Thus, by taking them to the inverse limit, we obtain

$$\mathrm{Col}^{\pm}\colon H^1\left(k(\mu_{p^\infty}), T_E\right)^{\Delta} \to \Lambda_{\mathrm{cyc}}^{d}.$$

Thus, to prove that $\mathrm{Col}^{\pm}$ is surjective, we only need to show $\mathrm{Col}_0^{\pm}$ is surjective. (Once we prove that, the rest follows immediately by Nakayama's Lemma.) We can see that $\mathrm{Col}_0^{\pm}$ is given by

$$\mathrm{Col}_0^{\pm}\colon H^1(k(\mu_p), T_E)^{\Delta} \to \mathrm{Hom}\left((C_1^{\pm})^{\Delta}, \mathbb{Z}_p\right) \to \mathbb{Z}_p^d.$$

This is surjective if $(C_1^{\pm})^{\Delta} = \widehat{E}(k(\mu_p))^{\Delta} = \widehat{E}(k)$.

We prove this statement for the minus group for now and the statement for the plus group in Theorem 2.8.

It is not hard to see that $C_1^{-} = C_0^{-}$. Note that C_0^{-} is generated by $\{c_{0,\zeta^i}\}_{i=0,\ldots,d-1}$, which satisfies

$$\log_{\widehat{E}}(c_{0,\zeta^i}) = \sum_{j=1}^{\infty}(-1)^{j-1}(\zeta^i)^{\varphi^{-(n+2j)}} \cdot p^j \equiv (\zeta^i)^{\varphi^{-2}} \cdot p \pmod{p^2}.$$

Thus, clearly $\{\log_{\widehat{E}}(c_{0,\zeta^i})\}_{i=0,\ldots,d-1}$ generates $p\mathcal{O}_k$. Since $\log_{\widehat{E}}\colon \widehat{E}(k) \to p\mathcal{O}_k$ is an isomorphism, we can see that $\{c_{0,\zeta^i}\}_{i=0,\ldots,d-1}$ generates $\widehat{E}(k)$. ∎

The referee suggested the following proof, for which the author is truly grateful.

Theorem 2.8 *If $p > 2$ and $4 \nmid d$, then we also have*

$$\left(\widehat{E}^{+}(k(\mu_{p^\infty}))^{\Delta} \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{\vee} \cong \Lambda_{\mathrm{cyc}}^{d}.$$

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

Proof As we saw in the proof of Theorem 2.7, we need to show

$$(C_1^+)^{\Delta} = \widehat{E}(k(\mu_p))^{\Delta} = \widehat{E}(k).$$

Similar to the same theorem, it is sufficient to show that the images of

$$\left\{ \log_{\widehat{E}}(c_{1,\zeta^i}) = \left(\sum_{j=1}^{\infty} (-1)^{j-1} (\zeta^i)^{\varphi^{-1-2j}} \cdot p^j \right) + (\zeta^i)^{\varphi^{-1}} \cdot (\zeta_p - 1) \right\}_{i=0,\dots,d-1}$$

under the trace $\mathrm{Tr}_{k(\mu_p)/k}$ generate $p \cdot \mathcal{O}_k$ (we use $\mathrm{Tr}_{k(\mu_p)/k}$ because its image is always invariant under the action of Δ). The trace of the term above can be explicitly computed:

$$\begin{aligned} \mathrm{Tr}_{k(\mu_p)/k}(\log_{\widehat{E}}(c_{1,\zeta^i})) &\equiv \mathrm{Tr}_{k(\mu_p)/k}\left((\zeta^i)^{\varphi^{-3}} \cdot p + (\zeta^i)^{\varphi^{-1}} \cdot (\zeta_p - 1) \right) \pmod{p^2} \\ &= (\zeta^i)^{\varphi^{-3}} \cdot (p-1)p - (\zeta^i)^{\varphi^{-1}} \cdot p \\ &\equiv -\left((\zeta^i)^{\varphi^{-3}} + (\zeta^i)^{\varphi^{-1}} \right) p \pmod{p^2}. \end{aligned}$$

Now the question comes down to showing that $\{(\zeta^i)^{\varphi^{-3}} + (\zeta^i)^{\varphi^{-1}}\}_{i=0,\dots,d-1}$ generates $\mathcal{O}_k/p\mathcal{O}_k$. Equivalently, we may ask whether $\{(\zeta^i)^{\varphi^{-2}} + (\zeta^i)\}_{i=0,\dots,d-1}$ generates $\mathcal{O}_k/p\mathcal{O}_k$ linearly, and since $\{1, \zeta, \dots, \zeta^{d-1}\}$ generates $\mathcal{O}_k/p\mathcal{O}_k$ by our assumption, this question is equivalent to whether $\varphi^{-2} + 1$ is surjective on $\mathcal{O}_k/p\mathcal{O}_k$. In turn, since $\mathcal{O}_k/p\mathcal{O}_k$ is a finite field, $\varphi^{-2} + 1$ is surjective if and only if it is injective on $\mathcal{O}_k/p\mathcal{O}_k$.

To find the kernel of $\varphi^{-2} + 1$, first we note that it is contained in the kernel of $\varphi^4 - 1$, which is $\mathbb{F}_{p^4}$. We also note that the kernel of $\varphi^{-2} + 1$ does not contain any element of $\mathbb{F}_{p^2}$ except 0 unless $p = 2$.

If $4 \nmid d$, then $\mathcal{O}_k/p\mathcal{O}_k \cap \mathbb{F}_{p^4}$ is $\mathbb{F}_{p^2}$ or $\mathbb{F}_p$. In either case, the kernel of $\varphi^{-2} + 1$ only contains 0. ∎

The next statement repeats [3, Proposition 3.15]. Even though we do not add anything substantial to it, we feel the need to restate it because the statement for the plus group was missing in [3].

Theorem 2.9 ([3] Proposition 3.15) *Suppose*

$$\left(\widehat{E}^{\pm}(k(\mu_{p^\infty}))^{\eta} \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^{\vee} \cong \Lambda_{\mathrm{cyc}}^d.$$

for every character η of Δ. Or, equivalently, suppose

$$\left(\widehat{E}^{\pm}(k(\mu_{p^\infty})) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^{\vee} \cong \Lambda_{\mathrm{cyc}}[\Delta]^d.$$

Then, for every $n, m \geq 0$,

$$\left(\widehat{E}^{\pm}(k(\mu_{p^\infty}))/p^m \widehat{E}^{\pm}(k(\mu_{p^\infty})) \right)^{\mathrm{Gal}(k(\mu_{p^\infty})/k(\mu_{p^{n+1}}))}$$

is the exact annihilator of itself with respect to the local Tate pairing of

$$H^1\left(k(\mu_{p^{n+1}}), E[p^m]\right) \times H^1\left(k(\mu_{p^{n+1}}), E[p^m]\right) \longrightarrow \mathbb{Z}/p^m\mathbb{Z}.$$

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

2.2 More on the Plus/Minus Norm Groups

We note that the local class field theory implies that an unramified extension over a local field is totally determined by its degree. We let k be a (finite) unramified extension of $\mathbb{Q}_p$, and for any $m \geq 0$, we let k_m be the unique unramified extension of k with $\mathrm{Gal}(k_m/k) \cong \mathbb{Z}/p^m\mathbb{Z}$. As usual, we let μ_{p^n} denote the set of p^n-th roots of unity, and μ_{p^∞} denote $\cup_{n=0}^{\infty}\mu_{p^n}$.

First we give the following proposition.

Proposition 2.10 *For each n, we have*

$$\left(\widehat{E}(k_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{\mathrm{Gal}(k_n/k)} = \widehat{E}(k) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

Proof First, we note that for any finite extension L of $\mathbb{Q}_p$, by the local Tate duality, $\widehat{E}(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is the exact annihilator of $\widehat{E}(L)$ with respect to the non-degenerate pairing

$$(\,\cdot\,,\,\cdot\,)_L \colon H^1(L, E[p^\infty]) \times H^1(L, T_p(E)) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

induced from the Weil pairing (and $H^2(L, \mu_{p^\infty}) \xrightarrow{\sim} \mathbb{Q}_p/\mathbb{Z}_p$).

We note that $N_{k_n/k}(\widehat{E}(k_n)) = \widehat{E}(k)$. (It is not very difficult to prove, so we will say only a few things about the proof. Since k_n is unramified over $\mathbb{Q}_p$, $\widehat{E}(k_n) \cong p\mathcal{O}_{k_n}$ through the logarithm map $\log_{\widehat{E}}$. Since k_n/k is unramified, $\mathrm{Tr}_{k_n/k}(\mathcal{O}_{k_n}) = \mathcal{O}_k$, and our claim follows.)

Then we have the commutative diagram

$$\begin{array}{ccccc} H^1\left(k_n, E[p^\infty]\right) & \times & H^1\left(k_n, T_p(E)\right) & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p \\ {\scriptstyle \mathrm{Res}}\uparrow & & {\scriptstyle \mathrm{Cor}}\downarrow & & \downarrow \\ H^1\left(k, E[p^\infty]\right) & \times & H^1\left(k, T_p(E)\right) & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p. \end{array}$$

In other words, $(\mathrm{Res}\, x, y)_{k_n} = (x, \mathrm{Cor}\, y)_k$.

Suppose $x \in (\widehat{E}(k_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(k_n/k)}$. We can assume that $x = \mathrm{Res}(x')$ for some $x' \in H^1(k, E[p^\infty])$ by the Hochschild–Serre spectral sequence. Then

$$(x, y)_{k_n} = (x', \mathrm{Cor}\, y)_k.$$

It follows that we have

$$\left(x', \widehat{E}(k)\right)_k = \left(x', N_{k_n/k}\widehat{E}(k_n)\right)_k = \left(x', \mathrm{Cor}(\widehat{E}(k_n))\right)_k = \left(x, \widehat{E}(k_n)\right)_{k_n} = 0$$

(the last line is by the local Tate duality). Since x' is an annihilator of $\widehat{E}(k)$, again by the local Tate duality, $x \in \widehat{E}(k) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. Thus, $(E(k_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(k_n/k)} \subset E(k) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, and our claim follows, because it is clear that

$$E(k) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset \left(E(k_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{\mathrm{Gal}(k_n/k)}. \qquad \blacksquare$$

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

Let Γ denote $\mathrm{Gal}(k_\infty(\mu_{p^\infty})/k(\mu_p)) \cong \mathbb{Z}_p^2$, and recall that Δ denotes $\mathrm{Gal}(k(\mu_p)/k)$. We can obtain the following proposition.

Proposition 2.11 *We have*

$$\big[\widehat{E}^-(k_\infty(\mu_{p^\infty}))^\Delta \otimes \mathbb{Q}_p/\mathbb{Z}_p\big]^\vee \cong \mathbb{Z}_p[[\Gamma]]^{[k:\mathbb{Q}_p]}.$$

A similar statement holds for $\widehat{E}^+(k_\infty(\mu_{p^\infty}))^\Delta$ *if* p *is odd, and* $4 \nmid [k:\mathbb{Q}_p]$.

Proof We prove our claim for $\widehat{E}^-$ first.

By applying Theorem 2.7 and Proposition 2.10 repeatedly to every n, we have

$$\big[\widehat{E}^-(k_\infty(\mu_{p^\infty}))^\Delta \otimes \mathbb{Q}_p/\mathbb{Z}_p\big]^\Gamma = \widehat{E}(k) \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

Then, by Nakayama's lemma, we know that $[\widehat{E}^-(k_\infty(\mu_{p^\infty}))^\Delta \otimes \mathbb{Q}_p/\mathbb{Z}_p]^\vee$ is generated by $[k:\mathbb{Q}_p]$ elements over $\mathbb{Z}_p[[\Gamma]]$. Indeed, considering that each $\widehat{E}^-(k_n(\mu_{p^\infty}))^\Delta \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is co-free over $\mathbb{Z}_p[[\Gamma']]$ of rank $[k_n:\mathbb{Q}_p]$ where Γ' denotes

$$\mathrm{Gal}\big(k_\infty(\mu_{p^\infty})/k_\infty(\mu_p)\big) \cong \mathrm{Gal}\big(k_n(\mu_{p^\infty})/k_n(\mu_p)\big) \cong \mathbb{Z}_p,$$

we can see that $\widehat{E}^-(k_\infty(\mu_{p^\infty}))^\Delta \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is co-free over $\mathbb{Z}_p[[\Gamma]]$ of rank $[k:\mathbb{Q}_p]$.

The proof for $\widehat{E}^+$ is similar except that we apply Theorem 2.8 instead of Theorem 2.7. ∎

2.3 $\pm/\pm$-Selmer groups

Let K be an imaginary quadratic field over $\mathbb{Q}$ such that p splits completely (in other words, $pO_K = \mathfrak{p}\overline{\mathfrak{p}}$ for different prime ideals $\mathfrak{p}$ and $\overline{\mathfrak{p}}$). Let $\mathfrak{f}$ be any integral ideal of K prime to p. Let Δ_1 denote the group $\mathrm{Gal}(K(\mathfrak{f}p)/K(\mathfrak{f}))$.

Suppose E is an elliptic curve defined over K with good supersingular reduction at $\mathfrak{p}$ and $\overline{\mathfrak{p}}$. We also suppose that $a_\mathfrak{p} = 1 + N\mathfrak{p} - \#(\tilde{E}_\mathfrak{p}(\mathcal{O}_K/\mathfrak{p})) = 0$ and $a_{\overline{\mathfrak{p}}} = 1 + N\overline{\mathfrak{p}} - \#(\tilde{E}_{\overline{\mathfrak{p}}}(\mathcal{O}_K/\overline{\mathfrak{p}})) = 0$ where $\tilde{E}_\mathfrak{p}$ and $\tilde{E}_{\overline{\mathfrak{p}}}$ are the reduced curves modulo $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ in the respective cases. Because p splits completely over $K/\mathbb{Q}$, and E has good supersingular reduction at $\mathfrak{p}$ and $\overline{\mathfrak{p}}$, $a_\mathfrak{p}$ and $a_{\overline{\mathfrak{p}}}$ are 0 if $p > 3$ by Hasse's Inequality.

We also let $\Gamma = \mathrm{Gal}(K(\mathfrak{f}p^\infty)/K(\mathfrak{f}p)) \cong \mathbb{Z}_p^2$, $\Gamma_\mathfrak{p} = \mathrm{Gal}(K(\mathfrak{f}\mathfrak{p}^\infty)/K(\mathfrak{f}\mathfrak{p})) \cong \mathbb{Z}_p$, and $\Gamma_{\overline{\mathfrak{p}}} = \mathrm{Gal}(K(\mathfrak{f}\overline{\mathfrak{p}}^\infty)/K(\mathfrak{f}\overline{\mathfrak{p}})) \cong \mathbb{Z}_p$. Indeed, $\Gamma_\mathfrak{p}, \Gamma_{\overline{\mathfrak{p}}}$ can be considered subgroups of Γ, and we have $\Gamma \cong \Gamma_\mathfrak{p} \times \Gamma_{\overline{\mathfrak{p}}}$.

We can define $\widehat{E}^\pm$ in the direction of either $\mathfrak{p}^\infty$ or $\overline{\mathfrak{p}}^\infty$ as follows: First, suppose $\mathfrak{q}$ is a prime of $K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty)$ above $\mathfrak{p}$. We define

$$\widehat{E}^+\big(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_\mathfrak{q}\big) = \Big\{ x \in \widehat{E}\big(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_\mathfrak{q}\big) \mid \mathrm{Tr}_{K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_\mathfrak{q}/K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{l+2})_\mathfrak{q}}\, x \in \widehat{E}\big(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{l+1})_\mathfrak{q}\big) \text{ where } 0 \le l < n, 2 \mid l \Big\},$$

$$\widehat{E}^-\big(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_\mathfrak{q}\big) = \Big\{ x \in \widehat{E}\big(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_\mathfrak{q}\big) \mid \mathrm{Tr}_{K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_\mathfrak{q}/K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{l+2})_\mathfrak{q}}\, x \in \widehat{E}\big(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{l+1})_\mathfrak{q}\big) \text{ where } -1 \le l < n, 2 \nmid l \Big\}.$$

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

Similarly, where $\bar{\mathfrak{q}}$ is a prime of $K(\mathfrak{f}\mathfrak{p}^{\infty}\overline{\mathfrak{p}}^{\infty})$ above $\overline{\mathfrak{p}}$, we define $\widehat{E}^{\pm}(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\bar{\mathfrak{q}}})$ with the roles of $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ reversed as follows:

$$\widehat{E}^{+}(K\big(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\bar{\mathfrak{q}}}\big) = \Big\{ x \in \widehat{E}\big(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\bar{\mathfrak{q}}}\big) \mid \mathrm{Tr}_{K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\bar{\mathfrak{q}}}/K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{l+2})_{\bar{\mathfrak{q}}}} x \in \widehat{E}\big(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{l+1})_{\bar{\mathfrak{q}}}\big) \text{ where } 0 \le l < m, 2 \mid l \Big\},$$

$$\widehat{E}^{-}\big(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\bar{\mathfrak{q}}}\big) = \Big\{ x \in \widehat{E}\big(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\bar{\mathfrak{q}}}\big) \mid \mathrm{Tr}_{K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\bar{\mathfrak{q}}}/K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{l+2})_{\bar{\mathfrak{q}}}} x \in \widehat{E}\big(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{l+1})_{\bar{\mathfrak{q}}}\big) \text{ where } 0 < l < m, 2 \nmid l \Big\}.$$

Now we define the $\pm/\pm$-Selmer groups.

Definition 2.12 ($\pm/\pm$-Selmer groups) For a prime $\mathfrak{q}$ of $K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})$ above $\mathfrak{p}$, we let

$$\widehat{E}^{\pm}\big(K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})_{\mathfrak{q}}\big) = \cup_{m,n}\widehat{E}^{\pm}\big(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_{\mathfrak{q}}\big),$$

where, by abuse of notation, $\mathfrak{q} \subset K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})$ also denotes the prime that $\mathfrak{q} \subset K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})$ lies above. Similarly, for a prime $\bar{\mathfrak{q}}$ of $K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})$ above $\overline{\mathfrak{p}}$, we let

$$\widehat{E}^{\pm}\big(K(\mathfrak{f}\mathfrak{p}^{\infty}\overline{\mathfrak{p}}^{\infty})_{\bar{\mathfrak{q}}}\big) = \cup_{n,m}\widehat{E}^{\pm}\big(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\bar{\mathfrak{q}}}\big).$$

Then we define

$$\begin{aligned}\mathrm{sel}_p^{\pm/\pm}(E/K(\mathfrak{f}p^{\infty})) = \ker(H^1(K(\mathfrak{f}p^{\infty}), E[p^{\infty}]) &\to \prod_{w\nmid p}\frac{H^1(K(\mathfrak{f}p^{\infty})_w, E[p^{\infty}])}{E(K(\mathfrak{f}p^{\infty})_w)\otimes\mathbb{Q}_p/\mathbb{Z}_p}\\ &\times\prod_{\mathfrak{q}\mid\mathfrak{p}}\frac{H^1(K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})_{\mathfrak{q}}, E[p^{\infty}])}{\widehat{E}^{\pm}(K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})_{\mathfrak{q}})\otimes\mathbb{Q}_p/\mathbb{Z}_p}\\ &\times\prod_{\bar{\mathfrak{q}}\mid\overline{\mathfrak{p}}}\frac{H^1(K(\mathfrak{f}\mathfrak{p}^{\infty}\overline{\mathfrak{p}}^{\infty})_{\bar{\mathfrak{q}}}, E[p^{\infty}])}{\widehat{E}^{\pm}(K(\mathfrak{f}\mathfrak{p}^{\infty}\overline{\mathfrak{p}}^{\infty})_{\bar{\mathfrak{q}}})\otimes\mathbb{Q}_p/\mathbb{Z}_p}).\end{aligned}$$

From now on, we will study a "control theorem" of $\mathrm{sel}_p^{\pm/\pm}(E/K(\mathfrak{f}p^{\infty}))^{\Delta_1}$. (Except for the $\mathrm{sel}_p^{-/-}$ group, we will assume $4\nmid[K(\mathfrak{f})_{\mathfrak{p}}:\mathbb{Q}_p]$, $4\nmid[K(\mathfrak{f})_{\overline{\mathfrak{p}}}:\mathbb{Q}_p]$, and $p>2$.)

First, we need to define some plus/minus groups that we will use only temporarily. By abuse of notation, we let $K(\mathfrak{f})_{\bar{m},n}$ denote the unique field satisfying $K(\mathfrak{f}) \subset K(\mathfrak{f})_{\bar{m},n} \subset K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})$, and

$$\mathrm{Gal}(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})/K(\mathfrak{f})_{\bar{m},n}) \cong \Delta_1$$

(n, m could be ∞).

Recall the notation k_m from Section 2.2 that is defined as the unique unramified extension of an unramified local field k such that $\mathrm{Gal}(k_m/k) \cong \mathbb{Z}/p^m\mathbb{Z}$.

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

Put $k = K(\mathfrak{f})_{\mathfrak{q}}$ where $\mathfrak{q}$ is a prime above $\mathfrak{p}$, then because $\mathfrak{q}$ is unramified over $K(\mathfrak{f})_{\bar{m},0}/K(\mathfrak{f})$ and the degree $[K(\mathfrak{f})_{\bar{m},0}/K(\mathfrak{f})]$ is equal to $[k_m:k] = p^m$, we have

$$(K(\mathfrak{f})_{\bar{m},0})_{\mathfrak{q}} = k_m.$$

We let $k_m^{(n)}$ denote the field satisfying

$$k_m \subset k_m^{(n)} \subset k_m(\mu_{n+1}), \quad \text{and} \quad \mathrm{Gal}(k_m(\mu_{n+1})/k_m^{(n)}) \cong (\mathbb{Z}/p\mathbb{Z})^{\times}.$$

(We may write $k^{(n)}$ for $k_0^{(n)}$, and $K(\mathfrak{f})_n$ for $K(\mathfrak{f})_{\bar{0},n}$.)

Lemma 2.13 *For any $m \geq n \geq 0$, $(K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}} = k_m^{(n)}$.*

Proof Since $N_{k(\mu_{p^{n+1}})/k}(\zeta_{p^{n+1}} - 1) = p$, by the local class field theory we have the isomorphism

$$\mathrm{Gal}(k(\mu_{p^{n+1}})/k) \cong k^{\times}/\langle p\rangle \cdot (1 + p^{n+1}\mathcal{O}_k),$$

where $\langle p\rangle$ is the multiplicative group $p^{\mathbb{Z}}$. Thus,

$$\mathrm{Gal}(k^{(n)}/k) \cong k^{\times}/\langle p\rangle \cdot \mu(k^{\times}) \cdot (1 + p^{n+1}\mathcal{O}_k),$$

where $\mu(k^{\times})$ is the set of roots of unity of $k^{\times}$.

Similarly, there is an isomorphism

$$\mathrm{Gal}\big((K(\mathfrak{f})_{\bar{0},n})_{\mathfrak{q}}/k\big) \cong k^{\times}/\langle \pi\rangle \cdot \mu(k^{\times}) \cdot (1 + p^{n+1}\mathcal{O}_k)$$

for some uniformizer π of k.

Considering $k_m^{(n)}$ is unramified over $k^{(n)}$ with degree p^m, we have

$$\mathrm{Gal}(k_m^{(n)}/k) \cong k^{\times}/\langle p^{p^m}\rangle \cdot \mu(k^{\times}) \cdot (1 + p^{n+1}\mathcal{O}_k),$$

and similarly we have

$$\mathrm{Gal}(\big(K(\mathfrak{f})_{\bar{m},n}\big)_{\mathfrak{q}}/k) \cong k^{\times}/\langle \pi^{p^m}\rangle \cdot \mu(k^{\times}) \cdot (1 + p^{n+1}\mathcal{O}_k).$$

Since $(\pi/p)^{p^m} \in \mu(k^{\times}) \cdot (1 + p^{m+1}\mathcal{O}_k)$, our claim follows. ∎

Now we define certain plus/minus groups that we use only temporarily. We let $\widehat{E}^{\pm}(k_m^{(n)})$ denote the plus/minus groups defined by

$$\widehat{E}^{+}(k_m^{(n)}) \stackrel{\mathrm{def}}{=} \{x \in \widehat{E}(k_m^{(n)}) \mid \mathrm{Tr}_{k_m^{(n)}/k_m^{(l+1)}}(x) \in \widehat{E}(k_m^{(l)}) \text{ for } 0 \leq l < n, 2|l\},$$

$$\widehat{E}^{-}(k_m^{(n)}) \stackrel{\mathrm{def}}{=} \{x \in \widehat{E}(k_m^{(n)}) \mid \mathrm{Tr}_{k_m^{(n)}/k_m^{(l+1)}}(x) \in \widehat{E}(k_m^{(l)}) \text{ for } -1 \leq l < n, 2 \nmid l\}.$$

(Notationwise, we let $k_m^{(-1)} = k_m$.) It is not hard to see that $\widehat{E}^{\pm}(k_m^{(n)})$ is the same as $\widehat{E}^{\pm}(k_m(\mu_{p^{n+1}}))^{\Delta}$ from Definition 2.1.

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

Similarly, we also define

$$\widehat{E}^{+}\big((K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}}\big) \overset{\text{def}}{=} \Big\{ x \in \widehat{E}\big((K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}}\big) \mid \mathrm{Tr}_{(K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}}/(K(\mathfrak{f})_{\bar{m},l+1})_{\mathfrak{q}}}(x) \in \widehat{E}\big((K(\mathfrak{f})_{\bar{m},l})_{\mathfrak{q}}\big) \text{ for } 0 \le l < n, 2 \mid l \Big\},$$

$$\widehat{E}^{-}\big((K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}}\big) \overset{\text{def}}{=} \Big\{ x \in \widehat{E}\big((K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}}\big) \mid \mathrm{Tr}_{(K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}}/(K(\mathfrak{f})_{\bar{m},l+1})_{\mathfrak{q}}}(x) \in \widehat{E}\big((K(\mathfrak{f})_{\bar{m},l})_{\mathfrak{q}}\big) \text{ for } -1 \le l < n, 2 \nmid l \Big\}.$$

(Similarly, we assume that $K(\mathfrak{f})_{\bar{m},-1} = K(\mathfrak{f})_{\bar{m},0}$.)

For the following, we will use the notation $K(\mathfrak{f})_{n,\bar{m}}$ interchangeably with $K(\mathfrak{f})_{\bar{m},n}$. In a way similar to the prior construction, we define $\widehat{E}^{\pm}((K(\mathfrak{f})_{n,\bar{m}})_{\bar{\mathfrak{q}}})$ with the roles of $\bar{m}$ and n reversed as follows:

$$\widehat{E}^{+}\big((K(\mathfrak{f})_{n,\bar{m}})_{\bar{\mathfrak{q}}}\big) \overset{\text{def}}{=} \Big\{ x \in \widehat{E}\big((K(\mathfrak{f})_{n,\bar{m}})_{\bar{\mathfrak{q}}}\big) \mid \mathrm{Tr}_{(K(\mathfrak{f})_{n,\bar{m}})_{\bar{\mathfrak{q}}}/\left(K(\mathfrak{f})_{n,\overline{l+1}}\right)_{\bar{\mathfrak{q}}}}(x) \in \widehat{E}\big((K(\mathfrak{f})_{n,\bar{l}})_{\bar{\mathfrak{q}}}\big) \text{ for } 0 \le l < m, 2|l \Big\}.$$

$$\widehat{E}^{-}\big((K(\mathfrak{f})_{n,\bar{m}})_{\bar{\mathfrak{q}}}\big) \overset{\text{def}}{=} \Big\{ x \in \widehat{E}\big((K(\mathfrak{f})_{n,\bar{m}})_{\bar{\mathfrak{q}}}\big) \mid \mathrm{Tr}_{(K(\mathfrak{f})_{n,\bar{m}})_{\bar{\mathfrak{q}}}/\left(K(\mathfrak{f})_{n,\overline{l+1}}\right)_{\bar{\mathfrak{q}}}}(x) \in \widehat{E}\big((K(\mathfrak{f})_{n,\bar{l}})_{\bar{\mathfrak{q}}}\big) \text{ for } -1 \le l < m, 2 \nmid l \Big\}.$$

We concede that these are confusing notations. We consider it an unfortunate but inevitable consequence of having two primes above p to deal with.

Nonetheless, we can relate the groups $\widehat{E}^{\pm}(k_m^{(n)})$ (and this type of group was studied in Section 2.2) with $\widehat{E}^{\pm}((K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}})$, since we have $(K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}} = k_m^{(n)}$ if $m \ge n$ by Lemma 2.13. Hence, we have the following lemma.

Lemma 2.14 *If $m \ge n$, then $\widehat{E}^{\pm}(k_m^{(n)}) = \widehat{E}^{\pm}\big((K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}}\big)$.*

Proof As mentioned above, we have $(K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}} = k_m^{(n)}$ if $m \ge n$, thus those two groups in the statement are defined the same way if $m \ge n$. ∎

Then we immediately obtain the following proposition.

Proposition 2.15 *If $m \ge n$, then*

$$\widehat{E}\big((K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}}\big) = \widehat{E}^{+}\big((K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}}\big) + \widehat{E}^{-}\big((K(\mathfrak{f})_{\bar{m},n})_{\mathfrak{q}}\big).$$

Proof This follows immediately from Proposition 2.6 and Lemma 2.14. ∎

We do not have an immediate application of Proposition 2.15 at hand, but this type of theorem has proven useful in the past, so we are hopeful that this proposition may also be useful in the future.

We make the following (somewhat self-evident) definition.

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

Definition 2.16 $\widehat{E}^{\pm}\big(K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})_{\mathfrak{q}}\big) \overset{\text{def}}{=} \cup_{n,m=0}^{\infty}\widehat{E}^{\pm}\big(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_{\mathfrak{q}}\big)$.

Proposition 2.17

$$\big[\widehat{E}^{-}(K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})_{\mathfrak{q}})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p\big]^{\vee}\cong\mathbb{Z}_p[[\Gamma]]^{[K(\mathfrak{f})_{\mathfrak{q}}:\mathbb{Q}_p]}.$$

If $4\nmid[K(\mathfrak{f})_{\mathfrak{q}}:\mathbb{Q}_p]$ *and* $p>2$, *then we also have*

$$\big[\widehat{E}^{+}(K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})_{\mathfrak{q}})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p\big]^{\vee}\cong\mathbb{Z}_p[[\Gamma]]^{[K(\mathfrak{f})_{\mathfrak{q}}:\mathbb{Q}_p]}.$$

Proof Since $\widehat{E}^{\pm}((K(\mathfrak{f})_{\bar{n},n})_{\mathfrak{q}})=\widehat{E}^{\pm}(k_n^{(n)})$, we have

$$\widehat{E}^{\pm}\big(K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})_{\mathfrak{q}}\big)^{\Delta_1}=\widehat{E}^{\pm}\big((K(\mathfrak{f})_{\bar{\infty},\infty})_{\mathfrak{q}}\big)=\widehat{E}^{\pm}\big(k_{\infty}^{(\infty)}\big)$$

by Lemma 2.14, and the rest follows from Proposition 2.11. ∎

We use this versatile property to prove the following statement of the control theorem. Recall the notations $\omega_n(X),\omega_n^{+}(X),\omega_n^{-}(X)$ from Notation 2.3. Recall that we have the decomposition $\Gamma\cong\Gamma_{\mathfrak{p}}\times\Gamma_{\overline{\mathfrak{p}}}$, and choose topological generators $\gamma_{\mathfrak{p}}$ and $\gamma_{\overline{\mathfrak{p}}}$ of $\Gamma_{\mathfrak{p}}$ and $\Gamma_{\overline{\mathfrak{p}}}$. We identify $\mathbb{Z}_p[[\Gamma]]$ with $\mathbb{Z}_p[[S,T]]$ by $\gamma_{\mathfrak{p}}=S+1$, $\gamma_{\overline{\mathfrak{p}}}=T+1$.

Proposition 2.18 *For any integers* $m,n\geq 0$ *and any polynomial* $f_m(X)$ *dividing* $\omega_m(X)$, *we have*

$$\big[\widehat{E}^{-}(K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})_{\mathfrak{q}})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p\big]\,[\omega_n^{-}(S)][f_m(T)]=\big[\widehat{E}^{-}(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_{\mathfrak{q}})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p\big]\,[f_m(T)].$$

If $4\nmid[K(\mathfrak{f})_{\mathfrak{q}}:\mathbb{Q}_p]$ *and* $p>2$, *then we also have*

$$\big[\widehat{E}^{+}(K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})_{\mathfrak{q}})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p\big]\,[\omega_n^{+}(S)][f_m(T)]=\big[\widehat{E}^{+}(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_{\mathfrak{q}})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p\big]\,[f_m(T)].$$

Proof We only need to study the case where $f_m(T)=\omega_m(T)$.

From Proposition 2.17, we have

$$\big[\widehat{E}^{\pm}(K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})_{\mathfrak{q}})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p\big]\,[\omega_n^{\pm}(S)][\omega_m(T)]^{\vee}=\big(\mathbb{Z}_p[S,T]/(\omega_n^{\pm}(S),\omega_m(T))\big)^{[K(\mathfrak{f})_{\mathfrak{q}}:\mathbb{Q}_p]}.$$

On the other hand, it follows immediately from the definition that

$$\big[\widehat{E}^{\pm}(K(\mathfrak{f}\overline{\mathfrak{p}}^{\infty}\mathfrak{p}^{\infty})_{\mathfrak{q}})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p\big]\,\big[\omega_n^{\pm}(S)\big]\,\big[\omega_m(T)\big]$$

should contain $\widehat{E}^{\pm}(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_{\mathfrak{q}})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p$.

Note that both groups are divisible. The rest follows by comparing the coranks (see Remark 2.4). ∎

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

We recall that the standard way to define a Selmer group over a number field L is

$$\mathrm{sel}_p(E/L) \stackrel{\mathrm{def}}{=} \ker\Big(H^1(L, E[p^\infty]) \to \prod_w \frac{H^1(L_w, E[p^\infty])}{E(L_w)\otimes \mathbb{Q}_p/\mathbb{Z}_p}\Big)$$

where w runs over all the places of L. Also, we may define $\pm/\pm$-Selmer group of finite level as

$$\begin{aligned}\mathrm{sel}_p^{\pm/\pm}\big(E/K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})\big) \stackrel{\mathrm{def}}{=} \ker\Big(H^1(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1}), E[p^\infty])\\ \to \prod_{w\nmid p} \frac{H^1(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_w, E[p^\infty])}{E(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_w)\otimes \mathbb{Q}_p/\mathbb{Z}_p}\\ \times \prod_{\mathfrak{q}\mid\mathfrak{p}} \frac{H^1(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_\mathfrak{q}, E[p^\infty])}{\widehat{E}^{\pm}(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_\mathfrak{q})\otimes \mathbb{Q}_p/\mathbb{Z}_p}\\ \times \prod_{\bar{\mathfrak{q}}\mid\overline{\mathfrak{p}}} \frac{H^1(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\bar{\mathfrak{q}}}, E[p^\infty])}{\widehat{E}^{\pm}(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\bar{\mathfrak{q}}})\otimes \mathbb{Q}_p/\mathbb{Z}_p}\Big).\end{aligned}$$

Proposition 2.19 (Control Theorem) *In the following, we assume that $p > 2$, and $4 \nmid [K(\mathfrak{f})_\mathfrak{P} : \mathbb{Q}_p]$ for every prime $\mathfrak{P}$ above p except in the case of the $\mathrm{sel}_p^{-/-}$ group. For any integers $m, n \geq 0$, the natural homomorphism*

$$\mathrm{sel}_p^{\pm/\pm}\big(E/K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})\big)^{\Delta_1} \longrightarrow \mathrm{sel}_p^{\pm/\pm}\big(E/K(\mathfrak{f}\mathfrak{p}^{\infty}\overline{\mathfrak{p}}^{\infty})\big)^{\Delta_1}\big[\omega_n^{\pm}(S)\big]\big[\omega_m^{\pm}(T)\big]$$

has bounded kernel and cokernel as n and m vary.

Proof We apply the Snake Lemma to the commutative diagram (which is too large to draw in this space) given by connecting the following two short exact sequences:

$$\begin{aligned}0 \to\ & \mathrm{sel}_p^{\pm/\pm}(E/K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1}))^{\Delta_1}\\ \to\ & H^1(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1}), E[p^\infty])^{\Delta_1}[\omega_n^{\pm}(S)][\omega_m^{\pm}(T)]\\ \to\ & \prod_{w\nmid p} \frac{H^1(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_w, E[p^\infty])}{E(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_w)\otimes \mathbb{Q}_p/\mathbb{Z}_p}\\ & \times \prod_{\mathfrak{q}\mid\mathfrak{p}} \frac{H^1(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_\mathfrak{q}, E[p^\infty])}{\Big(\widehat{E}^{\pm}(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_\mathfrak{q})\otimes \mathbb{Q}_p/\mathbb{Z}_p\Big)}\\ & \times \prod_{\bar{\mathfrak{q}}\mid\overline{\mathfrak{p}}} \frac{H^1(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\bar{\mathfrak{q}}}, E[p^\infty])}{\Big(\widehat{E}^{\pm}(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\bar{\mathfrak{q}}})\otimes \mathbb{Q}_p/\mathbb{Z}_p\Big)}\end{aligned}$$

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

and

$$\begin{aligned}0 &\to \mathrm{sel}_p(E/K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty))^{\Delta_1}[\omega_n^\pm(S)][\omega_m^\pm(T)]\\ &\to H^1(K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty),E[p^\infty])^{\Delta_1}[\omega_n^\pm(S)][\omega_m^\pm(T)]\\ &\to \prod_{w\nmid p}\frac{H^1(K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty)_w,E[p^\infty])}{E(K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty)_w)\otimes\mathbb{Q}_p/\mathbb{Z}_p}\\ &\qquad\times\prod_{\mathfrak{q}\mid\mathfrak{p}}\frac{H^1(K(\mathfrak{f}\overline{\mathfrak{p}}^\infty\mathfrak{p}^\infty)_\mathfrak{q},E[p^\infty])}{\left(\widehat{E}^\pm(K(\mathfrak{f}\overline{\mathfrak{p}}^\infty\mathfrak{p}^\infty)_\mathfrak{q})\otimes\mathbb{Q}_p/\mathbb{Z}_p\right)[\omega_n^\pm(S)]}\\ &\qquad\times\prod_{\tilde{\mathfrak{q}}\mid\overline{\mathfrak{p}}}\frac{H^1(K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty)_{\tilde{\mathfrak{q}}},E[p^\infty])}{(\widehat{E}^\pm(K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty)_{\tilde{\mathfrak{q}}})\otimes\mathbb{Q}_p/\mathbb{Z}_p)[\omega_m^\pm(T)]}.\end{aligned}$$

The map

$$H^1\big(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1}),E[p^\infty]\big)^{\Delta_1}\big[\omega_n^\pm(S)\big]\big[\omega_m^\pm(T)\big]\longrightarrow H^1\big(K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty),E[p^\infty]\big)^{\Delta_1}\big[\omega_n^\pm(S)\big]\big[\omega_m^\pm(T)\big]$$

is an isomorphism, because

$$H^1\big(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1}),E[p^\infty]\big)^{\Delta_1}\to H^1\big(K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty),E[p^\infty]\big)^{\Delta_1}\big[\omega_n(S)\big]\big[\omega_m(T)\big]$$

is an isomorphism by the Hochschild–Serre spectral sequence.

The following statement about the local conditions at places not above p is a variation of a number of similar statements that can be found in many papers, and we omit its proof. (Among the common references are a series of Greenberg's papers. Also, one can find a similar variation in [3].) If $w\nmid p$, the kernel of the map

$$\frac{H^1(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_w,E[p^\infty])}{E(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_w)\otimes\mathbb{Q}_p/\mathbb{Z}_p}\longrightarrow\frac{H^1(K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty)_w,E[p^\infty])}{E(K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty)_w)\otimes\mathbb{Q}_p/\mathbb{Z}_p}$$

is finite and bounded as n and m vary, and indeed, trivial if E has good reduction at w.

It remains to show that the kernels of

$$\frac{H^1(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_\mathfrak{q},E[p^\infty])^{\Delta_1}}{(\widehat{E}^\pm(K(\mathfrak{f}\overline{\mathfrak{p}}^{m+1}\mathfrak{p}^{n+1})_\mathfrak{q})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p)}\longrightarrow\frac{H^1(K(\mathfrak{f}\overline{\mathfrak{p}}^\infty\mathfrak{p}^\infty)_\mathfrak{q},E[p^\infty])^{\Delta_1}}{(\widehat{E}^\pm(K(\mathfrak{f}\overline{\mathfrak{p}}^\infty\mathfrak{p}^\infty)_\mathfrak{q})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p)[\omega_n^\pm(S)]}$$

$$\frac{H^1(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\tilde{\mathfrak{q}}},E[p^\infty])^{\Delta_1}}{(\widehat{E}^\pm(K(\mathfrak{f}\mathfrak{p}^{n+1}\overline{\mathfrak{p}}^{m+1})_{\tilde{\mathfrak{q}}})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p)}\longrightarrow\frac{H^1(K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty)_{\tilde{\mathfrak{q}}},E[p^\infty])^{\Delta_1}}{(\widehat{E}^\pm(K(\mathfrak{f}\mathfrak{p}^\infty\overline{\mathfrak{p}}^\infty)_{\tilde{\mathfrak{q}}})^{\Delta_1}\otimes\mathbb{Q}_p/\mathbb{Z}_p)[\omega_n^\pm(T)]}$$

are finite and bounded (indeed trivial) as n and m vary. This follows from Proposition 2.18. ∎

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

3 A Conjectural Link with Loeffler's Two-variable $\pm/\pm$-p-adic L-functions

Recently, D. Loeffler told the author about his construction of $\pm/\pm$-p-adic L-functions. The importance and relevance of his work was obvious to the author, especially in connection with the work of this paper. For an elliptic curve $E/\mathbb{Q}$ with $a_p(E) = 0$, he constructed four integral measures $L_p^{\pm,\pm}$ on $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)$ interpolating the special values of the L-functions of the automorphic representation attached to an imaginary quadratic field K, and the elliptic curve E, twisted by finite characters of $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)$. By a well-known theorem of Iwasawa Theory, such measures can be considered as elements of the Iwasawa algebra $\mathbb{Z}_p[[\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)]]$, in other words, p-adic L-functions. Loeffler and S. Zerbes predicted such p-adic L-functions would exist [11].

The philosophy of Iwasawa Theory suggests the following conjecture.

Conjecture 3.1

$$(L_p^{\pm,\pm}) = \mathrm{char}(X^{\pm/\pm})$$

where $X^{\pm/\pm}$ is the Pontryagin dual $\mathrm{Hom}(\mathrm{sel}_p^{\pm/\pm}(E/K(\mathfrak{f}p^\infty)), \mathbb{Q}_p/\mathbb{Z}_p)$.

Note that in the statement, $(L_p^{\pm,\pm})$ and $\mathrm{char}(X^{\pm/\pm})$ are considered principal ideals of the Iwasawa algebra $\mathbb{Z}_p[[\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)]]$.

Before we finish the paper, we briefly explain Loeffler's construction for readers. First, we discuss S. Haran's generalized Mazur-Tate elements [1].

Let K be a number field, and π an automorphic representation of GL_2/K that is cohomological in trivial weight, and whose central character is trivial.

For an integral ideal $\mathfrak{g}$ of K, we let $G_\mathfrak{g}$ denote the ray class group modulo $\mathfrak{g}$. Then the universal Mazur–Tate element of conductor $\mathfrak{g}$ is an element of the module $\mathbb{Z}[G_\mathfrak{g}] \otimes H^{BM}_{r_1+r_2}(Y, \mathbb{Z})$ where r_1, r_2 are the numbers of real and imaginary places of K, Y is the locally symmetric space for $GL_2(\mathbb{A}_K)$, and H^{BM} is the Borel–Moore homology. Then Haran's generalized Mazur–Tate element $\Theta_\mathfrak{g}(\pi) \in \mathbb{Z}[G_\mathfrak{g}] \otimes_\mathbb{Z} \Lambda_\pi$ is given by evaluating the universal Mazur–Tate element of conductor $\mathfrak{g}$ against a class of $H^{r_1+r_2}_{\mathrm{par}}(Y, \mathbb{C})$ arising from π. (Here, Λ_π is some finitely generated abelian subgroup of $\mathbb{C}$. One needs to show that one can choose the class in such way that the resulting Mazur–Tate elements have coefficients in a finite extension $F/\mathbb{Q}$.)

When π is given by the base-change to K from the modular form attached to $E/\mathbb{Q}$, we have $\Lambda_\pi = \mathbb{Z}$, thus we drop it from the notation. In the manner described above, Haran constructs $\Theta_\mathfrak{g}(\pi) \in \mathbb{Z}[G_\mathfrak{g}]$ for each $\mathfrak{g}$. If $\mathfrak{l}$ is an integral ideal dividing $\mathfrak{g}$, these elements satisfy the norm relation

$$N_\mathfrak{g}^{\mathfrak{g}\mathfrak{l}}\Theta_{\mathfrak{g}\mathfrak{l}}(\pi) = a_\mathfrak{l}(\pi)\Theta_\mathfrak{g}(\pi) - \Theta_{\mathfrak{g}/\mathfrak{l}}(\pi).$$

Loeffler "p-stabilizes" these elements depending on the choice of a root $\alpha_\mathfrak{p}$ of the local Euler factor of π at $\mathfrak{p}$ for every prime $\mathfrak{p}$ of K above p (see [10, 4.2]). The result is a unique distribution $L_{p,\alpha}(\pi)$ on the ray class group $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)$ where α denotes the set of chosen roots $\{\alpha_\mathfrak{p}\}_{\mathfrak{p}|p}$. (Though he works with $\mathrm{Gal}(K(p^\infty)/K)$, it is

https://doi.org/10.4153/CJM-2013-043-2 Published online by Cambridge University Press

plausible that the same construction works for $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)$ for any integral ideal $\mathfrak{f}$ prime to p.) The distribution has the interpolation property

$$L_{p,\alpha}(\pi)(\omega) = \prod_{\mathfrak{p}|p} \alpha_{\mathfrak{p}}^{-\,\mathrm{ord}_{\mathfrak{p}}\,\mathfrak{f}_\omega} \frac{L(\pi,\omega,1)}{\tau(\omega)\cdot|\mathfrak{f}_\omega|(4\pi)^{[K:\mathbb{Q}]}}, \tag{3.1}$$

where ω is a finite-order character of $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)$ and $\mathfrak{f}_\omega$ is its conductor.

Now suppose that K is an imaginary quadratic field over which p splits completely, so that $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. Also suppose that $a_{\mathfrak{p}} = a_{\overline{\mathfrak{p}}} = 0$ and the weight of the automorphic form is 2. Then there are two choices for both $\alpha_{\mathfrak{p}}$, and $\alpha_{\overline{\mathfrak{p}}}$. They are the roots α, β of $X^2 - a_{\mathfrak{p}}X + N_{K/\mathbb{Q}}\mathfrak{p} = X^2 - a_{\overline{\mathfrak{p}}}X + N_{K/\mathbb{Q}}\overline{\mathfrak{p}} = X^2 + p$. Clearly, $\alpha = -\beta$, which plays a critical role in [10, Proposition 5.3]. Loeffler's p-adic L-functions are given by

$$\begin{aligned}
L_p^{+,+} &= (L_{p,\alpha,\alpha} + L_{p,\alpha,\beta} + L_{p,\beta,\alpha} + L_{p,\beta,\beta})/\log_{\mathfrak{p}}^{+}\log_{\overline{\mathfrak{p}}}^{+},\\
L_p^{+,-} &= (L_{p,\alpha,\alpha} - L_{p,\alpha,\beta} + L_{p,\beta,\alpha} - L_{p,\beta,\beta})/\log_{\mathfrak{p}}^{+}\log_{\overline{\mathfrak{p}}}^{-},\\
L_p^{-,+} &= (L_{p,\alpha,\alpha} + L_{p,\alpha,\beta} - L_{p,\beta,\alpha} - L_{p,\beta,\beta})/\log_{\mathfrak{p}}^{-}\log_{\overline{\mathfrak{p}}}^{+},\\
L_p^{-,-} &= (L_{p,\alpha,\alpha} - L_{p,\alpha,\beta} - L_{p,\beta,\alpha} + L_{p,\beta,\beta})/\log_{\mathfrak{p}}^{-}\log_{\overline{\mathfrak{p}}}^{-},
\end{aligned}$$

where $\log_p^{\pm}(X)$ are the half-logarithms defined in [14]. (See [10, Proposition 5.3] for the reason why $L_p^{\pm,\pm}$ are well defined.) Their interpolation properties follow from (3.1).

Acknowledgements I am deeply grateful to the referee who made countless priceless contributions. Also, I am grateful to David Loeffler for sharing his ideas and insights, and especially letting me know about his recent work, which turned out to be very relevant.

References

[1] S. Haran, *P-adic L-functions for modular forms*. Compositio Math. **62**(1987), no. 1, 31–46.
[2] A. Iovita and R. Pollack, *Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields*. J. Reine Angew. Math. **598**(2006), 71–103.
[3] B. D. Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*. Compos. Math **143**(2007), no. 1, 47–72. http://dx.doi.org/10.1112/S0010437X06002569
[4] ———, *Two-variable p-adic L-functions of modular forms for non-ordinary primes*. http://homepages.ecs.vuw.ac.nz/~bdkim/
[5] S.-I. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*. Invent. Math. **152**(2003), no. 1, 1–36. http://dx.doi.org/10.1007/s00222-002-0265-4
[6] M. Kurihara, *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I*. Invent. Math. **149**(2002), no. 1, 195–224. http://dx.doi.org/10.1007/s002220100206
[7] A. Lei, *Iwasawa theory for modular forms at supersingular primes*. Compos. Math. **147**(2011), no. 3, 803–838. http://dx.doi.org/10.1112/S0010437X10005130
[8] A. Lei, D. Loeffler, and S. L. Zerbes, *Wach modules and Iwasawa theory for modular forms*. Asian J. Math. **14**(2010), no. 4, 475–528. http://dx.doi.org/10.4310/AJM.2010.v14.n4.a2
[9] ———, *Coleman maps and p-adic regulator*. Algebra Number Theory **5**(2011), no. 8, 1095–1131. http://dx.doi.org/10.2140/ant.2011.5.1095
[10] D. Loeffler, *P-adic integration on ray class groups and non-ordinary p-adic L-functions*. To appear, Proceedings of the Conference Iwasawa, 2012. arxiv:1304.4042.

[11] D. Loeffler and S. Zerbes, *Iwasawa theory and p-adic L-functions for $\mathbb{Z}_p^2$-extensions*. arxiv:1108.5954.
[12] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*. Invent. Math. **18**(1972), 183–266. http://dx.doi.org/10.1007/BF01389815
[13] B. Perrin-Riou, *Théorie d'Iwasawa p-adique locale et globale.* Invent. Math. **99**(1990), no. 2, 247–292. http://dx.doi.org/10.1007/BF01234420
[14] R. Pollack, *On the p-adic L-function of a modular form at a supersingular prime.* Duke Math. J. **118**(2003), no. 3, 523–558. http://dx.doi.org/10.1215/S0012-7094-03-11835-9
[15] K. Rubin, *Local units, elliptic units, Heegner points and elliptic curves.* Invent. Math. **88**(1987), no. 2, 405–422. http://dx.doi.org/10.1007/BF01388915
[16] F. Sprung, *Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures.* J. Number Theory **132**(2012), no. 7, 1483–1506. http://dx.doi.org/10.1016/j.jnt.2011.11.003

Victoria University of Wellington
e-mail: bdkimster@gmail.com