J. Math. Soc. Japan
Vol. 76, No. 3 (2024) pp. 855–919
doi: 10.2969/jmsj/90699069

On derivatives of Kato's Euler system for elliptic curves

By David Burns, Masato Kurihara and Takamichi Sano

(Received Jan. 6, 2023)

Abstract. In this paper, we formulate a new conjecture concerning Kato's Euler system for elliptic curves E over $\mathbb{Q}$. This 'Generalized Perrin-Riou Conjecture' predicts a precise congruence relation between a Darmon-type derivative of the zeta element of E over an arbitrary real abelian field and the critical value of an appropriate higher derivative of the L-function of E over $\mathbb{Q}$. We prove the conjecture specializes in the relevant case of analytic rank one to recover Perrin-Riou's conjecture on the logarithms of zeta elements, and also that, under mild technical hypotheses, the 'order of vanishing' part of the conjecture is unconditionally valid in arbitrary rank. This approach also allows us to prove a natural higher-rank generalization of Rubin's formula concerning derivatives of p-adic L-functions and to establish an explicit connection between the p-part of the classical Birch and Swinnerton-Dyer formula and the Iwasawa main conjecture in arbitrary rank and for arbitrary reduction at p. In a companion article we prove that the approach developed here also provides a new interpretation of the Mazur–Tate conjecture that leads to the first (unconditional) theoretical evidence in support of this conjecture for curves of strictly positive rank.

1. Introduction.

1.1. Background.

A central problem in modern number theory is to understand the arithmetic meaning of the values of zeta and L-functions. The Birch and Swinnerton-Dyer conjecture and main conjecture in Iwasawa theory are important instances of this problem, being respectively related to the Hasse–Weil L-function of an elliptic curve and to the p-adic L-function of an appropriate motive.

For an elliptic curve E defined over $\mathbb{Q}$, significant progress on the problem was made by Kato in [**23**] who used Beilinson elements in the K-theory of modular curves to define canonical 'zeta elements' in étale (Galois) cohomology groups that could be explicitly related to the values of Hasse–Weil L-functions.

To be a little more precise we fix an odd prime p, a finite abelian extension F of $\mathbb{Q}$, a finite set of places S of $\mathbb{Q}$ that contains the Archimedean place, p, all primes that ramify in F and all primes at which E has bad reduction. We write $\mathcal{O}_{F,S}$ for the subring of F comprising elements that are integral at all non-Archimedean places whose residue characteristic does not belong to S and $T_p(E)$ for the p-adic Tate module of E.

Then the zeta element z_F constructed by Kato belongs to the étale cohomology group $H^1(\mathcal{O}_{F,S}, T_p(E))$ and is explicitly related via the dual exponential map to the value at one of the Hasse–Weil L-function of E (we assume the integrality of Kato's

2020 *Mathematics Subject Classification.* Primary 11G40; Secondary 11S40, 14G10, 11R23.
Key Words and Phrases. elliptic curves, Generalized Perrin-Riou Conjecture, higher rank Rubin's formula, zeta elements, derivatives of L-functions.

zeta element for simplicity: for more precise statements see Section 2). As F varies over subfields of finite degree of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, these elements z_F form a projective system that can be used to recover the p-adic L-function of E. In addition, as F varies more generally, the elements z_F form an Euler system and so can be used to bound the p-adic Selmer group of E. In this way zeta elements have led to partial results on both the main conjecture and Birch and Swinnerton-Dyer conjecture for E. For this reason, such elements have subsequently been much studied in the literature and have led to numerous important results.

Our main purpose in these articles is to investigate a conjectural property of Kato's elements that it seems has not been observed previously and to demonstrate that this property, whenever valid, has significant applications. The conjecture itself predicts a precise link between a 'Darmon-type' derivative of z_F for any given F and the value at the critical point of an appropriate higher derivative of the L-function of E over $\mathbb{Q}$. This conjectural link constitutes a simultaneous refinement of well-known conjectures of Perrin-Riou [**34**] and of Mazur and Tate [**29**] and will be described in more detail in the next section.

Although we shall not pursue it here, it seems reasonable to expect that the general approach we develop can also be applied to elliptic curves with complex multiplication, with the role of Kato's zeta elements being replaced by elliptic units twisted by a Hecke character.

We also expect that it should be possible to extend our approach to the setting of abelian varieties and to modular forms and their families, and we hope to return to these questions in a subsequent article.

1.2. Conjectures and results at finite level.

We shall now give an overview of the central conjecture that we formulate and the evidence for it that we have so far obtained.

1.2.1. At the outset we fix a finite *real* abelian extension F of $\mathbb{Q}$ and set $G := \mathrm{Gal}(F/\mathbb{Q})$. Then, following a general idea introduced by Darmon in [**15**], the key object of our study will be the element

$$\mathcal{N}_{F/\mathbb{Q}}(z_F) := \sum_{\sigma \in G} \sigma(z_F) \otimes \sigma^{-1}$$

of $H^1(\mathcal{O}_{F,S}, T_p(E)) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]$.

We write r for the rank of $E(\mathbb{Q})$ and assume that $r > 0$, that $E(\mathbb{Q})$ has no element of order p and that the p-part of the Tate–Shafarevich group of $E/\mathbb{Q}$ is finite. Then, under these hypotheses, in Definition 2.4 we shall use the leading term at $s = 1$ of $L(E, s)$ to (unconditionally) define a canonical 'Birch and Swinnerton-Dyer element' η^{BSD} in the dimension one vector space over $\mathbb{C}_p$ that is spanned by $\bigwedge^r_{\mathbb{Z}_p} H^1(\mathbb{Z}_S, T_p(E))$. With I denoting the augmentation ideal of $\mathbb{Z}_p[G]$, we shall also define (in Section 2.3) a canonical 'Bockstein regulator map'

$$\mathrm{Boc}_F : \bigwedge^r_{\mathbb{Z}_p} H^1(\mathbb{Z}_S, T_p(E)) \longrightarrow H^1(\mathbb{Z}_S, T_p(E)) \otimes_{\mathbb{Z}_p} I^{r-1}/I^r.$$

Finally we note the $\mathbb{Z}_p$-module $H^1(\mathcal{O}_{F,S}, T_p(E))$ is free and so $H^1(\mathcal{O}_{F,S}, T_p(E)) \otimes_{\mathbb{Z}_p} I^{r-1}$ identifies with a submodule of $H^1(\mathcal{O}_{F,S}, T_p(E)) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]$.

Then, in terms of this notation, the central conjecture of this article can be stated as follows.

Conjecture 1.1 (the Generalized Perrin-Riou Conjecture).

(i) ('*Order of vanishing*') $\mathcal{N}_{F/\mathbb{Q}}(z_F)$ *belongs to* $H^1(\mathcal{O}_{F,S}, T_p(E)) \otimes_{\mathbb{Z}_p} I^{r-1}$.

(ii) ('*Integrality*') η^{BSD} *belongs to* $\bigwedge^r_{\mathbb{Z}_p} H^1(\mathbb{Z}_S, T_p(E))$.

(iii) ('*Leading term formula*') *The image of* $\mathcal{N}_{F/\mathbb{Q}}(z_F)$ *in* $H^1(\mathcal{O}_{F,S}, T_p(E)) \otimes_{\mathbb{Z}_p} I^{r-1}/I^r$ *is equal to* $\mathrm{Boc}_F(\eta^{\mathrm{BSD}})$.

Remark 1.2. A precise statement of Conjecture 1.1 will be given as Conjecture 2.12. For the moment, we note a key advantage of its formulation is that it uses a construction of regulators that works in the same way for all reduction types. A further crucial advantage is that, in the case $r = 1$, the conjecture takes a particularly simple form and can be proved under various natural hypotheses.

In the rest of this section we outline the evidence that we have obtained for the above conjecture and also explain why it constitutes a simultaneous refinement and generalization of conjectures of Perrin-Riou and of Mazur and Tate.

1.2.2. We observe first that the containment predicted by Conjecture 1.1(i) can be studied by using the equivariant theory of Euler systems that was recently described by Sakamoto and the first and third authors in [**10**]. In particular, by using this approach we are able to prove that Conjecture 1.1(i) is valid under certain mild hypotheses.

For example, the following concrete result will follow directly from stronger results that we prove in Section 3. This result is a natural analogue for zeta elements of the main result of Darmon [**15**, Theorem 2.4] concerning Heegner points.

Theorem 1.3. *The containment of Conjecture* 1.1(i) *is valid if all of the following conditions are satisfied.*

(a) $p > 3$;

(b) *the* p*-primary part of* $Ш(E/F)$ *is finite*;

(c) *the image of the representation* $G_{\mathbb{Q}} \to \mathrm{Aut}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$ *contains* $\mathrm{SL}_2(\mathbb{Z}_p)$;

(d) *for every prime number* ℓ *in* S *the group* $E(\mathbb{Q}_\ell)$ *contains no element of order* p.

Remark 1.4. The assumption (a) in Theorem 1.3 can be removed by using the theory of Kolyvagin systems for $p = 3$ which has recently been developed by Sakamoto [**38**].

Concerning Conjecture 1.1(ii), we can show in all cases that the predicted containment is valid whenever the p-part of the Birch and Swinnerton-Dyer formula for E over $\mathbb{Q}$, or '$\mathrm{BSD}_p(E)$' as we shall abbreviate it in the sequel, is valid. (In fact, a stronger version of this result will be proved in Proposition 2.6.)

Finally, to discuss the prediction of Conjecture 1.1(iii) we shall initially specialize to the case that the analytic rank $\mathrm{ord}_{s=1}L(E,s)$ of E is equal to one. In this case, well-known results of Gross and Zagier and of Kolyvagin (amongst others) imply that $r=1$ and so parts (i) and (ii) of Conjecture 1.1 are valid trivially.

It is also straightforward to check in this case that the equality in Conjecture 1.1(iii) is valid for every choice of field F if and only if one has $z_{\mathbb{Q}} = \eta^{\mathrm{BSD}}$. By analysing the latter equality, we shall thereby obtain the explicit interpretation of this case of Conjecture 1.1 that is given in the next result. (A proof of this result will be explained in Remark 2.13(ii).)

In the sequel we write $L_S(E,s)$ for the S-truncated Hasse–Weil L-function of E.

Theorem 1.5. *If E has analytic rank one, then Conjecture* 1.1 *is valid for any field F if and only if one has $z_{\mathbb{Q}} \in H^1_f(\mathbb{Q}, T_p(E))$ and*

$$\log_\omega(z_{\mathbb{Q}}) = \frac{L'_S(E,1)}{\Omega^+ \cdot \langle x, x\rangle_\infty} \log_\omega(x)^2.$$

Here $\log_\omega : H^1_f(\mathbb{Q}, T_p(E)) \to \mathbb{Q}_p$ is the formal logarithm associated to the (fixed) Néron differential ω, $L'_S(E,1)$ denotes the value at $s=1$ of the first derivative of $L_S(E,s)$, Ω^+ is the real Néron period, x is a generator of $E(\mathbb{Q})$ modulo torsion and $\langle -,-\rangle_\infty$ is the Néron–Tate height pairing.

The displayed equality in Theorem 1.5 is equivalent to the central conjecture formulated by Perrin-Riou in [**34**, Section 3.3]. This result therefore allows us to regard Conjecture 1.1 as a natural extension of Perrin-Riou's conjecture to elliptic curves of arbitrary rank and, at the same time, to interpret results in support of Perrin-Riou's conjecture (see, for example, Büyükboduk [**13**, Theorem 2.4(iv)], Venerucci [**45**, Theorem A], Büyükboduk, Pollack and Sasaki [**14**] and Bertolini, Darmon and Venerucci [**4**]) as evidence in support of Conjecture 1.1 in the case of analytic rank one.

In a different direction, we show in the companion article [**9**] that the formalism leading to Conjecture 1.1 also gives rise to a new interpretation of the Mazur–Tate conjecture (from [**29**]) concerning congruence relations between modular symbols and the discriminants of height pairings defined in terms of geometrical bi-extensions, and thereby leads to the first (unconditional) theoretical evidence in support of the latter conjecture for elliptic curves of strictly positive rank.

We hope these observations give an indication of the interest of the general approach underlying the formulation of Conjecture 1.1. In this regard, we observe that one of the key motivations behind the development of this approach was an attempt to formulate a natural analogue for elliptic curves of the conjecture formulated in [**6**, Conjecture 5.4] in the setting of the multiplicative group. We finally recall that the latter conjecture was itself formulated as a natural strengthening of the 'refined class number formula for $\mathbb{G}_m$' that was previously conjectured by the third author [**39**], and (independently) by Mazur and Rubin [**28**].

1.3. Iwasawa-theoretic considerations.

In this section we discuss how the simultaneous study of Conjecture 1.1 for the family of intermediate fields F of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$ sheds light on a range of important problems.

1.3.1. To explain this, for each natural number n we write $\mathbb{Q}_n$ for the unique subfield of $\mathbb{Q}_\infty$ of degree p^n over $\mathbb{Q}$.

We know the validity of Conjecture 1.1(i) with $F = \mathbb{Q}_n$ (see Proposition 4.4), and we write κ_n for the image of $\mathcal{N}_{\mathbb{Q}_n/\mathbb{Q}}(z_{\mathbb{Q}_n})$ under the natural projection

$$H^1(\mathcal{O}_{\mathbb{Q}_n,S}, T_p(E)) \otimes_{\mathbb{Z}_p} I_n^{r-1} \to H^1(\mathcal{O}_{\mathbb{Q}_n,S}, T_p(E)) \otimes_{\mathbb{Z}_p} I_n^{r-1}/I_n^r,$$

where I_n denotes the augmentation ideal of $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]$.

Then we can show the element κ_n belongs to the subgroup $H^1(\mathbb{Z}_S, T_p(E)) \otimes_{\mathbb{Z}_p} I_n^{r-1}/I_n^r$ of $H^1(\mathcal{O}_{\mathbb{Q}_n,S}, T_p(E)) \otimes_{\mathbb{Z}_p} I_n^{r-1}/I_n^r$ and, moreover, that as n varies the elements κ_n are compatible with the natural projection maps

$$H^1(\mathbb{Z}_S, T_p(E)) \otimes_{\mathbb{Z}_p} I_n^{r-1}/I_n^r \to H^1(\mathbb{Z}_S, T_p(E)) \otimes_{\mathbb{Z}_p} I_{n-1}^{r-1}/I_{n-1}^r.$$

Hence, writing I for the augmentation ideal of $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$, one obtains an element of $H^1(\mathbb{Z}_S, T_p(E)) \otimes_{\mathbb{Z}_p} I^{r-1}/I^r$ by setting

$$\kappa_\infty := \varprojlim_n \kappa_n \in \varprojlim_n H^1(\mathbb{Z}_S, T_p(E)) \otimes_{\mathbb{Z}_p} I_n^{r-1}/I_n^r \simeq H^1(\mathbb{Z}_S, T_p(E)) \otimes_{\mathbb{Z}_p} I^{r-1}/I^r$$

(cf. Definition 4.5; we note that no conjecture is needed to deduce the existence of κ_∞).

In addition, the family of maps $(\mathrm{Boc}_{\mathbb{Q}_n})_n$ induces a canonical homomorphism

$$\mathbb{C}_p \cdot \bigwedge_{\mathbb{Z}_p}^r H^1(\mathbb{Z}_S, T_p(E)) \to \mathbb{C}_p \cdot H^1(\mathbb{Z}_S, T_p(E)) \otimes_{\mathbb{Z}_p} I^{r-1}/I^r$$

and the fact that the $\mathbb{Z}_p$-module I^{r-1}/I^r is torsion-free implies that the natural map

$$H^1(\mathbb{Z}_S, T_p(E)) \otimes_{\mathbb{Z}_p} I^{r-1}/I^r \to \mathbb{C}_p \cdot H^1(\mathbb{Z}_S, T_p(E)) \otimes_{\mathbb{Z}_p} I^{r-1}/I^r$$

is injective. In particular, this allows one to formulate Conjecture 1.1(iii) for the family of elements $\mathcal{N}_{\mathbb{Q}_n/\mathbb{Q}}(z_{\mathbb{Q}_n})$ without having to assume the validity of Conjecture 1.1(ii).

We shall show (in Proposition 4.14) that this version of Conjecture 1.1(iii) is equivalent to the following prediction.

In the sequel we write $L_S^{(r)}(E,1)$ for the coefficient of $(s-1)^r$ in the Taylor expansion at $s=1$ of $L_S(E,s)$.

Conjecture 1.6 (Conjecture 4.8). *If r is also equal to the analytic rank $\mathrm{ord}_{s=1}L(E,s)$ of E, then one has*

$$\kappa_\infty = \frac{L_S^{(r)}(E,1)}{\Omega^+ \cdot R_\infty} \cdot R_\omega^{\mathrm{Boc}},$$

*where Ω^+ is the real Néron period, R_∞ is the Néron–Tate regulator and R_ω^{Boc} is the '*Bockstein regulator*' in $H^1(\mathbb{Z}_S, T_p(E)) \otimes_{\mathbb{Z}_p} I^{r-1}/I^r$ that is introduced in Definition* 4.10.

Remark 1.7. If r is equal to $\mathrm{ord}_{s=1}L(E,s)$, then the r-th derivative of $L_S(E,s)$ is holomorphic at $s=1$ and its (non-zero) value at $s=1$ is equal to $r!\cdot L_S^{(r)}(E,1)$.

Remark 1.8. We will show that the Bockstein regulator that occurs in Conjecture 1.6 has the following properties.

(i) If $r=1$, then

$$R_\omega^{\mathrm{Boc}} = \log_\omega(x)\cdot x$$

for any element x of $E(\mathbb{Q})$ that generates $E(\mathbb{Q})$ modulo torsion (cf. Remark 4.12).

(ii) Suppose that E does not have additive reduction at p and write $\langle -,-\rangle_p$ for the classical p-adic height pairing. Then for any element x of $E(\mathbb{Q})$ one has

$$\langle x, R_\omega^{\mathrm{Boc}}\rangle_p = \log_\omega(x)\cdot R_p,$$

where R_p denotes the p-adic regulator (cf. Theorems 5.6 and 5.11).

If $r=1$, then κ_∞ simply coincides with $z_{\mathbb{Q}}$ and so Remark 1.8(i) implies that Conjecture 1.6 is valid if and only if one has

$$z_{\mathbb{Q}} = \frac{L_S'(E,1)}{\Omega^+\cdot R_\infty}\log_\omega(x)\cdot x$$

for any element x of $E(\mathbb{Q})$ that generates $E(\mathbb{Q})$ modulo torsion. This equality is equivalent to Perrin-Riou's conjecture.

In addition, whilst Remark 1.8(ii) implies that the Bockstein regulator R_ω^{Boc} is a variant of the classical p-adic regulator, a key role will be played in our approach by the fact that R_ω^{Boc} can be defined even in the case that E has additive reduction at p (in which case a construction of the p-adic regulator is still unknown).

1.3.2. To interpret Conjecture 1.6 in terms of p-adic L-functions, we must first prove a 'generalized Rubin formula' for the element κ_∞.

To discuss this result, and some of its consequences, we assume until further notice that E does not have additive reduction at p.

If E has good reduction at p, then we write α for an allowable root of the Hecke polynomial X^2-a_pX+p. We set $\beta := p/\alpha$.

If E has non-split multiplicative reduction at p, then we set $\alpha := -1$ and $\beta := -p$.

We also write $\mathcal{L}_{S,p}^{(r)}$ for the 'r-th derivative' of the S-truncated p-adic L-function $\mathcal{L}_{S,p}$ of E (for a precise definition of this term see Section 6.2).

Theorem 1.9 (the generalized Rubin formula, Theorem 6.2).

(i) *If E has good or non-split multiplicative reduction at p, then for every element x of $E(\mathbb{Q})$ one has*

$$\langle x,\kappa_\infty\rangle_p = \left(1-\frac{1}{\alpha}\right)^{-1}\left(1-\frac{1}{\beta}\right)\log_\omega(x)\cdot\mathcal{L}_{S,p}^{(r)}.$$

(ii) *If E has split multiplicative reduction at p, then for every element x of $E(\mathbb{Q})$ one has*

$$\langle x, \kappa_\infty \rangle_p \cdot \mathcal{L} = \left(1 - \frac{1}{p}\right) \log_\omega(x) \cdot \mathcal{L}_{S,p}^{(r+1)},$$

where $\mathcal{L}$ denotes the '$\mathcal{L}$-invariant' of E (see Remark 6.4).

REMARK 1.10. If $r = 1$, then one has $\kappa_\infty = z_\mathbb{Q}$ and Theorem 1.9(i) recovers the formula that is proved by Rubin in [**36**, Theorem 1(ii)] in the case that E has good ordinary reduction at p.

We shall then show that this result has the following consequences.

COROLLARY 1.11 (Corollary 6.7). *The Generalized Perrin-Riou Conjecture (Conjecture 1.6) implies the following 'p-adic Beilinson formula': one has*

$$\left(1 - \frac{1}{\alpha}\right)^{-1} \left(1 - \frac{1}{\beta}\right) \mathcal{L}_{S,p}^{(r)} = \frac{L_S^{(r)}(E,1)}{\Omega^+ \cdot R_\infty} R_p$$

if E has good or non-split multiplicative reduction at p, and

$$\mathcal{L}_{S,p}^{(r+1)} = \mathcal{L} \cdot \frac{L_{S\setminus\{p\}}^{(r)}(E,1)}{\Omega^+ \cdot R_\infty} R_p$$

if E has split multiplicative reduction at p.

In the next result we refer to the Iwasawa main conjecture for E and $\mathbb{Q}_\infty/\mathbb{Q}$ that is formulated in Conjecture 7.1.

COROLLARY 1.12 (Corollary 7.4). *Assume that the p-primary part of $Ш(E/\mathbb{Q})$ is finite and E does not have additive reduction at p. Then the Iwasawa main conjecture for E and $\mathbb{Q}_\infty/\mathbb{Q}$ implies the validity up to multiplication by an element of $\mathbb{Z}_p^\times$ of the p-adic Birch and Swinnerton-Dyer formula for E.*

REMARK 1.13. If the p-adic height pairing is non-degenerate, then the result of Corollary 1.12 was first proved by Schneider [**41**] (in the good ordinary case), Jones [**21**] (in the multiplicative case) and Perrin-Riou in [**34**] (in the good supersingular case).

1.3.3. Going beyond the result of Corollary 1.12, our approach also allows the detailed analysis of descent arguments in Iwasawa theory without restrictive hypotheses on either the analytic rank or reduction type of E (and hence, therefore, for curves with additive reduction at p).

For example, in this way we are able to prove the following analogue for E of the main result of our earlier article [**7**] concerning the equivariant Tamagawa number conjecture for $\mathbb{G}_m$ (cf. Remark 7.7). We note, in particular, that since the following result imposes no restrictions on the reduction of E at p, it sheds some new light on the link between main conjectures in Iwasawa theory and the classical Birch and Swinnerton-Dyer conjecture.

Theorem 1.14 (Theorem 7.6). *Assume all of the following hypotheses*:

- $Ш(E/\mathbb{Q})$ *is finite*;
- *the analytic rank of* E *is equal to the rank* r *of* $E(\mathbb{Q})$;
- *the Iwasawa main conjecture of Conjecture* 7.1 *is valid*;
- *the Generalized Perrin-Riou Conjecture of Conjecture* 1.6 *is valid*;
- *the Bockstein regulator* R_ω^{Boc} *does not vanish.*

Then there exists an element u *of* $\mathbb{Z}_p^\times$ *such that*

$$\frac{L^{(r)}(E,1)}{\Omega^+ \cdot R_\infty} = u \cdot \frac{\#Ш(E/\mathbb{Q}) \cdot \mathrm{Tam}(E)}{\#E(\mathbb{Q})_{\mathrm{tors}}^2},$$

where $\mathrm{Tam}(E)$ *denotes the product of the Tamagawa factors of* $E/\mathbb{Q}$.

In particular, the conjecture $\mathrm{BSD}_p(E)$ *is valid.*

1.4. General notation.

For the reader's convenience we collect together some of the general notation that will be used throughout this article.

At the outset we fix an *odd* prime number p. The symbol ℓ will also usually denote a prime number.

For a field K, the absolute Galois group of K is denoted by G_K.

We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. We also fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

For a positive integer m, we denote by $\mu_m \subset \overline{\mathbb{Q}}$ the group of m-th roots of unity.

For an abelian group X, we use the following notations:

- X_{tors}: the subgroup of torsion elements;
- $X_{\mathrm{tf}} := X/X_{\mathrm{tors}}$: the torsion-free quotient;
- $\mathrm{rank}(X) := \mathrm{rank}_{\mathbb{Z}}(X_{\mathrm{tf}})$;
- $X[p]$: the subgroup of elements annihilated by p;
- $X[p^\infty]$: the subgroup of elements annihilated by a power of p.

If X is endowed with an action of complex conjugation, we denote by X^+ the subgroup of X fixed by the action.

If X is an R-module (with R a commutative ring), we set

$$X^* := \mathrm{Hom}_R(X, R).$$

Note that this notation has ambiguity, since X may be regarded as an R'-module with another ring R' and X^* can mean $\mathrm{Hom}_{R'}(X, R')$. However, this ambiguity would not make any danger of confusion since the meaning is usually clear from the context.

For an element $x \in X$, we denote by $\langle x \rangle_R$ the submodule generated by x over R. We abbreviate it to $\langle x \rangle$ when R is clear from the context.

Suppose that X is a free R-module with basis $\{x_1, \dots, x_r\}$. We denote by

$$x_i^* : X \to R$$

the dual of x_i, i.e., the map defined by

$$x_j \mapsto \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

For a perfect complex C of R-modules, we denote by $\det_R(C)$ the determinant module of C. This module is understood to be a graded invertible R-module (with the grade suppressed from the symbol).

For a number field F and a finite set S of places of $\mathbb{Q}$, we denote by $\mathcal{O}_{F,S}$ the ring of S_F-integers of F, where S_F denotes the set of places of F lying above a place in S. In particular, $\mathcal{O}_{\mathbb{Q},S}$ is denoted simply by $\mathbb{Z}_S$. We denote by $\mathsf{R}\Gamma(\mathcal{O}_{F,S}, -)$ the etale cohomology complex $\mathsf{R}\Gamma_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_{F,S}), -)$.

As usual, the notation $H^i_f(F, -)$ indicates the Bloch–Kato Selmer group and $H^i_f(F_v, -)$ the Bloch–Kato local condition for a place v of F.

For an elliptic curve E defined over $\mathbb{Q}$, we denote by $L(E, s)$ the Hasse–Weil L-function of E. For a finite set S of places of $\mathbb{Q}$, we denote by $L_S(E, s)$ the S-truncated L-function of E. We denote by $L^*_S(E, 1)$ the leading term at $s = 1$.

The Tate–Shafarevich group of E over a number field F is denoted by $Ш(E/F)$. The product of Tamagawa factors of $E/\mathbb{Q}$ is denoted by $\mathrm{Tam}(E)$.

We use some other standard notations concerning elliptic curves and modular curves, such as $\Gamma(E, \Omega^1_{E/\mathbb{Q}})$, $H_1(E(\mathbb{C}), \mathbb{Q})$, $E_1(\mathbb{Q}_p)$, $Y_1(N)$, $X_1(N)$, etc.

2. Formulation of the Generalized Perrin-Riou Conjecture.

We fix a prime number p and assume throughout the article that p is odd.

2.1. Kato's Euler system.

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N.

Fix a modular parametrization $\phi : X_1(N) \to E$ and write $f = \sum_{n=1}^{\infty} a_n q^n$ for the normalized newform of weight 2 and level N corresponding to E.

Let $T_p(E)$ be the p-adic Tate module of E and set $V := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(E)$. Let T be a $G_{\mathbb{Q}}$-stable sublattice of V that is given by the image of the following map:

$$\begin{aligned} H^1(Y_1(N) \times_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Z}_p(1)) &\hookrightarrow H^1(Y_1(N) \times_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_p(1)) \\ &\twoheadrightarrow H^1(X_1(N) \times_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_p(1)) \\ &\xrightarrow{\phi_*} H^1(E \times_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_p(1)) \\ &= V^*(1) \\ &\simeq V, \end{aligned} \tag{2.1.1}$$

where the second arrow is the Manin–Drinfeld splitting (see [**42**, Section 5.2] or [**18**, Section 1.9.3]), the third is induced by ϕ and the last is induced by the Weil pairing.

Note that T identifies with the maximal quotient of $H^1(Y_1(N) \times_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Z}_p(1))$ on which Hecke operators $T(n)$ act via a_n and may be different from $T_p(E)$. If $E[p]$ is an irreducible $G_{\mathbb{Q}}$-representation, we may assume $T = T_p(E)$.

We fix the following data:

- an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$;
- a finite set S of places of $\mathbb{Q}$ such that $\{\infty\} \cup \{\ell \mid pN\} \subset S$;
- integers $c, d > 1$ such that cd is coprime to 6 and all primes in S, and that $c \equiv d \equiv 1 \pmod{N}$;
- an element $\xi \in \mathrm{SL}_2(\mathbb{Z})$.

For this data and any positive integer m that is coprime to cd, Kato constructed in [**23**, (8.1.3)] a 'zeta element'

$$ {}_{c,d}z_m(\xi, S_m) := {}_{c,d}z_m^{(p)}(f, 1, 1, \xi, S_m \setminus \{\infty\}) $$

in $H^1(\mathcal{O}_{\mathbb{Q}(\mu_m), S_m}, T)$, where S_m denotes the set $S \cup \{\ell \mid m\}$.

It is also known that the collection $({}_{c,d}z_m(\xi, S_m))_m$ forms an Euler system (see [**23**, Example 13.3]).

For a finite abelian extension F of $\mathbb{Q}$ that is unramified outside S, we set

$$ {}_{c,d}z_F = {}_{c,d}z_F(\xi, S) := \mathrm{Cor}_{\mathbb{Q}(\mu_m)/F}({}_{c,d}z_m(\xi, S)), $$

where $m = m_F$ denotes the conductor of F.

For later purposes we make a specific choice of ξ as follows. Just as in (2.1.1), the fixed modular parametrization $\phi : X_1(N) \to E$ induces a map

$$ \begin{aligned} H_1(X_1(N)(\mathbb{C}), \{\text{cusps}\}, \mathbb{Z}) &\simeq H^1(Y_1(N)(\mathbb{C}), \mathbb{Z}(1)) \\ &\to H^1(E(\mathbb{C}), \mathbb{Q}(1)) \simeq H_1(E(\mathbb{C}), \mathbb{Q}), \end{aligned} \tag{2.1.2} $$

where the first and last isomorphisms are obtained by the Poincaré duality.

We write $\mathscr{H}$ for the image of this map (so $\mathscr{H}$ is a lattice of $H_1(E(\mathbb{C}), \mathbb{Q})$) and let

$$ \delta(\xi) \in \mathscr{H} $$

denote the image under the map (2.1.2) of the modular symbol

$$ \{\xi(0), \xi(\infty)\} \in H_1(X_1(N)(\mathbb{C}), \{\text{cusps}\}, \mathbb{Z}). $$

Let g denote the complex conjugation and set $e^+ := (1 + g)/2$.

We then fix ξ so that the following condition is satisfied:

$$ \text{the element } e^+\delta(\xi) \text{ of } H_1(E(\mathbb{C}), \mathbb{Q})^+ \text{ is a } \mathbb{Z}_{(p)}\text{-basis of } (\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathscr{H})^+. \tag{2.1.3} $$

The existence of such $\xi \in \mathrm{SL}_2(\mathbb{Z})$ is justified as follows. By a well-known theorem of Manin, we know that $H_1(X_1(N)(\mathbb{C}), \{\text{cusps}\}, \mathbb{Z})$ is generated by the set $\{\{\alpha(0), \alpha(\infty)\} \mid \alpha \in \mathrm{SL}_2(\mathbb{Z})\}$. This implies that the $\mathbb{Z}_{(p)}$-module $(\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathscr{H})^+$ is generated by the set $\{e^+\delta(\alpha) \mid \alpha \in \mathrm{SL}_2(\mathbb{Z})\}$. Since $(\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathscr{H})^+ \simeq \mathbb{Z}_{(p)}$ and $\mathbb{Z}_{(p)}$ is local, Nakayama's lemma implies the existence of $\xi \in \mathrm{SL}_2(\mathbb{Z})$ such that $e^+\delta(\xi)$ generates $(\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathscr{H})^+$.

Throughout this article, we also fix a minimal Weierstrass model of E over $\mathbb{Z}$ and let

$$\omega \in \Gamma(E, \Omega^1_{E/\mathbb{Q}})$$

be the corresponding Néron differential.

We define the real period for (ω, ξ) by setting

$$\Omega_\xi := \int_{e^+\delta(\xi)} \omega. \tag{2.1.4}$$

(In general, this integral need only agree with the usual real Néron period Ω^+ up to multiplication by an element of $\mathbb{Q}^\times$. However, if $E[p]$ is irreducible, then Ω_ξ and Ω^+ will agree up to multiplication by an element of $\mathbb{Z}_{(p)}^\times$.)

Then Kato's reciprocity law [**23**, Theorems 6.6 and 9.7] gives the formula

$$\exp^*_\omega({}_{c,d}z_{\mathbb{Q}}) = cd(c-1)(d-1)\frac{L_S(E,1)}{\Omega_\xi} \text{ in } \mathbb{Q}, \tag{2.1.5}$$

where $\exp^*_\omega : H^1(\mathbb{Z}_S, T) \to H^1(\mathbb{Q}_p, T) \to \mathbb{Q}_p$ is the dual exponential map associated to ω.

Remark 2.1. As in [**23**, Theorem 12.5], one may normalize Kato's zeta element in order to construct an element z of $H^1(\mathbb{Z}_S, V)$ with the property that $\exp^*_\omega(z) = L_{\{p\}}(E,1)/\Omega^+$, where the L-function is truncated just at p rather than at all places in S. However, one does not in general know that this element z lies in $H^1(\mathbb{Z}_S, T)$. This delicate integrality issue is the reason that we prefer to use ${}_{c,d}z_{\mathbb{Q}} = {}_{c,d}z_{\mathbb{Q}}(\xi, S)$ rather than the normalized element. In addition, if $H^1(\mathbb{Z}_S, T)$ is $\mathbb{Z}_p$-free, then one expects that the element

$$z_{\mathbb{Q}} := \frac{1}{cd(c-1)(d-1)} \cdot {}_{c,d}z_{\mathbb{Q}}$$

of $H^1(\mathbb{Z}_S, V)$ actually belongs to $H^1(\mathbb{Z}_S, T)$ but, as far as we are aware, this has not been proved in full generality.

2.2. Birch and Swinnerton-Dyer elements.

In this subsection, we introduce a natural notion of 'Birch and Swinnerton-Dyer element'.

Such elements constitute an analogue for elliptic curves of the 'Rubin–Stark elements' that are associated to the multiplicative group.

In the sequel we shall denote the 'algebraic rank' $\mathrm{rank}(E(\mathbb{Q}))$ of E over $\mathbb{Q}$ by r_{alg} or often, for simplicity, by r.

Throughout this section we shall then assume the following.

HYPOTHESIS 2.2.

(i) $H^1(\mathbb{Z}_S, T)$ *is* $\mathbb{Z}_p$*-free*;

(ii) $r := r_{\mathrm{alg}} > 0$;

(iii) $Ш(E/\mathbb{Q})[p^\infty]$ *is finite.*

REMARK 2.3. If $E[p]$ is irreducible, then $T = T_p(E)$ and $E(\mathbb{Q})[p] = 0$ so Hypothesis 2.2(i) is automatically satisfied.

Following [**10**, Lemma 6.1], we note that these assumptions imply the existence of a canonical isomorphism

$$H^1(\mathbb{Z}_S, V) \simeq \mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q}) \tag{2.2.1}$$

and also, since the image of the localization map $H^1(\mathbb{Z}_S, V) \to H^1(\mathbb{Q}_p, V)$ lies in $H^1_f(\mathbb{Q}_p, V) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} E_1(\mathbb{Q}_p)$, of a canonical short exact sequence

$$0 \to \mathbb{Q}_p \otimes_{\mathbb{Z}_p} E_1(\mathbb{Q}_p)^* \to \mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})^* \to H^2(\mathbb{Z}_S, V) \to 0. \tag{2.2.2}$$

We fix an embedding $\mathbb{R} \hookrightarrow \mathbb{C}_p$ and consider the following canonical 'period-regulator' isomorphism of $\mathbb{C}_p$-modules

$$\begin{aligned}
\lambda : \mathbb{C}_p \otimes_{\mathbb{Z}_p} \bigwedge\nolimits^r_{\mathbb{Z}_p} H^1(\mathbb{Z}_S, T) &\simeq \mathbb{C}_p \otimes_{\mathbb{Z}} \bigwedge\nolimits^r_{\mathbb{Z}} E(\mathbb{Q}) \\
&\simeq \mathbb{C}_p \otimes_{\mathbb{Z}} \bigwedge\nolimits^r_{\mathbb{Z}} E(\mathbb{Q})^* \\
&\simeq \mathbb{C}_p \otimes_{\mathbb{Q}_p} \left(E_1(\mathbb{Q}_p)^* \otimes_{\mathbb{Z}_p} \bigwedge\nolimits^{r-1}_{\mathbb{Q}_p} H^2(\mathbb{Z}_S, V) \right) \\
&\simeq \mathbb{C}_p \otimes_{\mathbb{Q}_p} \left(\Gamma\big(E, \Omega^1_{E/\mathbb{Q}}\big) \otimes_{\mathbb{Q}} \bigwedge\nolimits^{r-1}_{\mathbb{Q}_p} H^2(\mathbb{Z}_S, V) \right) \\
&\simeq \mathbb{C}_p \otimes_{\mathbb{Q}_p} \left(H_1(E(\mathbb{C}), \mathbb{Q})^{+,*} \otimes_{\mathbb{Q}} \bigwedge\nolimits^{r-1}_{\mathbb{Q}_p} H^2(\mathbb{Z}_S, V) \right).
\end{aligned}$$

Here the first isomorphism is induced by (2.2.1), the second by the Néron–Tate height pairing

$$\langle -, - \rangle_\infty : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R},$$

the third by (2.2.2), the fourth by the dual exponential map

$$\exp^* : E_1(\mathbb{Q}_p)^* \to \mathbb{Q}_p \otimes_{\mathbb{Q}} \Gamma\big(E, \Omega^1_{E/\mathbb{Q}}\big),$$

the last by the period map

$$\Gamma(E, \Omega^1_{E/\mathbb{Q}}) \to H_1(E(\mathbb{C}), \mathbb{R})^{+,*};\ \omega \mapsto \left(\gamma \mapsto \int_\gamma \omega \right).$$

DEFINITION 2.4. Fix an element $\boldsymbol{x}$ of the space $\bigwedge_{\mathbb{Q}_p}^{r-1} H^2(\mathbb{Z}_S, V)$. Then the *Birch and Swinnerton-Dyer element* $\eta_{\boldsymbol{x}}^{\mathrm{BSD}} = \eta_{\boldsymbol{x}}^{\mathrm{BSD}}(\xi, S)$ of the data ξ, S and $\boldsymbol{x}$ is the element of $\mathbb{C}_p \otimes_{\mathbb{Z}_p} \bigwedge_{\mathbb{Z}_p}^{r} H^1(\mathbb{Z}_S, T)$ obtained by setting

$$\eta_{\boldsymbol{x}}^{\mathrm{BSD}} := \lambda^{-1}\big(L_S^*(E,1) \cdot (e^+\delta(\xi)^* \otimes \boldsymbol{x})\big).$$

The '(c,d)-modified Birch and Swinnerton-Dyer element' for the given data is the element

$${}_{c,d}\eta_{\boldsymbol{x}}^{\mathrm{BSD}} := cd(c-1)(d-1) \cdot \eta_{\boldsymbol{x}}^{\mathrm{BSD}}.$$

REMARK 2.5. Each choice of an ordered basis of $E(\mathbb{Q})_{\mathrm{tf}}$ gives rise to a natural choice of element $\boldsymbol{x}$ as above (see Section 4.3.2). In the special case $r = 1$ and $\boldsymbol{x} = 1$, the above definition simplifies to an equality

$$\eta_{\boldsymbol{x}}^{\mathrm{BSD}} = \frac{L_S^*(E,1)}{\Omega_\xi \cdot R_\infty} \cdot \log_\omega(x) \cdot x$$

in $\mathbb{C}_p \otimes_{\mathbb{Z}} E(\mathbb{Q}) \simeq \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^1(\mathbb{Z}_S, T)$, where R_∞ is the Néron–Tate regulator, $\log_\omega : E(\mathbb{Q}) \to E(\mathbb{Q}_p) \to \mathbb{Q}_p$ is the formal group logarithm associated to ω and x is any element of $E(\mathbb{Q})$ that generates $E(\mathbb{Q})_{\mathrm{tf}}$.

The p-part of the Birch and Swinnerton-Dyer formula for E asserts that there should be an equality of $\mathbb{Z}_p$-submodules of $\mathbb{C}_p$ of the form

$$L^*(E,1) \cdot \mathbb{Z}_p = \big(\#Ш(E/\mathbb{Q})[p^\infty] \cdot \mathrm{Tam}(E) \cdot \#E(\mathbb{Q})_{\mathrm{tors}}^{-2} \cdot \Omega^+ \cdot R_\infty\big) \cdot \mathbb{Z}_p,$$

where $\mathrm{Tam}(E)$ denotes the product of the Tamagawa factors of $E/\mathbb{Q}$. In the sequel we shall abbreviate this equality of lattices to '$\mathrm{BSD}_p(E)$'.

The next result explains the connection between this conjectural equality and the integrality properties of Birch and Swinnerton-Dyer elements.

PROPOSITION 2.6. *Set $r := r_{\mathrm{alg}}$ and fix a $\mathbb{Z}_p$-basis $\boldsymbol{x}$ of the lattice $\bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}}$. Then $\mathrm{BSD}_p(E)$ is valid if and only if there is an equality of $\mathbb{Z}_p$-lattices*

$$\mathbb{Z}_p \cdot \eta_{\boldsymbol{x}}^{\mathrm{BSD}} = \#H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \cdot \bigwedge_{\mathbb{Z}_p}^{r} H^1(\mathbb{Z}_S, T). \tag{2.2.3}$$

In particular, the validity of $\mathrm{BSD}_p(E)$ implies that $\eta_{\boldsymbol{x}}^{\mathrm{BSD}}$ belongs to $\bigwedge_{\mathbb{Z}_p}^{r} H^1(\mathbb{Z}_S, T)$.

PROOF. It is well-known that the validity of $\mathrm{BSD}_p(E)$ is equivalent to the equality of lattices that underlies the statement of the Tamagawa number conjecture (or 'TNC' for short) for the pair $(h^1(E)(1), \mathbb{Z}_p)$ (this has been shown, for example, by Kings in [**24**]). It is therefore sufficient to show that the equality (2.2.3) is equivalent to the TNC and to do this we must recall the formulation of the latter conjecture.

The statement of the TNC involves a canonical isomorphism of $\mathbb{C}_p$-modules

$$\vartheta : \mathbb{C}_p \otimes_{\mathbb{Z}_p} \det_{\mathbb{Z}_p}^{-1}\big(\mathrm{R}\Gamma_c(\mathbb{Z}_S, T^*(1))\big) \xrightarrow{\sim} \mathbb{C}_p \tag{2.2.4}$$

that arises as follows. Firstly, global duality induces a canonical isomorphism

$$\det_{\mathbb{Z}_p}^{-1}\big(\mathsf{R}\Gamma_c(\mathbb{Z}_S, T^*(1))\big) \simeq \det_{\mathbb{Z}_p}^{-1}(\mathsf{R}\Gamma(\mathbb{Z}_S, T)) \otimes_{\mathbb{Z}_p} T^*(1)^+$$

(cf. [**11**, Proposition 2.22]) and hence also a canonical isomorphism

$$\begin{aligned}&\mathbb{C}_p \otimes_{\mathbb{Z}_p} \det_{\mathbb{Z}_p}^{-1}\big(\mathsf{R}\Gamma_c(\mathbb{Z}_S, T^*(1))\big)\\ &\quad\simeq \mathbb{C}_p \otimes_{\mathbb{Q}_p} \left(\bigwedge_{\mathbb{Q}_p}^{r} H^1(\mathbb{Z}_S, V) \otimes_{\mathbb{Q}_p} \bigwedge_{\mathbb{Q}_p}^{r-1} H^2(\mathbb{Z}_S, V)^* \otimes_{\mathbb{Q}_p} V^*(1)^+\right). \qquad (2.2.5)\end{aligned}$$

The isomorphism ϑ in (2.2.4) is then obtained by combining the latter isomorphism with the canonical 'comparison' isomorphism

$$V^*(1)^+ \simeq \mathbb{Q}_p \otimes_{\mathbb{Q}} H^1(E(\mathbb{C}), \mathbb{Q}(1))^+ \simeq \mathbb{Q}_p \otimes_{\mathbb{Q}} H_1(E(\mathbb{C}), \mathbb{Q})^+$$

and the period-regulator isomorphism

$$\lambda : \mathbb{C}_p \otimes_{\mathbb{Q}_p} \bigwedge_{\mathbb{Q}_p}^{r} H^1(\mathbb{Z}_S, V) \simeq \mathbb{C}_p \otimes_{\mathbb{Q}_p} \left(H_1(E(\mathbb{C}), \mathbb{Q})^{+,*} \otimes_{\mathbb{Q}} \bigwedge_{\mathbb{Q}_p}^{r-1} H^2(\mathbb{Z}_S, V)\right)$$

constructed earlier.

If $\mathfrak{z}$ is the unique element of $\mathbb{C}_p \otimes_{\mathbb{Z}_p} \det_{\mathbb{Z}_p}^{-1}(\mathsf{R}\Gamma_c(\mathbb{Z}_S, T^*(1)))$ that satisfies $\vartheta(\mathfrak{z}) = L_S^*(E, 1)$, then the TNC predicts that

$$\mathbb{Z}_p \cdot \mathfrak{z} = \det_{\mathbb{Z}_p}^{-1}\big(\mathsf{R}\Gamma_c(\mathbb{Z}_S, T^*(1))\big).$$

Given this, the claimed result is a consequence of the fact that the isomorphism (2.2.5) sends the element $\mathfrak{z}$ to

$$\eta_{\boldsymbol{x}}^{\mathrm{BSD}} \otimes \boldsymbol{x}^* \otimes e^+\delta(\xi) \in \mathbb{C}_p \otimes_{\mathbb{Q}_p} \left(\bigwedge_{\mathbb{Q}_p}^{r} H^1(\mathbb{Z}_S, V) \otimes_{\mathbb{Q}_p} \bigwedge_{\mathbb{Q}_p}^{r-1} H^2(\mathbb{Z}_S, V)^* \otimes_{\mathbb{Q}_p} V^*(1)^+\right),$$

and the lattice $\det_{\mathbb{Z}_p}^{-1}(\mathsf{R}\Gamma_c(\mathbb{Z}_S, T^*(1)))$ to

$$\#H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \cdot \bigwedge_{\mathbb{Z}_p}^{r} H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} \bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)^*_{\mathrm{tf}} \otimes_{\mathbb{Z}_p} T^*(1)^+. \qquad \square$$

2.3. Bockstein regulator maps.

In this subsection, we shall introduce a canonical construction of Bockstein regulator maps (see (2.3.3) below).

We first set some notations. Let $F/\mathbb{Q}$ be a finite abelian extension unramified outside S and G its Galois group. Since all results and conjectures we study are of p-adic nature, we may assume that $[F : \mathbb{Q}]$ is a p-power. In particular, since p is odd, F is a totally real field. The augmentation ideal

$$I_F := \ker(\mathbb{Z}_p[G] \twoheadrightarrow \mathbb{Z}_p)$$

and the augmentation quotients

$$Q_F^a := I_F^a / I_F^{a+1}$$

for a non-negative integer a will play important roles. We remark that Q_F^0 is understood to be $\mathbb{Z}_p[G]/I_F = \mathbb{Z}_p$.

For simplicity, in this subsection we shall abbreviate the ideal I_F to I.

At the outset we note that the tautological short exact sequence

$$0 \to I/I^2 \to \mathbb{Z}_p[G]/I^2 \to \mathbb{Z}_p \to 0$$

gives rise to a canonical exact triangle of complexes of $\mathbb{Z}_p$-modules of the form

$$\mathsf{R}\Gamma(\mathcal{O}_{F,S}, T) \otimes^{\mathsf{L}}_{\mathbb{Z}_p[G]} I/I^2 \to \mathsf{R}\Gamma(\mathcal{O}_{F,S}, T) \otimes^{\mathsf{L}}_{\mathbb{Z}_p[G]} \mathbb{Z}_p[G]/I^2 \to \mathsf{R}\Gamma(\mathcal{O}_{F,S}, T) \otimes^{\mathsf{L}}_{\mathbb{Z}_p[G]} \mathbb{Z}_p.$$

Next we recall (from, for example, [**17**, Proposition 1.6.5]) that $\mathsf{R}\Gamma(\mathcal{O}_{F,S}, T)$ is acyclic outside degrees one and two and that there exists a canonical isomorphism in the derived category of $\mathbb{Z}_p$-modules

$$\mathsf{R}\Gamma(\mathcal{O}_{F,S}, T) \otimes^{\mathsf{L}}_{\mathbb{Z}_p[G]} \mathbb{Z}_p \simeq \mathsf{R}\Gamma(\mathbb{Z}_S, T). \tag{2.3.1}$$

Taking account of these facts, the above triangle gives rise to a morphism of complexes of $\mathbb{Z}_p$-modules

$$\delta_F : \mathsf{R}\Gamma(\mathbb{Z}_S, T) \to \big(\mathsf{R}\Gamma(\mathbb{Z}_S, T) \otimes^{\mathsf{L}}_{\mathbb{Z}_p} I/I^2\big)[1]$$

and hence to a composite homomorphism of $\mathbb{Z}_p$-modules

$$\begin{aligned} \beta_F : H^1(\mathbb{Z}_S, T) &\xrightarrow{(-1)\times H^1(\delta_F)} H^2\big(\mathsf{R}\Gamma(\mathbb{Z}_S, T) \otimes^{\mathsf{L}}_{\mathbb{Z}_p} I/I^2\big) \\ &= \quad H^2(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} I/I^2 \\ &\twoheadrightarrow \quad H^2(\mathbb{Z}_S, T)_{\mathrm{tf}} \otimes_{\mathbb{Z}_p} I/I^2, \end{aligned} \tag{2.3.2}$$

in which the equality is valid since $\mathsf{R}\Gamma(\mathbb{Z}_S, T)$ is acyclic in degrees greater than two and the last map is induced by the natural map from $H^2(\mathbb{Z}_S, T)$ to $H^2(\mathbb{Z}_S, T)_{\mathrm{tf}}$.

We write

$$\mathrm{Boc}_F : \bigwedge^r_{\mathbb{Z}_p} H^1(\mathbb{Z}_S, T) \to H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} \bigwedge^{r-1}_{\mathbb{Z}_p} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}} \otimes_{\mathbb{Z}_p} Q_F^{r-1}$$

for the homomorphism of $\mathbb{Z}_p$-modules with the property that

$$\mathrm{Boc}_F(y_1 \wedge \cdots \wedge y_r) = \sum_{i=1}^{r} (-1)^{i+1} y_i \otimes \big(\beta_F(y_1) \wedge \cdots \wedge \beta_F(y_{i-1}) \wedge \beta_F(y_{i+1}) \wedge \cdots \beta_F(y_r)\big)$$

for all elements y_i of $H^1(\mathbb{Z}_S, T)$.

Then, each choice of basis element $\boldsymbol{x}$ of the (free, rank one) $\mathbb{Z}_p$-module $\bigwedge^{r-1}_{\mathbb{Z}_p} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}}$, gives rise to a composite 'Bockstein regulator' homomorphism

$$\begin{aligned} \mathrm{Boc}_{F,\boldsymbol{x}} : \bigwedge^r_{\mathbb{Z}_p} H^1(\mathbb{Z}_S, T) &\xrightarrow{\mathrm{Boc}_F} H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} \bigwedge^{r-1}_{\mathbb{Z}_p} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}} \otimes_{\mathbb{Z}_p} Q_F^{r-1} \\ &\xrightarrow{\mathrm{id}\otimes\phi_{\boldsymbol{x}}\otimes\mathrm{id}} H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} Q_F^{r-1}, \end{aligned} \tag{2.3.3}$$

where $\phi_{\boldsymbol{x}}$ is the isomorphism $\bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}} \simeq \mathbb{Z}_p$ induced by the choice of $\boldsymbol{x}$.

REMARK 2.7. If $r = 1$ and $\boldsymbol{x} = 1$ is the canonical basis of $\bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}} = \mathbb{Z}_p$, then $\mathrm{Boc}_{F,\boldsymbol{x}} = \mathrm{Boc}_F$ is simply equal to the identity map on $H^1(\mathbb{Z}_S, T)$.

2.4. The Generalized Perrin-Riou Conjecture.

In the sequel we shall write r_{an} for the analytic rank $\mathrm{ord}_{s=1} L(E, s)$ of E.

2.4.1. In [**34**], Perrin-Riou investigates relations between Kato's Euler system and the p-adic Birch and Swinnerton-Dyer conjecture. In particular, she formulates the following conjecture.

CONJECTURE 2.8 (Perrin-Riou [**34**], see also [**13**]).

(i) *The element* ${}_{c,d}z_{\mathbb{Q}}$ *is non-zero if and only if* r_{an} *is at most one.*

(ii) *If* $r_{\mathrm{an}} = r_{\mathrm{alg}} = 1$, *then in* $\mathbb{C}_p \otimes_{\mathbb{Z}_p} H^1(\mathbb{Z}_S, T) \simeq \mathbb{C}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})$ *one has*

$$ {}_{c,d}z_{\mathbb{Q}} = cd(c-1)(d-1)\frac{L'_S(E,1)}{\Omega_\xi \cdot R_\infty} \log_\omega(x) \cdot x, \tag{2.4.1} $$

where x *is any element of* $E(\mathbb{Q})$ *that generates* $E(\mathbb{Q})_{\mathrm{tf}}$.

REMARK 2.9. This conjecture is a slight modification of, but equivalent to, Perrin-Riou's original formulation of the conjecture. By Kato's reciprocity law (2.1.5), the element ${}_{c,d}z_{\mathbb{Q}}$ is explicitly related to $L(E,1)$ and, in particular, does not vanish if $r_{\mathrm{an}} = 0$. Perrin-Riou's conjecture predicts that ${}_{c,d}z_{\mathbb{Q}}$ does not vanish even if $r_{\mathrm{an}} = 1$ and, moreover, that it should be explicitly related to the first derivative $L'(E,1)$ via the formula (2.4.1).

By Remark 2.5, we immediately obtain the following interpretation of Perrin-Riou's conjecture in terms of the BSD element.

PROPOSITION 2.10. *If* $r_{\mathrm{an}} = r_{\mathrm{alg}} = 1$ *and* $\boldsymbol{x} = 1$, *then Conjecture* 2.8(ii) *is valid if and only if one has* ${}_{c,d}z_{\mathbb{Q}} = {}_{c,d}\eta_{\boldsymbol{x}}^{\mathrm{BSD}}$.

REMARK 2.11. An interpretation of Perrin-Riou's conjecture in the same style as Proposition 2.10 was previously given by Sakamoto and the first and the third authors in [**10**, Section 6]. (In fact, a natural 'equivariant' refinement of this conjecture is also formulated in loc. cit.)

2.4.2. We shall now give a precise formulation of Conjecture 1.1.

For this purpose we will always assume the validity of Hypothesis 2.2. We also use the notation I_F and Q_F^a introduced in Section 2.3.

We set $r := r_{\mathrm{alg}}$ and write

$$ \begin{aligned} \iota_F : H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} Q_F^{r-1} &\to H^1(\mathcal{O}_{F,S}, T) \otimes_{\mathbb{Z}_p} Q_F^{r-1} \\ &\to H^1(\mathcal{O}_{F,S}, T) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]/I_F^r \end{aligned} \tag{2.4.2} $$

for the composite homomorphism that is induced by the restriction map $H^1(\mathbb{Z}_S, T) \to H^1(\mathcal{O}_{F,S}, T)$ and the natural inclusion $Q_F^{r-1} \hookrightarrow \mathbb{Z}_p[G]/I_F^r$. This map ι_F is actually injective. (This follows easily from the facts that $H^1(\mathbb{Z}_S, T)$ is $\mathbb{Z}_p$-free and that $H^1(\mathbb{Z}_S, T)$ identifies with the submodule $H^1(\mathcal{O}_{F,S}, T)^G$ of G-invariant elements in $H^1(\mathcal{O}_{F,S}, T)$ (since $H^0(\mathbb{Z}_S, T)$ vanishes).)

Motivated by constructions of Darmon in [**16**] and [**15**] (relating to cyclotomic units and to Heegner points respectively), we define the 'Darmon norm' of ${}_{c,d}z_F$ to be the element of $H^1(\mathcal{O}_{F,S}, T) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]$ obtained by setting

$$\mathcal{N}_{F/\mathbb{Q}}({}_{c,d}z_F) := \sum_{\sigma \in G} \sigma({}_{c,d}z_F) \otimes \sigma^{-1}.$$

We can now give a precise formulation of Conjecture 1.1. This prediction involves the Birch and Swinnerton-Dyer element ${}_{c,d}\eta_{\boldsymbol{x}}^{\mathrm{BSD}}$ and Bockstein regulator map $\mathrm{Boc}_{F,\boldsymbol{x}}$ that were respectively defined in Sections 2.2 and 2.3.

Conjecture 2.12 (the Generalized Perrin-Riou Conjecture). *Set $r := r_{\mathrm{alg}}$. Then for each $\mathbb{Z}_p$-basis element $\boldsymbol{x}$ of $\bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}}$ the following claims are valid.*

(i) *The element ${}_{c,d}\eta_{\boldsymbol{x}}^{\mathrm{BSD}}$ belongs to $\bigwedge_{\mathbb{Z}_p}^{r} H^1(\mathbb{Z}_S, T)$.*

(ii) *The image in $H^1(\mathcal{O}_{F,S}, T) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]/I_F^r$ of the Darmon norm $\mathcal{N}_{F/\mathbb{Q}}({}_{c,d}z_F)$ of ${}_{c,d}z_F$ is equal to $\iota_F\big(\mathrm{Boc}_{F,\boldsymbol{x}}({}_{c,d}\eta_{\boldsymbol{x}}^{\mathrm{BSD}})\big)$.*

Remark 2.13.

(i) Proposition 2.6 shows that Conjecture 2.12(i) is implied by the validity of $\mathrm{BSD}_p(E)$.

(ii) Assume $r_{\mathrm{alg}} = 1$ and that $\boldsymbol{x} = 1$ in $\bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}} = \mathbb{Z}_p$. Then in this case one has

$$\mathcal{N}_{F/\mathbb{Q}}({}_{c,d}z_F) = \mathrm{N}_{F/\mathbb{Q}}({}_{c,d}z_F) \text{ in } H^1(\mathcal{O}_{F,S}, T) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]/I_F \simeq H^1(\mathcal{O}_{F,S}, T),$$

where $\mathrm{N}_{F/\mathbb{Q}} := \sum_{\sigma \in G} \sigma$. In particular, since $\mathrm{Cor}_{F/\mathbb{Q}}({}_{c,d}z_F) = {}_{c,d}z_{\mathbb{Q}}$ and $\mathrm{Boc}_{F,\boldsymbol{x}}$ is the identity map on $H^1(\mathbb{Z}_S, T)$ (by Remark 2.7), Conjecture 2.12 is equivalent in this case to an equality ${}_{c,d}z_{\mathbb{Q}} = {}_{c,d}\eta_{\boldsymbol{x}}^{\mathrm{BSD}}$. From Proposition 2.10 it therefore follows that if $r_{\mathrm{an}} = r_{\mathrm{alg}} = 1$ then Conjecture 2.12 is equivalent to Perrin-Riou's conjecture (as stated in Conjecture 2.8(ii)). This observation proves Theorem 1.5 and also motivates us to refer to Conjecture 2.12 as the 'Generalized Perrin-Riou Conjecture'.

Remark 2.14. The formulation of Conjecture 2.12 can also be regarded as a natural analogue for elliptic curves of the conjectural 'refined class number formula for $\mathbb{G}_m$' concerning Rubin–Stark elements that was originally formulated independently by Mazur and Rubin [**28**, Conjecture 5.2] and by the third author [**39**, Conjecture 3] and then subsequently refined by the present authors in [**6**, Conjecture 5.4].

Remark 2.15. It is straightforward to show that the element $\mathrm{Boc}_{F,\boldsymbol{x}}({}_{c,d}\eta_{\boldsymbol{x}}^{\mathrm{BSD}})$, and hence also the validity of Conjecture 2.12(ii), is independent of the choice of basis element $\boldsymbol{x}$.

Remark 2.16. In Section 4.1 we will reinterpret Conjecture 2.12 in terms of a natural 'Darmon-type' derivative of ${}_{c,d}z_F$.

2.5. An algebraic analogue.

We now formulate an analogue of Conjecture 2.12 that is more algebraic, and elementary, in nature.

To do this we recall that if $Ш(E/\mathbb{Q})$ is finite, then the Birch and Swinnerton-Dyer formula for E predicts that

$$L_S^*(E,1) = \left(\prod_{\ell \in S\setminus\{\infty\}} L_\ell\right) \frac{\#Ш(E/\mathbb{Q}) \cdot \mathrm{Tam}(E) \cdot \Omega^+ \cdot R_\infty}{\#E(\mathbb{Q})_{\mathrm{tors}}^2}, \tag{2.5.1}$$

where Ω^+ is the usual real Néron period of E, L_ℓ is the standard Euler factor at ℓ of the Hasse–Weil L-function (so that $(\prod_{\ell\in S\setminus\{\infty\}} L_\ell)L^*(E,1) = L_S^*(E,1)$) and $\mathrm{Tam}(E)$ is the product of Tamagawa factors.

Definition 2.17. Set $r := r_{\mathrm{alg}}$. Then for each element $\boldsymbol{x}$ of $\bigwedge_{\mathbb{Q}_p}^{r-1} H^2(\mathbb{Z}_S, V)$ the *algebraic Birch and Swinnerton-Dyer element* $\eta_{\boldsymbol{x}}^{\mathrm{alg}} = \eta_{\boldsymbol{x}}^{\mathrm{alg}}(\xi, S)$ of the data ξ, S and $\boldsymbol{x}$ is the element of $\mathbb{C}_p \otimes_{\mathbb{Z}_p} \bigwedge_{\mathbb{Z}_p}^r H^1(\mathbb{Z}_S, T)$ obtained by setting

$$\eta_{\boldsymbol{x}}^{\mathrm{alg}} := \lambda^{-1}\left(\left(\prod_{\ell\in S\setminus\{\infty\}} L_\ell\right) \frac{\#Ш(E/\mathbb{Q}) \cdot \mathrm{Tam}(E) \cdot \Omega^+ \cdot R_\infty}{\#E(\mathbb{Q})_{\mathrm{tors}}^2} \cdot (e^+\delta(\xi)^* \otimes \boldsymbol{x})\right).$$

The '(c,d)-modified algebraic Birch and Swinnerton-Dyer element' of the given data is then defined by setting

$${}_{c,d}\eta_{\boldsymbol{x}}^{\mathrm{alg}} := cd(c-1)(d-1) \cdot \eta_{\boldsymbol{x}}^{\mathrm{alg}}.$$

Remark 2.18. It is clear that, if $\boldsymbol{x}$ is non-zero, then the Birch and Swinnerton-Dyer formula (2.5.1) is valid for E if and only if the elements $\eta_{\boldsymbol{x}}^{\mathrm{alg}}$ and ${}_{c,d}\eta_{\boldsymbol{x}}^{\mathrm{alg}}$ are respectively equal to the Birch and Swinnerton-Dyer elements $\eta_{\boldsymbol{x}}^{\mathrm{BSD}}$ and ${}_{c,d}\eta_{\boldsymbol{x}}^{\mathrm{BSD}}$ from Definition 2.4.

An easy exercise shows that if $\boldsymbol{x}$ is a $\mathbb{Z}_p$-basis element of $\bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}}$, then there is an equality of lattices

$$\mathbb{Z}_p \cdot \eta_{\boldsymbol{x}}^{\mathrm{alg}} = \#H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \cdot \bigwedge_{\mathbb{Z}_p}^r H^1(\mathbb{Z}_S, T) \tag{2.5.2}$$

and hence $\eta_{\boldsymbol{x}}^{\mathrm{alg}}$ belongs to $\bigwedge_{\mathbb{Z}_p}^r H^1(\mathbb{Z}_S, T)$.

Upon combining this fact with Remark 2.18, one is led to formulate the following algebraic analogue of Conjecture 2.12.

Conjecture 2.19 (the refined Mazur–Tate conjecture). *Set $r := r_{\mathrm{alg}}$. Then for each $\mathbb{Z}_p$-basis element $\boldsymbol{x}$ of $\bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}}$ the image in $H^1(\mathcal{O}_{F,S}, T) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]/I_F^r$ of $\mathcal{N}_{F/\mathbb{Q}}({}_{c,d}z_F)$ is equal to $\iota_F\big(\mathrm{Boc}_{F,\boldsymbol{x}}({}_{c,d}\eta_{\boldsymbol{x}}^{\mathrm{alg}})\big)$.*

REMARK 2.20. We refer to this conjecture as a 'refined Mazur–Tate conjecture' since in the complementary article [**9**] it is proved (in general, modulo standard assumptions concerning the non-vanishing of p-adic regulators) that, under mild and natural hypotheses on E at p, the equality predicted by Conjecture 2.19 in the setting of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ (see Conjecture 4.15 below) implies the p-component of the congruences for modular elements that are conjectured by Mazur and Tate in [**29**]. This fact is in turn a key ingredient in the approach used in [**9**] to obtain the first (unconditional) theoretical evidence in support of the conjecture of Mazur and Tate for elliptic curves of strictly positive rank.

3. Fitting ideals and order of vanishing.

In this section we shall discuss a further arithmetic property of Kato's zeta elements and, in particular, use it to prove Theorem 1.3.

Throughout we fix F, G and I_F as in Section 2.3 and continue to assume that $H^1(\mathbb{Z}_S, T)$ is $\mathbb{Z}_p$-free. However, unless explicitly stated, in this subsection we do *not* need to assume either that $r_{\mathrm{alg}} > 0$ or that $Ш(E/\mathbb{Q})[p^\infty]$ is finite.

3.1. A 'main conjecture' at finite level.

We write m for the conductor of F and set

$$t_{c,d} := cd(c - \sigma_c)(d - \sigma_d) \in \mathbb{Z}_p[G],$$

where σ_a is the element of G obtained by restriction of the automorphism of $\mathbb{Q}(\mu_m)$ that sends ζ_m to ζ_m^a.

We then propose the following conjecture involving the initial Fitting ideal of the $\mathbb{Z}_p[G]$-module $H^2(\mathcal{O}_{F,S}, T)$.

CONJECTURE 3.1.

$$\big\{\Phi({}_{c,d}z_F) \mid \Phi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(H^1(\mathcal{O}_{F,S}, T), \mathbb{Z}_p[G])\big\} = t_{c,d} \cdot \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathcal{O}_{F,S}, T)).$$

REMARK 3.2. Conjecture 3.1 is analogous to the 'weak main conjecture' for modular elements that is formulated by Mazur and Tate [**29**, Conjecture 3]. (In fact, since our conjecture predicts an equality rather than simply an inclusion, it corresponds to a strengthening of [**29**, Conjecture 3]). It is also an analogue of the conjectures [**6**, Conjecture 7.3] and [**8**, Conjecture 3.6(ii)] that were formulated by the present authors in the setting of the multiplicative group.

The prediction in Conjecture 3.1 can be studied by using the equivariant theory of Euler systems developed by Sakamoto and the first and third authors in [**10**]. In this way, the following evidence for Conjecture 3.1 is obtained in [**10**, Theorem 6.11].

PROPOSITION 3.3. *Assume that the following conditions are all satisfied.*

(a) $p > 3$ (*see Remark* 1.4 *for* $p = 3$);

(b) $Ш(E/F)[p^\infty]$ *is finite*;

(c) *the image of the representation* $G_{\mathbb{Q}} \to \mathrm{Aut}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$ *contains* $\mathrm{SL}_2(\mathbb{Z}_p)$;

(d) $E(\mathbb{Q}_\ell)[p]$ *vanishes for all primes* ℓ *in* S.

Then for any homomorphism $\Phi : H^1(\mathcal{O}_{F,S}, T) \to \mathbb{Z}_p[G]$ *of* $\mathbb{Z}_p[G]$*-modules one has*

$$\Phi({}_{c,d}z_F) \in \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathcal{O}_{F,S}, T)).$$

3.2. The proof of Theorem 1.3.

In the rest of this section, we assume the conditions (a), (b), (c) and (d) in Theorem 1.3 (which are the same as those in Proposition 3.3). In particular, $E[p]$ is irreducible by (c), and we may assume $T = T_p(E)$.

3.2.1. The connection between Conjecture 3.1 and Conjecture 1.1(i) is explained by the following result.

Proposition 3.4. *Assume that* $E(F)[p]$ *vanishes and* $Ш(E/\mathbb{Q})[p^\infty]$ *is finite. Set* $a := \max\{0, r_{\mathrm{alg}} - 1\}$ *and define a* $\mathbb{Z}_p[G]$*-submodule of* I_F^a *by setting*

$$I_{F,S,a} := \#H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \cdot I_F^a + I_F^{a+1}.$$

Then $\mathcal{N}_{F/\mathbb{Q}}({}_{c,d}z_F)$ *belongs to* $H^1(\mathcal{O}_{F,S}, T) \otimes_{\mathbb{Z}_p} I_{F,S,a}$ *whenever one has*

$$\Phi({}_{c,d}z_F) \in \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathcal{O}_{F,S}, T)) \tag{3.2.1}$$

for all $\Phi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(H^1(\mathcal{O}_{F,S}, T), \mathbb{Z}_p[G])$.

Proof. Set $M := H^1(\mathcal{O}_{F,S}, T)$ and $J_{F,S} := \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathcal{O}_{F,S}, T))$.

Then there exists a canonical isomorphism of $\mathbb{Z}_p$-modules

$$\iota : \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p[G]}(M, \mathbb{Z}_p[G]);\ \varphi \mapsto \sum_{\sigma \in G} \varphi(\sigma(-))\sigma^{-1}.$$

Hence, for every $\phi \in \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$, one has

$$(\phi \otimes 1)(\mathcal{N}_{F/\mathbb{Q}}({}_{c,d}z_F)) = \iota(\phi)({}_{c,d}z_F) \in J_{F,S}. \tag{3.2.2}$$

Here $\phi \otimes 1$ denotes the map $M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G] \to \mathbb{Z}_p[G]$ induced naturally by ϕ so that the equality follows directly from a comparison of the definitions of $\mathcal{N}_{F/\mathbb{Q}}({}_{c,d}z_F)$ and ι, and the containment in $J_{F,S}$ is an immediate consequence of (3.2.1).

Since $E(F)[p]$ is assumed to vanish, the $\mathbb{Z}_p$-module M is free. We fix a basis $\{x_i\}_{1 \le i \le n}$ of M and write $\mathcal{N}_{F/\mathbb{Q}}({}_{c,d}z_F)$ as a sum

$$\mathcal{N}_{F/\mathbb{Q}}({}_{c,d}z_F) = \sum_{j=1}^{n} x_j \otimes t_j$$

with each $t_j \in \mathbb{Z}_p[G]$. Then, with $\{x_i^*\}_{1 \le i \le n}$ denoting the corresponding dual basis of $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$, for every i the containment (3.2.2) (with $\phi = x_i^*$) implies that

$$t_i = (x_i^* \otimes 1)\left(\sum_{j=1}^{n} x_j \otimes t_j\right) = (x_i^* \otimes 1)(\mathcal{N}_{F/\mathbb{Q}}({}_{c,d}z_F)) \in J_{F,S}$$

and hence also that $\mathcal{N}_{F/\mathbb{Q}}({}_{c,d}z_F) \in M \otimes_{\mathbb{Z}_p} J_{F,S}$.

To complete the proof it is therefore enough to prove an inclusion

$$J_{F,S} \subset I_{F,S,a}. \tag{3.2.3}$$

To do this we note that $H^i(\mathcal{O}_{F,S}, T)$ vanishes for all $i > 2$ and hence that the natural corestriction map $H^2(\mathcal{O}_{F,S}, T) \twoheadrightarrow H^2(\mathbb{Z}_S, T)$ is surjective.

In addition, since $Ш(E/\mathbb{Q})[p^\infty]$ is assumed to be finite, the $\mathbb{Z}_p$-rank of $H^2(\mathbb{Z}_S, T)$ is equal to a and so the $\mathbb{Z}_p$-module $H^2(\mathbb{Z}_S, T)$ is isomorphic to $H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \oplus \mathbb{Z}_p^a$.

The corestriction map therefore induces a surjective homomorphism of $\mathbb{Z}_p[G]$-modules

$$H^2(\mathcal{O}_{F,S}, T) \twoheadrightarrow H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \oplus \mathbb{Z}_p^a$$

and hence an inclusion of Fitting ideals

$$\begin{aligned} J_{F,S} &= \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathcal{O}_{F,S}, T)) \\ &\subset \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}\big(H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \oplus \mathbb{Z}_p^a\big) = \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathbb{Z}_S, T)_{\mathrm{tors}}) \cdot I_F^a. \end{aligned}$$

To deduce (3.2.3) from this it is thus enough to note the image of $\mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathbb{Z}_S, T)_{\mathrm{tors}})$ under the natural map $\mathbb{Z}_p[G] \to \mathbb{Z}_p[G]/I_F \simeq \mathbb{Z}_p$ is equal to

$$\mathrm{Fitt}^0_{\mathbb{Z}_p}\big((H^2(\mathbb{Z}_S, T)_{\mathrm{tors}})_G\big) = \mathrm{Fitt}^0_{\mathbb{Z}_p}(H^2(\mathbb{Z}_S, T)_{\mathrm{tors}}) = \#H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \cdot \mathbb{Z}_p. \qquad \square$$

REMARK 3.5. The above argument also shows the validity of the containment (3.2.1) would imply that

$$\Phi({}_{c,d}z_F) \in I_F^a \text{ for every } \Phi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}\big(H^1(\mathcal{O}_{F,S}, T), \mathbb{Z}_p[G]\big). \tag{3.2.4}$$

This prediction constitutes an analogue for Kato's Euler system ${}_{c,d}z_F$ of the 'weak vanishing' conjecture for modular elements that is formulated by Mazur and Tate in [**29**, Conjecture 1].

3.2.2. If the algebraic rank $r := r_{\mathrm{alg}}$ of E over $\mathbb{Q}$ is strictly positive, then the integer a in Proposition 3.4 is equal to $r - 1$ and so one has $I_F^a = I_F^{r-1}$.

One therefore obtains a proof of Theorem 1.3 directly upon combining the results of Propositions 3.3 and 3.4.

4. Derivatives of Kato's Euler system.

In this section, we shall define a canonical 'Darmon derivative' ${}_{c,d}\kappa_F$ of Kato's zeta element ${}_{c,d}z_F$ and use it to reinterpret the conjectures formulated above.

In particular, in this way we are able to formulate more explicit versions of the Conjectures 2.12 and 2.19 for subfields F of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Throughout this section, we assume that $H^1(\mathbb{Z}_S, T)$ is $\mathbb{Z}_p$-free and $Ш(E/\mathbb{Q})[p^\infty]$ is finite.

4.1. Darmon derivatives.

We use the notations in Section 2.3.

4.1.1. We shall use the fact that the complex

$$C_F := \mathsf{R}\,\mathrm{Hom}_{\mathbb{Z}_p}\big(\mathsf{R}\Gamma_c(\mathcal{O}_{F,S}, T^*(1)), \mathbb{Z}_p[-2]\big)$$

is a perfect complex of $\mathbb{Z}_p[G]$-modules that is acyclic outside degrees zero and one, and that there exists a canonical isomorphism

$$H^0(C_F) \simeq H^1(\mathcal{O}_{F,S}, T) \tag{4.1.1}$$

and a canonical exact sequence

$$0 \to H^2(\mathcal{O}_{F,S}, T) \to H^1(C_F) \to \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p} T^*(1)^{+,*} \to 0. \tag{4.1.2}$$

(See [**11**, Proposition 2.22].)

In particular, by [**11**, Proposition A.11(i)], one finds that C_F is represented by a complex of the form $P_F \to P_F$, where P_F is a finitely generated free $\mathbb{Z}_p[G]$-module and the first term is placed in degree zero.

In this way we obtain an exact sequence of $\mathbb{Z}_p[G]$-modules

$$0 \to H^1(\mathcal{O}_{F,S}, T) \to P_F \xrightarrow{f_F} P_F \to H^1(C_F) \to 0. \tag{4.1.3}$$

Then (2.3.1) implies that $C_\mathbb{Q}$ is represented by the complex $P_\mathbb{Q} \xrightarrow{f_\mathbb{Q}} P_\mathbb{Q}$ obtained by taking G-invariants of the complex $P_F \xrightarrow{f_F} P_F$ and hence that there is an exact sequence

$$0 \to H^1(\mathbb{Z}_S, T) \to P_\mathbb{Q} \xrightarrow{f_\mathbb{Q}} P_\mathbb{Q} \to H^1(C_\mathbb{Q}) \to 0. \tag{4.1.4}$$

We use this sequence to regard $H^1(\mathbb{Z}_S, T)$ as a submodule of $P_\mathbb{Q}$. We also note that, just as in (2.4.2), there are natural injective homomorphisms

$$\iota_F : P_\mathbb{Q} \otimes_{\mathbb{Z}_p} Q_F^a \hookrightarrow P_F \otimes_{\mathbb{Z}_p} Q_F^a \hookrightarrow P_F \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]/I_F^{a+1}$$

(where, we recall, Q_F^a denotes I_F^a/I_F^{a+1}).

DEFINITION 4.1. Set $a := \max\{0, r_{\mathrm{alg}} - 1\}$ and assume that the containment (3.2.4) is valid for all Φ in $\mathrm{Hom}_{\mathbb{Z}_p[G]}(H^1(\mathcal{O}_{F,S}, T), \mathbb{Z}_p[G])$. Then [**6**, Proposition 4.17] implies the existence of a unique element ${}_{c,d}\kappa_F$ of $P_\mathbb{Q} \otimes_{\mathbb{Z}_p} Q_F^a$ with the property that

$$\iota_F({}_{c,d}\kappa_F) = \mathcal{N}_{F/\mathbb{Q}}({}_{c,d}z_F)$$

in $P_F \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]/I_F^{a+1}$. We shall refer to ${}_{c,d}\kappa_F$ as the *Darmon derivative* of ${}_{c,d}z_F$.

4.1.2. Conjecture 2.12 predicts that the element ${}_{c,d}\kappa_F$ belongs to the image of the (injective) homomorphism

$$H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} Q_F^a \to P_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} Q_F^a. \tag{4.1.5}$$

At this stage, however, we can only verify this prediction in certain special cases.

In the next section we shall verify that it is valid if F is contained in the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$. In the following result we record some evidence in the general case.

Before stating the result we note that the condition

$$\Phi({}_{c,d}z_F) \in \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathcal{O}_{F,S}, T)) \text{ for every } \Phi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}\big(H^1(\mathcal{O}_{F,S}, T), \mathbb{Z}_p[G]\big)$$

is valid whenever the data E, F, S and p satisfy the conditions (a), (b), (c) and (d) of Proposition 3.3 and that, in general, its validity would follow from that of Conjecture 3.1.

We further note that claim (ii) of the following result constitutes a natural analogue for zeta elements of one of the main results of Darmon in [**15**, Theorem 2.5] concerning Heegner points.

THEOREM 4.2. *Set $z := {}_{c,d}z_F$ and $\kappa := {}_{c,d}\kappa_F$. If one has $\Phi(z) \in \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathcal{O}_{F,S}, T))$ for every Φ in $\mathrm{Hom}_{\mathbb{Z}_p[G]}(H^1(\mathcal{O}_{F,S}, T), \mathbb{Z}_p[G])$, then the following claims are valid.*

(i) *If p^N is the minimum of the exponents of the groups $\#H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \cdot Q_F^a$ and $H^2(\mathbb{Z}_S, T)_{\mathrm{tors}}$, then $p^N \cdot \kappa$ belongs to the image of the map* (4.1.5).

(ii) *The image of κ under the natural map*

$$P_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} Q_F^a \to P_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} Q_F^a \otimes_{\mathbb{Z}} \mathbb{Z}/(p)$$

belongs to the image of the map

$$H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} Q_F^a \otimes_{\mathbb{Z}} \mathbb{Z}/(p) \to P_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} Q_F^a \otimes_{\mathbb{Z}} \mathbb{Z}/(p)$$

induced by (4.1.5).

PROOF. Set $\widetilde{Q}_F^a := \#H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \cdot Q_F^a \subset \mathbb{Z}_p[G]/I_F^{a+1}$. Then the sequences (4.1.3) and (4.1.4) combine to give a commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1(\mathcal{O}_{F,S}, T) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]/I_F^{a+1} & \longrightarrow & P_F \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]/I_F^{a+1} & \xrightarrow{\tilde{f}_F} & P_F \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]/I_F^{a+1} \\
 & & \uparrow{\scriptstyle \tilde{\iota}_F} & & \uparrow{\scriptstyle \tilde{\iota}_F} & & \uparrow{\scriptstyle \tilde{\iota}_F} \\
0 & \longrightarrow & H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} \widetilde{Q}_F^a & \longrightarrow & P_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} \widetilde{Q}_F^a & \xrightarrow{\tilde{f}_{\mathbb{Q}}} & P_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} \widetilde{Q}_F^a
\end{array}$$

in which the maps $\tilde{\iota}_F$ are obtained by restricting ι_F.

Then the argument of Proposition 3.4 implies that

$$\kappa \in P_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} \widetilde{Q}_F^a \subset P_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} Q_F^a, \tag{4.1.6}$$

and so the commutativity of this diagram implies that

$$\tilde{\iota}_F(\tilde{f}_{\mathbb{Q}}(\kappa)) = \tilde{f}_F(\tilde{\iota}_F(\kappa)) = \tilde{f}_F(\mathcal{N}_{F/\mathbb{Q}}(z)) = 0$$

and hence, since $\tilde{\iota}_F$ is injective, that $\tilde{f}_{\mathbb{Q}}(\kappa) = 0$.

Now, the exact sequence (4.1.4) induces exact sequences

$$0 \to H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} \widetilde{Q}_F^a \to P_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} \widetilde{Q}_F^a \xrightarrow{\mu_1} \mathrm{im}(f_{\mathbb{Q}}) \otimes_{\mathbb{Z}_p} \widetilde{Q}_F^a \to 0$$

and

$$0 \to \mathrm{Tor}_1^{\mathbb{Z}_p}\big(H^2(\mathbb{Z}_S, T)_{\mathrm{tors}}, \widetilde{Q}_F^a\big) \xrightarrow{\mu_2} \mathrm{im}(f_{\mathbb{Q}}) \otimes_{\mathbb{Z}_p} \widetilde{Q}_F^a \xrightarrow{\mu_3} P_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} \widetilde{Q}_F^a$$

with the property that $\mu_3 \circ \mu_1$ is equal to $\tilde{f}_{\mathbb{Q}}$. (The first sequence here is exact since the $\mathbb{Z}_p$-module $\mathrm{im}(f_{\mathbb{Q}})$ is free and the second is exact as consequence of the fact that (4.1.2) identifies $H^2(\mathbb{Z}_S, T)_{\mathrm{tors}}$ with $H^1(C_{\mathbb{Q}})_{\mathrm{tors}}$.)

These sequences combine with the equality $\tilde{f}_{\mathbb{Q}}(\kappa) = 0$ to imply $\mu_1(\kappa)$ belongs to the image of μ_2 in the lower sequence above.

Thus, since the definition of p^N ensures it annihilates the group $\mathrm{Tor}_1^{\mathbb{Z}_p}\big(H^2(\mathbb{Z}_S, T)_{\mathrm{tors}}, \widetilde{Q}_F^a\big)$, it follows that $\mu_1(p^N \cdot \kappa)$ vanishes, and hence that $p^N \cdot \kappa$ belongs to $H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} \widetilde{Q}_F^a \subset H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} Q_F^a$. This proves claim (i).

Turning to claim (ii), we note first that if $H^2(\mathbb{Z}_S, T)_{\mathrm{tors}}$ is trivial, then claim (i) implies κ belongs to the image of the map (4.1.5) and so claim (ii) follows immediately.

On the other hand, if $H^2(\mathbb{Z}_S, T)_{\mathrm{tors}}$ is non-trivial, then $\widetilde{Q}_F^a$ is contained in $p \cdot Q_F^a$ and so (4.1.6) implies that the projection of κ to $P_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} Q_F^a \otimes \mathbb{Z}/(p)$ vanishes. In this case, therefore, the result of claim (ii) is also clear. □

Remark 4.3. If G has exponent p and $r_{\mathrm{alg}} > 0$, then $a > 0$ and so Q_F^a is annihilated by p. In any such case, therefore, Theorem 4.2(ii) implies (under the stated hypotheses) that κ belongs to the image of the map (4.1.5). In general, the argument of Theorem 4.2 shows that the group $H^2(\mathbb{Z}_S, T)_{\mathrm{tors}}$ constitutes the obstruction to attempts to deduce this containment from Euler system arguments (via the result of Proposition 3.3). To describe this obstruction more explicitly we assume that $E[p]$ is an irreducible $G_{\mathbb{Q}}$-representation. In this case, one can assume $T = T_p(E)$ and then one sees that the obstruction $H^2(\mathbb{Z}_S, T)_{\mathrm{tors}}$ sits in the exact sequence

$$E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \bigoplus_{\ell \in S \setminus \{\infty\}} \varprojlim_n E(\mathbb{Q}_\ell)/p^n \to \big(H^2(\mathbb{Z}_S, T)_{\mathrm{tors}}\big)^\vee \to Ш(E/\mathbb{Q})[p^\infty] \to 0$$

obtained from global duality, in which the first arrow denotes the natural diagonal map.

4.2. Iwasawa–Darmon derivatives.

To consider the above constructions in an Iwasawa-theoretic setting we shall use the following notations for non-negative integers n and i:

- $\mathbb{Q}_n$: the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$ (i.e., the subfield of $\mathbb{Q}_\infty$ such that $[\mathbb{Q}_n : \mathbb{Q}] = p^n$),

- $G_n := \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$,
- $I_n := \ker(\mathbb{Z}_p[G_n] \twoheadrightarrow \mathbb{Z}_p)$,
- $Q_n^a := I_n^a/I_n^{a+1}$ with $a := \max\{0, r_{\mathrm{alg}} - 1\}$ as above,
- $H_n^i := H^i(\mathcal{O}_{\mathbb{Q}_n,S}, T)$,
- ${}_{c,d}z_n := {}_{c,d}z_{\mathbb{Q}_n}$,
- $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$,
- $\Lambda := \mathbb{Z}_p[[\Gamma]]$,
- $I := \ker(\mathbb{Z}_p[[\Gamma]] \twoheadrightarrow \mathbb{Z}_p)$,
- $Q^a = I^a/I^{a+1}$,
- $\mathbb{H}^i := \varprojlim_n H_n^i$.

4.2.1. We first verify the prediction (3.2.4) in this setting.

Proposition 4.4. *For any non-negative integer n, the element ${}_{c,d}z_n$ belongs to $I_n^a \cdot H_n^1$.*

In particular, the weak vanishing order prediction of (3.2.4) *holds for the field $F = \mathbb{Q}_n$ for every n.*

Proof. We use Kato's result on the Iwasawa main conjecture [**23**, Section 12]. By [**23**, Theorem 12.4(2)], we know that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{H}^1$ is a free $\mathbb{Q} \otimes_{\mathbb{Z}} \Lambda$-module of rank one. This together with the injectivity of $\mathbb{H}^1/I\mathbb{H}^1 \to H^1(\mathbb{Z}_S, T)$ and the assumption that $H^1(\mathbb{Z}_S, T)$ is $\mathbb{Z}_p$-free implies that $\mathbb{H}^1$ is a free Λ-module of rank one. Since

$$\mathbb{H}^2 \twoheadrightarrow H^2(\mathbb{Z}_S, T)_{\mathrm{tf}} \simeq \mathbb{Z}_p^a$$

is surjective, the characteristic ideal of $\mathbb{H}^2$ is in I^a. Therefore, the characteristic ideal of $\mathbb{H}^1/\langle {}_{c,d}z_\infty \rangle$ is also in it by [**23**, Theorem 12.5(3)], where ${}_{c,d}z_\infty := ({}_{c,d}z_n)_n$ (note that $({}_{c,d}z_n)_n$ is in the inverse limit $\varprojlim_n H_n^1 = \mathbb{H}^1$). This shows that

$${}_{c,d}z_\infty \in I^a \cdot \mathbb{H}^1,$$

which implies the conclusion of Proposition 4.4. □

By using Proposition 4.4, we can now explicitly construct the Darmon derivative of ${}_{c,d}z_n$. To do this we fix a topological generator γ of Γ and denote the image of γ in G_n by the same symbol. In view of Proposition 4.4 one has

$${}_{c,d}z_n = (\gamma - 1)^a w_n$$

for some choice of element w_n of H_n^1.

We then compute

$$\begin{aligned}\mathcal{N}_{\mathbb{Q}_n/\mathbb{Q}}({}_{c,d}z_n) &= \sum_{\sigma\in G_n} \sigma({}_{c,d}z_n)\otimes\sigma^{-1}\\ &= \sum_{\sigma\in G_n} \sigma(\gamma-1)^a w_n\otimes\sigma^{-1}\\ &= \sum_{\sigma\in G_n} \sigma w_n\otimes\sigma^{-1}(\gamma-1)^a \in H^1_n\otimes_{\mathbb{Z}_p} I_n^a.\end{aligned}$$

Thus, in $H^1_n\otimes_{\mathbb{Z}_p} Q_n^a$, we have

$$\mathcal{N}_{\mathbb{Q}_n/\mathbb{Q}}({}_{c,d}z_n) = \sum_{\sigma\in G_n}\sigma w_n\otimes(\gamma-1)^a.$$

Hence, the derivative in Definition 4.1 is explicitly given by

$${}_{c,d}\kappa_n := \mathrm{Cor}_{\mathbb{Q}_n/\mathbb{Q}}(w_n)\otimes(\gamma-1)^a \in H^1_0\otimes_{\mathbb{Z}_p} Q_n^a. \tag{4.2.1}$$

One easily sees that this element is well-defined, i.e., independent of the choice of w_n. Furthermore, the collection $({}_{c,d}\kappa_n)_n$ is an inverse system, so we can give the following definition.

Definition 4.5. We define the *Iwasawa–Darmon derivative* of Kato's Euler system by

$${}_{c,d}\kappa_\infty := ({}_{c,d}\kappa_n)_n \in \varprojlim_n H^1_0\otimes_{\mathbb{Z}_p} Q_n^a = H^1(\mathbb{Z}_S,T)\otimes_{\mathbb{Z}_p} Q^a.$$

We also define the normalized version

$$\kappa_\infty := \frac{1}{cd(c-1)(d-1)}\cdot {}_{c,d}\kappa_\infty \in H^1(\mathbb{Z}_S,V)\otimes_{\mathbb{Z}_p} Q^a.$$

Remark 4.6. The Iwasawa–Darmon derivative can be regarded as a natural analogue of the 'cyclotomic p-units' that are defined by Solomon in [**43**] in the setting of the classical cyclotomic unit Euler system. In a more general setting, it is an analogue of the derivative κ of the (conjectural) Rubin–Stark Euler system that occurs in [**7**, Conjecture 4.2].

Remark 4.7. If r_{alg} is at most one, then $a=0$, $Q^a=\mathbb{Z}_p$ and in $H^1(\mathbb{Z}_S,V)$ one has

$$\kappa_\infty = z_{\mathbb{Q}} := \frac{1}{cd(c-1)(d-1)}\cdot {}_{c,d}z_{\mathbb{Q}}$$

so that Definition 4.5 gives nothing new in this case.

4.3. The Generalized Perrin-Riou Conjecture at infinite level.

In this section we assume Hypothesis 2.2 in order to state an Iwasawa-theoretic version of Conjecture 2.12. We set $r := r_{\mathrm{alg}}$.

4.3.1. To do this we fix a $\mathbb{Z}_p$-basis $\boldsymbol{x}$ of $\bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}}$ and write

$$\mathrm{Boc}_{n,\boldsymbol{x}} = \mathrm{Boc}_{\mathbb{Q}_n,\boldsymbol{x}} : \bigwedge_{\mathbb{Z}_p}^{r} H^1(\mathbb{Z}_S, T) \to H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} I_n^{r-1}/I_n^r$$

for the Bockstein regulator map (2.3.3) for the field $\mathbb{Q}_n$, as defined in Section 2.3.

As n varies these maps combine to induce a homomorphism

$$\varprojlim_n \mathrm{Boc}_{n,\boldsymbol{x}} : \bigwedge_{\mathbb{Z}_p}^{r} H^1(\mathbb{Z}_S, T) \to H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} \varprojlim_n I_n^{r-1}/I_n^r = H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} Q^{r-1}$$

and hence also, by scalar extension, a homomorphism

$$\mathrm{Boc}_{\infty,\boldsymbol{x}} : \mathbb{C}_p \otimes_{\mathbb{Z}_p} \bigwedge_{\mathbb{Z}_p}^{r} H^1(\mathbb{Z}_S, T) \to \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} Q^{r-1}. \tag{4.3.1}$$

We recall from Definition 2.4 the Birch and Swinnerton-Dyer element $\eta_{\boldsymbol{x}}^{\mathrm{BSD}}$ that is constructed (unconditionally) in the space $\mathbb{C}_p \otimes_{\mathbb{Z}_p} \bigwedge_{\mathbb{Z}_p}^{r} H^1(\mathbb{Z}_S, T)$.

Conjecture 4.8. *One has*

$$\kappa_\infty = \mathrm{Boc}_{\infty,\boldsymbol{x}}\big(\eta_{\boldsymbol{x}}^{\mathrm{BSD}}\big)$$

in $\mathbb{C}_p \otimes_{\mathbb{Z}_p} H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} Q^{r-1}$.

Remark 4.9. In contrast to the more general situation considered in Conjecture 2.12 we do not here need to assume $\eta_{\boldsymbol{x}}^{\mathrm{BSD}}$ belongs to $\bigwedge_{\mathbb{Z}_p}^{r} H^1(\mathbb{Z}_S, T)$. This is because the group Q^{r-1} is $\mathbb{Z}_p$-torsion-free and so one loses no information by defining the Bockstein homomorphism $\mathrm{Boc}_{\infty,\boldsymbol{x}}$ on $\mathbb{C}_p$-modules. In particular, if $r = 1$, then the discussion of Remark 2.13 shows that Conjecture 4.8 is equivalent to Perrin-Riou's original conjecture. Finally, we observe that Conjecture 4.8 is a natural analogue for elliptic curves of the conjecture formulated for the multiplicative group in [**7**, Conjecture 4.2].

4.3.2. We shall now give an explicit interpretation of Conjecture 4.8 in terms of the leading term $L_S^*(E, 1)$ (see Proposition 4.14 below).

Take a $\mathbb{Z}$-basis $\{x_1, \dots, x_r\}$ of $E(\mathbb{Q})_{\mathrm{tf}}$. We define an element $\boldsymbol{x} \in \bigwedge_{\mathbb{Q}_p}^{r-1} H^2(\mathbb{Z}_S, V)$ as the element corresponding to

$$1 \otimes x_1 \otimes (x_1^* \wedge \cdots \wedge x_r^*) \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Big(E_1(\mathbb{Q}_p) \otimes_{\mathbb{Z}} \bigwedge_{\mathbb{Z}}^{r} E(\mathbb{Q})^*\Big)$$

under the isomorphism

$$\bigwedge_{\mathbb{Q}_p}^{r-1} H^2(\mathbb{Z}_S, V) \simeq \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Big(E_1(\mathbb{Q}_p) \otimes_{\mathbb{Z}} \bigwedge_{\mathbb{Z}}^{r} E(\mathbb{Q})^*\Big)$$

induced by (2.2.2). (Here we regard $1 \otimes x_1 \in \mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})$ as an element of $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} E_1(\mathbb{Q}_p)$.) We note that, by linearity, the definition of the Bockstein regulator map (4.3.1) is extended for any element in $\bigwedge_{\mathbb{Q}_p}^{r-1} H^2(\mathbb{Z}_S, V)$, which is not necessarily a $\mathbb{Z}_p$-basis of $\bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}}$. Thus $\mathrm{Boc}_{\infty,\boldsymbol{x}}$ is defined for above $\boldsymbol{x}$.

Let ω be the fixed Néron differential and $\log_\omega : E(\mathbb{Q}) \to E(\mathbb{Q}_p) \to \mathbb{Q}_p$ the formal logarithm associated to ω. We give the following definition.

Definition 4.10. We define the *Bockstein regulator* associated to ω by setting

$$R_\omega^{\mathrm{Boc}} := \log_\omega(x_1) \cdot \mathrm{Boc}_{\infty,\boldsymbol{x}}(x_1 \wedge \cdots \wedge x_r) \in (\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})) \otimes_{\mathbb{Z}_p} Q^{r-1}.$$

(Here we identify $H^1(\mathbb{Z}_S, V) = \mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})$ by (2.2.1).) One can check that this does not depend on the choice of the basis $\{x_1, \dots, x_r\}$ of $E(\mathbb{Q})_{\mathrm{tf}}$.

Remark 4.11. The Bockstein regulator defined above is closely related to the classical p-adic regulators: for details, see Theorems 5.6 and 5.11 below.

Remark 4.12. When $r = 1$, then $\mathrm{Boc}_{\infty,\boldsymbol{x}}$ is the identity map and one has

$$R_\omega^{\mathrm{Boc}} = \log_\omega(x) \cdot x \in \mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})$$

for any generator x of $E(\mathbb{Q})_{\mathrm{tf}}$.

Remark 4.13. Let Ω_ξ be as in (2.1.4) and R_∞ the Néron–Tate regulator. Then one can check that

$$\mathrm{Boc}_{\infty,\boldsymbol{x}}\big(\eta_{\boldsymbol{x}}^{\mathrm{BSD}}\big) = \frac{L_S^*(E,1)}{\Omega_\xi \cdot R_\infty} \cdot R_\omega^{\mathrm{Boc}}.$$

In fact, by the definition of the Birch and Swinnerton-Dyer element, one checks that

$$\eta_{\boldsymbol{x}}^{\mathrm{BSD}} = \frac{L_S^*(E,1)}{\Omega_\xi \cdot R_\infty} \cdot \log_\omega(x_1) \cdot x_1 \wedge \cdots \wedge x_r. \tag{4.3.2}$$

By Remark 4.13, we obtain the following interpretation of Conjecture 4.8.

Proposition 4.14. *Conjecture* 4.8 *is valid if and only if one has*

$$\kappa_\infty = \frac{L_S^*(E,1)}{\Omega_\xi \cdot R_\infty} \cdot R_\omega^{\mathrm{Boc}}$$

in $\mathbb{C}_p \otimes_{\mathbb{Z}_p} H^1(\mathbb{Z}_S, T) \otimes_{\mathbb{Z}_p} Q^{r-1} \simeq (\mathbb{C}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})) \otimes_{\mathbb{Z}_p} Q^{r-1}$.

4.3.3. Using Proposition 4.14 we state an Iwasawa-theoretic version of the 'algebraic' variant Conjecture 2.19 of Conjecture 2.12. This conjecture is therefore a natural 'algebraic' variant of Conjecture 4.8.

We recall that L_ℓ denotes the Euler factor at a prime ℓ so that one has

$$\left(\prod_{\ell \in S \setminus \{\infty\}} L_\ell\right) \cdot L^*(E,1) = L_S^*(E,1).$$

We also write v_ξ for the non-zero rational number that is defined by the equality

$$\Omega^+ = v_\xi \cdot \Omega_\xi \tag{4.3.3}$$

where Ω^+ is the real Néron period that occurs in (2.5.1).

CONJECTURE 4.15. *If* $Ш(E/\mathbb{Q})$ *is finite, then in* $(\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})) \otimes_{\mathbb{Z}_p} Q^{r-1}$ *one has*

$$\kappa_\infty = v_\xi \left(\prod_{\ell \in S \setminus \{\infty\}} L_\ell \right) \frac{\#Ш(E/\mathbb{Q}) \cdot \mathrm{Tam}(E)}{\#E(\mathbb{Q})^2_{\mathrm{tors}}} \cdot R_\omega^{\mathrm{Boc}}.$$

REMARK 4.16. One checks easily that Conjecture 4.15 is equivalent to an equality

$$\kappa_\infty = \mathrm{Boc}_{\infty,\boldsymbol{x}}\big(\eta_{\boldsymbol{x}}^{\mathrm{alg}}\big),$$

where $\boldsymbol{x}$ is any non-zero element of $\bigwedge_{\mathbb{Q}_p}^{r-1} H^2(\mathbb{Z}_S, V)$ and $\eta_{\boldsymbol{x}}^{\mathrm{alg}}$ is the algebraic Birch and Swinnerton-Dyer element that is defined (unconditionally) in Definition 2.17.

REMARK 4.17. In Corollary 6.6 below we will show that Conjecture 4.15 is a refinement of the p-adic Birch and Swinnerton-Dyer formula (from [**30**, Chapter II, Section 10]). Similarly, in Corollary 6.7 we will show that Conjecture 4.8 leads to an explicit formula for the leading term of the p-adic L-function (which we will refer to as a 'p-adic Beilinson formula').

A key advantage of the formulations of Conjectures 4.8 and 4.15 is that they do not involve the p-adic L-function and so are not in principle dependent on the precise reduction type of E at p. In particular, the conjectures make sense (and are canonical) even when E has additive reduction at p.

5. *p*-adic height pairings and the Bockstein regulator.

In this section, as an important preliminary to the proofs of Theorem 1.9 and Corollaries 1.11 and 1.12, we shall make an explicit comparison of the Bockstein regulator R_ω^{Boc} defined in Definition 4.10 with the various notions of classical p-adic regulator (see Theorems 5.6 and 5.11 below).

In the following, we say 'p is $-$' if E has $-$ reduction at p. For example, 'p is good ordinary' means that E has good ordinary reduction at p.

In this section, we assume that E does not have additive reduction at p.

We shall use the same notations as in Sections 2 and 4.

5.1. Review of *p*-adic height pairings.

In this section, we give a review of the construction of p-adic height pairing using Selmer complexes.

5.1.1. The ordinary case. Suppose first that p is ordinary, i.e., good ordinary or multiplicative. In this case we follow Nekovář's construction of a p-adic height pairing in [**32**, Section 11]. (It is possible to treat this case in a more general context in Section 5.1.2 below, but it requires the theory of (φ, Γ)-modules.)

We recall the definition of Nekovář's Selmer complex.

To do this we note that, since p is ordinary, we have a canonical filtration $F^+V \subset V$ of $G_{\mathbb{Q}_p}$-modules (due to Greenberg, see [**19**]).

We set $F^+T := T \cap F^+V$. For any non-negative integer n, we also denote the unique p-adic place of $\mathbb{Q}_n$ by $\mathfrak{p}$.

Then, following the exact triangle given in (the third row of) [**32**, (6.1.3.2)], we define the Selmer complex of T by setting

$$\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q}_n, T) := \mathrm{Cone}\left(\mathsf{R}\Gamma(\mathcal{O}_{\mathbb{Q}_n,S}, T) \to \mathsf{R}\Gamma(\mathbb{Q}_{n,\mathfrak{p}}, T/F^+T) \oplus \bigoplus_{v \in S_{\mathbb{Q}_n} \setminus \{\mathfrak{p}\}} \mathsf{R}\Gamma_{/f}(\mathbb{Q}_{n,v}, T)\right)[-1].$$

(The local conditions are as in [**32**, (7.8.2)].)

We set

$$\widetilde{H}^i_f(\mathbb{Q}_n, T) := H^i(\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q}_n, T)) \quad \text{and} \quad \widetilde{H}^i_f(\mathbb{Q}_n, V) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \widetilde{H}^i_f(\mathbb{Q}_n, T).$$

We have a natural isomorphism

$$\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q}_n, T) \otimes^{\mathsf{L}}_{\mathbb{Z}_p[G_n]} \mathbb{Z}_p \simeq \widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q}, T)$$

(see [**32**, Proposition 8.10.1] or [**17**, Proposition 1.6.5(3)]), and so we can define (-1)-times the Bockstein map

$$\widetilde{H}^1_f(\mathbb{Q}, T) \to \widetilde{H}^2_f(\mathbb{Q}, T) \otimes_{\mathbb{Z}_p} I_n/I_n^2$$

associated to the complex $\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q}_n, T)$ (in the same way as (2.3.2)). Taking $\varprojlim_n$ and $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} -$, we obtain a map

$$\widetilde{\beta} : \widetilde{H}^1_f(\mathbb{Q}, V) \to \widetilde{H}^2_f(\mathbb{Q}, V) \otimes_{\mathbb{Z}_p} I/I^2. \tag{5.1.1}$$

Combining this map with the global duality map

$$\widetilde{H}^2_f(\mathbb{Q}, V) \to \widetilde{H}^1_f(\mathbb{Q}, V)^*$$

(see [**32**, Section 6.3]), we obtain a pairing

$$\langle -, - \rangle_p : \widetilde{H}^1_f(\mathbb{Q}, V) \times \widetilde{H}^1_f(\mathbb{Q}, V) \to \mathbb{Q}_p \otimes_{\mathbb{Z}_p} I/I^2.$$

Noting that there is a natural embedding $\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q}) \hookrightarrow \widetilde{H}^1_f(\mathbb{Q}, V)$ (see Remark 5.1 below), we obtain the p-adic height pairing

$$\langle -, - \rangle_p : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{Q}_p \otimes_{\mathbb{Z}_p} I/I^2.$$

REMARK 5.1. If p is good ordinary or non-split multiplicative, then $\widetilde{H}^1_f(\mathbb{Q}, V)$ coincides with the usual Selmer group $H^1_f(\mathbb{Q}, V)$ (see [**32**, Section 0.10]). If p is split multiplicative, then we have a canonical decomposition

$$\widetilde{H}^1_f(\mathbb{Q}, V) \simeq H^1_f(\mathbb{Q}, V) \oplus \mathbb{Q}_p$$

(see [**32**, Section 11.4.2]). In any case, we have a canonical embedding $\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q}) \hookrightarrow \widetilde{H}^1_f(\mathbb{Q}, V)$.

REMARK 5.2. For comparisons of the above p-adic height pairing with the classical ones, see [**32**, Sections 11.3 and 11.4].

5.1.2. The supersingular case. Suppose that p is good supersingular. In this case we follow the construction of the p-adic height pairing due to Benois [**2**]. His construction uses Selmer complexes associated to (φ,Γ)-modules, which was studied by Pottharst [**35**]. See also the review in [**3**].

We fix one of the roots $\alpha \in \overline{\mathbb{Q}}_p$ of the polynomial $X^2 - a_p X + p$. We set

$$L := \mathbb{Q}_p(\alpha).$$

We also set

$$V_L := L \otimes_{\mathbb{Q}_p} V \quad \text{and} \quad D_L := D_{\mathrm{crys}}(V_L) = D_{\mathrm{dR}}(V_L) \simeq L \otimes_{\mathbb{Q}} H^1_{\mathrm{dR}}(E/\mathbb{Q}),$$

which is endowed with an action of the Frobenius operator φ and also a natural decreasing filtration $\{D_L^i\}_{i\in\mathbb{Z}}$ such that $D_L^0 \simeq L \otimes_{\mathbb{Q}} \Gamma(E, \Omega^1_{E/\mathbb{Q}})$. We set

$$t_{V,L} := D_L/D_L^0 \simeq L \otimes_{\mathbb{Q}} \mathrm{Lie}(E).$$

Let N_α be the subspace of D_L on which φ acts via αp^{-1}. Explicitly, N_α is the subspace generated by $\varphi(\omega) - \alpha^{-1}\omega \in D_L$. Then the natural projection $D_L \twoheadrightarrow D_L/D_L^0 = t_{V,L}$ induces an isomorphism

$$N_\alpha \xrightarrow{\sim} t_{V,L}. \tag{5.1.2}$$

A subspace of D_L with this property is called a 'splitting submodule' in [**2**, Section 4.1.1].

We shall define a p-adic height pairing

$$\langle -,-\rangle_p = \langle -,-\rangle_{p,\alpha} : E(\mathbb{Q}) \times E(\mathbb{Q}) \to L \otimes_{\mathbb{Z}_p} I/I^2.$$

Since there is a natural embedding $\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q}) \hookrightarrow H^1_f(\mathbb{Q}, V)$, it is sufficient to construct a pairing

$$\langle -,-\rangle_p : H^1_f(\mathbb{Q}, V) \times H^1_f(\mathbb{Q}, V) \to L \otimes_{\mathbb{Z}_p} I/I^2.$$

We recall some basic facts from the theory of (φ,Γ)-modules. Let $\mathbb{D}^\dagger_{\mathrm{rig}}(V_L)$ denote the $(\varphi,\Gamma_{\mathbb{Q}_p})$-module associated V_L (where $\Gamma_{\mathbb{Q}_p} := \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$). (See [**2**, Theorem 2.1.3].) By [**2**, Theorem 2.2.3], there is a submodule $\mathbb{D}_\alpha \subset \mathbb{D}^\dagger_{\mathrm{rig}}(V_L)$ corresponding to $N_\alpha \subset D_L$. (Note that N_α has the filtration induced by that of D_L.) For a general $(\varphi,\Gamma_{\mathbb{Q}_p})$-module $\mathbb{D}$, one can define a complex (the 'Fontaine–Herr complex')

$$\mathsf{R}\Gamma(\mathbb{Q}_p, \mathbb{D}),$$

which is denoted by $C^\bullet_{\varphi,\gamma_{\mathbb{Q}_p}}(\mathbb{D})$ in [**2**, Section 2.4]. When $\mathbb{D} = \mathbb{D}^\dagger_{\mathrm{rig}}(V_L)$, this is naturally quasi-isomorphic to $\mathsf{R}\Gamma(\mathbb{Q}_p, V_L)$ (see [**2**, Proposition 2.5.2]). So there is a natural morphism in the derived category of L-vector spaces

$$\mathsf{R}\Gamma(\mathbb{Z}_S, V_L) \to \mathsf{R}\Gamma(\mathbb{Q}_p, V_L) \simeq \mathsf{R}\Gamma\big(\mathbb{Q}_p, \mathbb{D}^\dagger_{\mathrm{rig}}(V_L)\big) \to \mathsf{R}\Gamma\big(\mathbb{Q}_p, \mathbb{D}^\dagger_{\mathrm{rig}}(V_L)/\mathbb{D}_\alpha\big).$$

We define the Selmer complex by

$$\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q}, V_L) := \mathrm{Cone}\left(\mathsf{R}\Gamma(\mathbb{Z}_S, V_L) \to \mathsf{R}\Gamma\big(\mathbb{Q}_p, \mathbb{D}^\dagger_{\mathrm{rig}}(V_L)/\mathbb{D}_\alpha\big) \oplus \bigoplus_{\ell \in S\setminus\{p\}} \mathsf{R}\Gamma_{/f}(\mathbb{Q}_\ell, V_L)\right)[-1].$$

(We adopt [**3**, (2.6)] as the definition.) We set $\widetilde{H}^i_f(\mathbb{Q}, V_L) := H^i(\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q}, V_L))$. It is known that

$$H^1_f(\mathbb{Q}, V_L) \simeq \widetilde{H}^1_f(\mathbb{Q}, V_L).$$

(See [**2**, Theorem III].)

We next study the Iwasawa-theoretic version. We set

$$\mathcal{H} := \left\{ f(X) = \sum_{n=0}^{\infty} c_n X^n \in L[[X]] \;\middle|\; f(X) \text{ converges on the open unit disk} \right\}.$$

Then, for a general $(\varphi, \Gamma_{\mathbb{Q}_p})$-module $\mathbb{D}$, one can define an Iwasawa cohomology complex of $\mathcal{H}$-modules

$$\mathsf{R}\Gamma_{\mathrm{Iw}}(\mathbb{Q}_p, \mathbb{D}).$$

(See [**2**, Section 2.8].) We fix a topological generator $\gamma \in \Gamma$. Then Γ acts on $\mathcal{H}$ by identifying $X = \gamma - 1$. We set

$$\overline{V}_L := V_L \otimes_L \mathcal{H},$$

where $G_{\mathbb{Q}}$ acts on $\mathcal{H}$ via

$$G_{\mathbb{Q}} \twoheadrightarrow \Gamma \xrightarrow{\gamma \mapsto \gamma^{-1}} \Gamma.$$

When $\mathbb{D} = \mathbb{D}^\dagger_{\mathrm{rig}}(V_L)$, we have a natural quasi-isomorphism $\mathsf{R}\Gamma_{\mathrm{Iw}}(\mathbb{Q}_p, \mathbb{D}) \simeq \mathsf{R}\Gamma(\mathbb{Q}_p, \overline{V}_L)$ (see [**2**, Theorem 2.8.2]). Thus there is a natural morphism in the derived category of $\mathcal{H}$-modules

$$\mathsf{R}\Gamma(\mathbb{Z}_S, \overline{V}_L) \to \mathsf{R}\Gamma(\mathbb{Q}_p, \overline{V}_L) \simeq \mathsf{R}\Gamma_{\mathrm{Iw}}\big(\mathbb{Q}_p, \mathbb{D}^\dagger_{\mathrm{rig}}(V_L)\big) \to \mathsf{R}\Gamma_{\mathrm{Iw}}\big(\mathbb{Q}_p, \mathbb{D}^\dagger_{\mathrm{rig}}(V_L)/\mathbb{D}_\alpha\big).$$

We define the Iwasawa Selmer complex by

$$\widetilde{\mathsf{R}\Gamma}_{f,\mathrm{Iw}}(\mathbb{Q}, V_L) := \mathrm{Cone}\left(\mathsf{R}\Gamma(\mathbb{Z}_S, \overline{V}_L) \to \mathsf{R}\Gamma_{\mathrm{Iw}}\big(\mathbb{Q}_p, \mathbb{D}^\dagger_{\mathrm{rig}}(V_L)/\mathbb{D}_\alpha\big) \oplus \bigoplus_{\ell \in S\setminus\{p\}} \mathsf{R}\Gamma_{/f}(\mathbb{Q}_\ell, \overline{V}_L)\right)[-1].$$

We know the following 'control theorem'

$$\widetilde{\mathsf{R}\Gamma}_{f,\mathrm{Iw}}(\mathbb{Q}, V_L) \otimes^{\mathsf{L}}_{\mathcal{H}} L \simeq \widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q}, V_L). \tag{5.1.3}$$

(See [**35**, Theorem 1.12].)

We now give the definition of the p-adic height pairing. Let $\mathcal{I} := (X)$ be the augmentation ideal of $\mathcal{H}$. Note that $\mathcal{I}/\mathcal{I}^2$ is identified with $L \otimes_{\mathbb{Z}_p} I/I^2$. From the exact sequence

$$0 \to \mathcal{I}/\mathcal{I}^2 \to \mathcal{H}/\mathcal{I}^2 \to L \to 0,$$

we obtain the exact triangle

$$\widetilde{\mathsf{R}\Gamma}_{f,\mathrm{Iw}}(\mathbb{Q}, V_L) \otimes^{\mathsf{L}}_{\mathcal{H}} \mathcal{I}/\mathcal{I}^2 \to \widetilde{\mathsf{R}\Gamma}_{f,\mathrm{Iw}}(\mathbb{Q}, V_L) \otimes^{\mathsf{L}}_{\mathcal{H}} \mathcal{H}/\mathcal{I}^2 \to \widetilde{\mathsf{R}\Gamma}_{f,\mathrm{Iw}}(\mathbb{Q}, V_L) \otimes^{\mathsf{L}}_{\mathcal{H}} L.$$

By the control theorem (5.1.3), we have

$$\widetilde{\mathsf{R}\Gamma}_{f}(\mathbb{Q}, V_L) \otimes^{\mathsf{L}}_{L} \mathcal{I}/\mathcal{I}^2 \to \widetilde{\mathsf{R}\Gamma}_{f,\mathrm{Iw}}(\mathbb{Q}, V_L) \otimes^{\mathsf{L}}_{\mathcal{H}} \mathcal{H}/\mathcal{I}^2 \to \widetilde{\mathsf{R}\Gamma}_{f}(\mathbb{Q}, V_L).$$

The (-1)-times connecting homomorphism of this triangle gives a map

$$\widetilde{H}^1_f(\mathbb{Q}, V_L) \to H^2\big(\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q}, V_L) \otimes^{\mathsf{L}}_{L} \mathcal{I}/\mathcal{I}^2\big) = \widetilde{H}^2_f(\mathbb{Q}, V_L) \otimes_L \mathcal{I}/\mathcal{I}^2.$$

Composing this map with the global duality map

$$\widetilde{H}^2_f(\mathbb{Q}, V_L) \to \widetilde{H}^1_f(\mathbb{Q}, V_L)^*$$

(see [**2**, Theorem 3.1.5]), we obtain

$$\widetilde{H}^1_f(\mathbb{Q}, V_L) \to \widetilde{H}^1_f(\mathbb{Q}, V_L)^* \otimes_L \mathcal{I}/\mathcal{I}^2.$$

This gives the desired p-adic height pairing.

Remark 5.3. The above construction makes sense even when p is good ordinary. In this case, α is canonically chosen so that $\mathrm{ord}_p(\alpha) < 1$, and we can take N_α to be $D_{\mathrm{crys}}(F^+V)$. One sees that the p-adic height pairing with this choice coincides with that in Section 5.1.1.

Remark 5.4. Comparisons of this p-adic height pairing with the classical ones are studied in detail by Benois [**2**]. In particular, this p-adic height pairing coincides with the one constructed by Nekovář in [**31**], which is used by Kobayashi in [**26**].

5.2. A comparison result.

We shall define the p-adic regulator and compare it with the Bockstein regulator R^{Boc}_ω. In this subsection, we assume Hypothesis 2.2.

5.2.1. Let L be the splitting field of the polynomial $X^2 - a_pX + p$ over $\mathbb{Q}_p$. Note that $L = \mathbb{Q}_p$ unless p is supersingular.

Let

$$\langle -, - \rangle_p : E(\mathbb{Q}) \times E(\mathbb{Q}) \to L \otimes_{\mathbb{Z}_p} I/I^2$$

be the p-adic height pairing defined above. (When p is supersingular, this depends on the choice of a root α of $X^2 - a_pX + p$.)

DEFINITION 5.5. The p-adic regulator

$$R_p = R_{p,\alpha} \in L \otimes_{\mathbb{Z}_p} Q^r$$

is defined to be the discriminant of the p-adic height pairing, i.e.,

$$R_p := \det(\langle x_i, x_j \rangle_p)_{1 \le i,j \le r}$$

with $\{x_1, \dots, x_r\}$ a basis of $E(\mathbb{Q})_{\mathrm{tf}}$.

The p-adic height pairing induces a map

$$\begin{aligned} E(\mathbb{Q}) \times (\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})) \otimes_{\mathbb{Z}_p} Q^{r-1} &\to L \otimes_{\mathbb{Z}_p} Q^r \\ (x, (a \otimes y) \otimes b) &\mapsto a \cdot b \cdot \langle x, y \rangle_p, \end{aligned} \tag{5.2.1}$$

which we denote also by $\langle -, - \rangle_p$.

The following gives a relation between R_p and R_ω^{Boc}.

THEOREM 5.6. *For any $x \in E(\mathbb{Q})$ we have*

$$\left\langle x, R_\omega^{\mathrm{Boc}} \right\rangle_p = \log_\omega(x) \cdot R_p.$$

5.2.2. The proof of Theorem 5.6 will be given in Section 5.2.3. However, we first need to prove several preliminary technical results.

LEMMA 5.7. *The p-adic height pairing is symmetric, i.e.,*

$$\langle x, y \rangle_p = \langle y, x \rangle_p$$

for any $x, y \in E(\mathbb{Q})$.

PROOF. See [**32**, Corollary 11.2.2] and [**2**, Theorem I] in the ordinary and supersingular cases respectively. □

LEMMA 5.8. *The following diagram is commutative.*

$$\begin{array}{ccc} E(\mathbb{Q}) & \longrightarrow & (L \otimes_{\mathbb{Z}} E(\mathbb{Q}))^* \otimes_{\mathbb{Z}_p} I/I^2 \\ & \searrow^{\varprojlim_n \beta_n} & \Big\downarrow (2.2.2) \\ & & L \otimes_{\mathbb{Q}_p} H^2(\mathbb{Z}_S, V) \otimes_{\mathbb{Z}_p} I/I^2, \end{array}$$

where the horizontal arrow is the map induced by the p-adic height pairing

$$x \mapsto (y \mapsto \langle x, y \rangle_p).$$

(*For the definition of $\beta_n := \beta_{\mathbb{Q}_n}$, see* (2.3.2).)

PROOF. We first suppose that p is ordinary. We have the commutative diagram

$$\begin{array}{ccccc}
\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q},T)\otimes^{\mathsf{L}}_{\mathbb{Z}_p} I_n/I_n^2 & \longrightarrow & \widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q}_n,T)\otimes^{\mathsf{L}}_{\mathbb{Z}_p[G_n]} \mathbb{Z}_p[G_n]/I_n^2 & \longrightarrow & \widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q},T) \\
\downarrow & & \downarrow & & \downarrow \\
\mathsf{R}\Gamma(\mathbb{Z}_S,T)\otimes^{\mathsf{L}}_{\mathbb{Z}_p} I_n/I_n^2 & \longrightarrow & \mathsf{R}\Gamma(\mathcal{O}_{\mathbb{Q}_n,S},T)\otimes^{\mathsf{L}}_{\mathbb{Z}_p[G_n]} \mathbb{Z}_p[G_n]/I_n^2 & \longrightarrow & \mathsf{R}\Gamma(\mathbb{Z}_S,T),
\end{array}$$

whose rows are exact triangles. The map β_n is defined by the connecting homomorphism of the bottom triangle. On the other hand, the p-adic height pairing is defined by the connecting homomorphism of the top triangle. Thus the claim follows from the functoriality of the connecting homomorphism, i.e., the commutativity of the diagram

$$\begin{array}{ccc}
\widetilde{H}^1_f(\mathbb{Q},T) & \longrightarrow & \widetilde{H}^2_f(\mathbb{Q},T)\otimes_{\mathbb{Z}_p} I_n/I_n^2 \\
\downarrow & & \downarrow \\
H^1(\mathbb{Z}_S,T) & \longrightarrow & H^2(\mathbb{Z}_S,T)\otimes_{\mathbb{Z}_p} I_n/I_n^2,
\end{array}$$

where the horizontal arrows are connecting homomorphisms.

Next, suppose that p is good supersingular. With the notations in Section 5.1.2, we have the commutative diagram with exact rows

$$\begin{array}{ccccc}
\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q},V_L)\otimes^{\mathsf{L}}_{L} \mathcal{I}/\mathcal{I}^2 & \longrightarrow & \widetilde{\mathsf{R}\Gamma}_{f,\mathrm{Iw}}(\mathbb{Q},V_L)\otimes^{\mathsf{L}}_{\mathcal{H}} \mathcal{H}/\mathcal{I}^2 & \longrightarrow & \widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q},V_L) \\
\downarrow & & \downarrow & & \downarrow \\
\mathsf{R}\Gamma(\mathbb{Z}_S,V_L)\otimes^{\mathsf{L}}_{L} \mathcal{I}/\mathcal{I}^2 & \longrightarrow & \mathsf{R}\Gamma(\mathbb{Z}_S,\overline{V}_L)\otimes^{\mathsf{L}}_{\mathcal{H}} \mathcal{H}/\mathcal{I}^2 & \longrightarrow & \mathsf{R}\Gamma(\mathbb{Z}_S,V_L).
\end{array}$$

Since the map $\varprojlim_n \beta_n$ coincides with the map defined by the connecting homomorphism of the bottom triangle (by Shapiro's lemma), the claim follows by the same argument as in the ordinary case. □

LEMMA 5.9. *Let M and N be L-vector spaces of dimension r and $r-1$ respectively. Suppose that an exact sequence*

$$0 \to N \xrightarrow{\iota} M \xrightarrow{\ell} L \to 0 \tag{5.2.2}$$

and L-linear maps $f : M \to M^*$ and $g : M \to N^*$ are given. Assume the following.

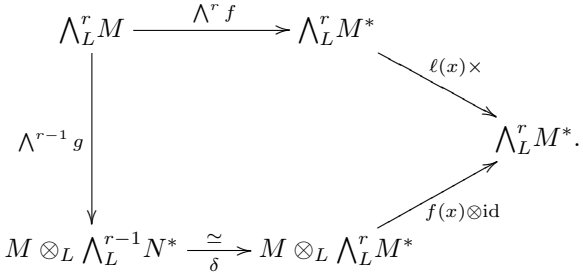
(a) *The diagram*

$$\begin{array}{ccc}
M & \xrightarrow{f} & M^* \\
& \searrow^{g} & \downarrow{\scriptstyle \iota^*} \\
& & N^*
\end{array}$$

is commutative.

(b) *The map f satisfies $f(x)(y) = f(y)(x)$ for any $x, y \in M$.*

Then for any $x \in M$ the following diagram is commutative.



(5.2.3)

Here δ is the natural isomorphism induced by (5.2.2)*, and the left vertical arrow is defined by*

$$\left(\bigwedge^{r-1} g\right)(x_1 \wedge \cdots \wedge x_r) = \sum_{i=1}^{r} (-1)^{i+1} x_i \otimes g(x_1) \wedge \cdots \wedge g(x_{i-1}) \wedge g(x_{i+1}) \wedge \cdots \wedge g(x_r).$$

PROOF. Let $\{x_1, \ldots, x_r\}$ be a basis of M and fix $x \in M$. It is sufficient to prove

$$f(x) \circ \delta \circ \left(\bigwedge^{r-1} g\right)(x_1 \wedge \cdots \wedge x_r) = \ell(x) \cdot f(x_1) \wedge \cdots \wedge f(x_r).$$

We shall describe the left hand side explicitly. Using assumption (a), we have

$$\begin{aligned} &\delta \circ \left(\bigwedge^{r-1} g\right)(x_1 \wedge \cdots \wedge x_r) \\ &\quad = \sum_{i=1}^{r} x_i \otimes f(x_1) \wedge \cdots \wedge f(x_{i-1}) \wedge \ell \wedge f(x_{i+1}) \wedge \cdots \wedge f(x_r). \end{aligned} \tag{5.2.4}$$

Thus we have

$$\begin{aligned} &f(x) \circ \delta \circ \left(\bigwedge^{r-1} g\right)(x_1 \wedge \cdots \wedge x_r) \\ &\quad = \sum_{i=1}^{r} f(x)(x_i) \cdot f(x_1) \wedge \cdots \wedge f(x_{i-1}) \wedge \ell \wedge f(x_{i+1}) \wedge \cdots \wedge f(x_r). \end{aligned}$$

Suppose first that f is bijective. Then $\{f(x_1), \ldots, f(x_r)\}$ is a basis of M^* and we can write

$$\ell = \sum_{i=1}^{r} a_i f(x_i) \text{ in } M^*$$

with some $a_1, \ldots, a_r \in L$. By assumption (b), we have $f(x)(x_i) = f(x_i)(x)$ and so we compute

$$\begin{aligned}&\sum_{i=1}^{r} f(x)(x_i)\cdot f(x_1)\wedge\cdots\wedge f(x_{i-1})\wedge\ell\wedge f(x_{i+1})\wedge\cdots\wedge f(x_r)\\&\quad=\sum_{i=1}^{r} a_i f(x_i)(x)\cdot f(x_1)\wedge\cdots\wedge f(x_r)\\&\quad=\ell(x)\cdot f(x_1)\wedge\cdots\wedge f(x_r).\end{aligned}$$

This proves the lemma in this case.

Suppose next that f is not bijective. Then $\{f(x_1),\dots,f(x_r)\}$ is linearly dependent so we may assume

$$f(x_1)=\sum_{i=2}^{r} a_i f(x_i)$$

with some $a_2,\dots,a_r\in L$.

We then compute

$$\begin{aligned}&\sum_{i=1}^{r} f(x)(x_i)\cdot f(x_1)\wedge\cdots\wedge f(x_{i-1})\wedge\ell\wedge f(x_{i+1})\wedge\cdots\wedge f(x_r)\\&\quad=\sum_{i=1}^{r} f(x_i)(x)\cdot f(x_1)\wedge\cdots\wedge f(x_{i-1})\wedge\ell\wedge f(x_{i+1})\wedge\cdots\wedge f(x_r)\\&\quad=\left(\sum_{i=2}^{r} a_i f(x_i)(x)\right)\cdot\ell\wedge f(x_2)\wedge\cdots\wedge f(x_r)\\&\qquad+\sum_{i=2}^{r} f(x_i)(x)\cdot\left(\sum_{j=2}^{r} a_j f(x_j)\right)\wedge f(x_2)\wedge\cdots\wedge f(x_{i-1})\wedge\ell\wedge f(x_{i+1})\wedge\cdots\wedge f(x_r)\\&\quad=\sum_{i=2}^{r} a_i f(x_i)(x)\cdot\ell\wedge f(x_2)\wedge\cdots\wedge f(x_r)\\&\qquad+\sum_{i=2}^{r} a_i f(x_i)(x)\cdot f(x_i)\wedge f(x_2)\wedge\cdots\wedge f(x_{i-1})\wedge\ell\wedge f(x_{i+1})\wedge\cdots\wedge f(x_r)\\&\quad=0.\end{aligned}$$

Since $\bigwedge^r f$ is also zero in this case, this proves the desired commutativity. □

5.2.3. We are now ready to prove Theorem 5.6.

To do this we first apply Lemma 5.9 with $M:=L\otimes_{\mathbb{Z}}E(\mathbb{Q})$, $N:=L\otimes_{\mathbb{Q}_p}H^2(\mathbb{Z}_S,V)^*$ and the exact sequence

$$0\to L\otimes_{\mathbb{Q}_p}H^2(\mathbb{Z}_S,V)^*\to L\otimes_{\mathbb{Z}}E(\mathbb{Q})\xrightarrow{\log_\omega} L\to 0,$$

which is obtained from (2.2.2) (so we let ℓ in (5.2.2) be $\log_\omega$). We fix a $\mathbb{Z}_p$-basis of I/I^2 and identify it with $\mathbb{Z}_p$. By letting

$$f : M \to M^*;\ x \mapsto (y \mapsto \langle x, y\rangle_p)$$

and

$$g := \varprojlim_n \beta_n : M \to N^*,$$

we see that assumptions (a) and (b) in Lemma 5.9 are satisfied by Lemmas 5.8 and 5.7 respectively.

Let $\{x_1, \dots, x_r\}$ be a basis of $E(\mathbb{Q})_{\mathrm{tf}} \subset M$. By the definition of R_p, we have

$$\left(\bigwedge\nolimits^r f\right)(x_1 \wedge \cdots \wedge x_r) = R_p \cdot x_1^* \wedge \cdots \wedge x_r^* \in \bigwedge\nolimits_L^r M^*.$$

On the other hand, we have

$$\delta \circ \left(\bigwedge\nolimits^{r-1} g\right)(x_1 \wedge \cdots \wedge x_r) = R_\omega^{\mathrm{Boc}} \otimes (x_1^* \wedge \cdots \wedge x_r^*) \in M \otimes_L \bigwedge\nolimits_L^r M^*, \tag{5.2.5}$$

where δ is as in (5.2.3). This again follows from the definition of R_ω^{Boc}. Hence, for any $x \in E(\mathbb{Q})$, the commutativity of (5.2.3) implies

$$f(x)\big(R_\omega^{\mathrm{Boc}}\big) = \ell(x) \cdot R_p,$$

i.e.,

$$\big\langle x, R_\omega^{\mathrm{Boc}}\big\rangle_p = \log_\omega(x) \cdot R_p.$$

This completes the proof of Theorem 5.6.

5.3. Schneider's height pairing.

We now consider the case that p is split multiplicative. In this case, the classical p-adic height pairing constructed by Schneider [**40**] is different from that of Nekovář constructed above. Explicitly, Schneider's p-adic height pairing

$$\langle -, - \rangle_p^{\mathrm{Sch}} : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{Q}_p \otimes_{\mathbb{Z}_p} I/I^2$$

is related to Nekovář's height pairing $\langle -, - \rangle_p$ by

$$\ell_p\big(\langle x, y\rangle_p^{\mathrm{Sch}}\big) = \ell_p(\langle x, y\rangle_p) - \frac{\log_\omega(x)\log_\omega(y)}{\log_p(q_E)} \ \text{ in } \mathbb{Q}_p, \tag{5.3.1}$$

where ℓ_p denotes the isomorphism

$$\ell_p : \mathbb{Q}_p \otimes_{\mathbb{Z}_p} I/I^2 \xrightarrow{\gamma - 1 \mapsto \gamma} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Gamma \xrightarrow{\chi_{\mathrm{cyc}}} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} (1 + p\mathbb{Z}_p) \xrightarrow{\log_p} \mathbb{Q}_p, \tag{5.3.2}$$

with χ_{cyc} the cyclotomic character, and $q_E \in \mathbb{Q}_p$ is the p-adic Tate period of E. (See [**32**, Theorem 11.4.6], where Schneider's height is denoted by h_π^{norm}.) Note that, by the so-called 'Saint Etienne theorem' of Barré-Sirieix, Diaz, Gramain and Philibert [**1**], one has $\log_p(q_E) \neq 0$ and so the above formula makes sense. Since the relation (5.3.1)

characterizes $\langle -,-\rangle_p^{\mathrm{Sch}}$, we adopt it as the definition of Schneider's p-adic height pairing.

DEFINITION 5.10. We define Schneider's p-adic regulator

$$R_p^{\mathrm{Sch}} \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} Q^r$$

by the discriminant of Schneider's p-adic height pairing, i.e.,

$$R_p^{\mathrm{Sch}} := \det\bigl(\langle x_i, x_j\rangle_p^{\mathrm{Sch}}\bigr)_{1\le i,j\le r}$$

with $\{x_1,\dots,x_r\}$ a basis of $E(\mathbb{Q})_{\mathrm{tf}}$.

We identify $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} I/I^2 = \mathbb{Q}_p$ via the isomorphism ℓ_p. By using the relation (5.3.1), one checks that

$$R_p^{\mathrm{Sch}} = R_p - \frac{1}{\log_p(q_E)} \sum_{i=1}^{r} \log_\omega(x_i) \det \begin{pmatrix} \langle x_1,x_1\rangle_p & \langle x_1,x_2\rangle_p & \cdots & \log_\omega(x_1) & \cdots & \langle x_1,x_r\rangle_p \\ \langle x_2,x_1\rangle_p & \cdots & \cdots & \log_\omega(x_2) & \cdots & \langle x_2,x_r\rangle_p \\ \vdots & & & \vdots & & \vdots \\ \langle x_r,x_1\rangle_p & \cdots & \cdots & \log_\omega(x_r) & \cdots & \langle x_r,x_r\rangle_p \end{pmatrix},$$

where the vector $(\log_\omega(x_j))_j$ is put on the i-th column in the matrix on the right hand side. In fact, this follows from the elementary formula

$$\det(a_{ij} + cb_ib_j) = \det(a_{ij}) + c\sum_{i=1}^{r} b_i \det \begin{pmatrix} a_{11} & a_{12} & \cdots & b_1 & \cdots & a_{1r} \\ a_{21} & \cdots & \cdots & b_2 & \cdots & a_{2r} \\ \vdots & & & \vdots & & \vdots \\ a_{r1} & \cdots & \cdots & b_r & \cdots & a_{rr} \end{pmatrix}$$

(with the vector $(b_j)_j$ put on the i-th column). Furthermore, by (5.2.4) and (5.2.5), we have

$$R_\omega^{\mathrm{Boc}} = \sum_{i=1}^{r} x_i \otimes \det \begin{pmatrix} \langle x_1,x_1\rangle_p & \langle x_1,x_2\rangle_p & \cdots & \log_\omega(x_1) & \cdots & \langle x_1,x_r\rangle_p \\ \langle x_2,x_1\rangle_p & \cdots & \cdots & \log_\omega(x_2) & \cdots & \langle x_2,x_r\rangle_p \\ \vdots & & & \vdots & & \vdots \\ \langle x_r,x_1\rangle_p & \cdots & \cdots & \log_\omega(x_r) & \cdots & \langle x_r,x_r\rangle_p \end{pmatrix},$$

and hence we have

$$R_p^{\mathrm{Sch}} = R_p - \frac{\log_\omega(R_\omega^{\mathrm{Boc}})}{\log_p(q_E)}.$$

From this and Theorem 5.6, we obtain the following.

THEOREM 5.11. *For any $x \in E(\mathbb{Q})$ we have*

$$\bigl\langle x, R_\omega^{\mathrm{Boc}}\bigr\rangle_p^{\mathrm{Sch}} = \log_\omega(x)\cdot R_p^{\mathrm{Sch}}.$$

6. The generalized Rubin formula and consequences.

In this section we relate Conjectures 4.8 and 4.15 to the p-adic analogue of the Birch and Swinnerton-Dyer conjecture formulated by Mazur, Tate and Teitelbaum in [**30**] (see Corollaries 6.6 and 6.7).

In particular, we continue to assume in this section that E does not have additive reduction at p.

6.1. Review of the p-adic L-function.

In this subsection, we review the p-adic L-function of Mazur–Tate–Teitelbaum [**30**]. See also the review in [**23**, Section 16.1].

When p is good, let $\alpha \in \overline{\mathbb{Q}}_p$ be a root of $X^2 - a_p X + p$ such that $\mathrm{ord}_p(\alpha) < 1$ (an 'allowable root'), and $\beta(:= p/\alpha)$ the other root. Note that, when p is good ordinary, α is uniquely determined by this property.

When p is split (resp. non-split) multiplicative, we set $\alpha := 1$ (resp. -1) and $\beta := p$ (resp. $-p$).

We set

$$L := \mathbb{Q}_p(\alpha).$$

Note that $L = \mathbb{Q}_p$ unless p is supersingular.

Recall that $\mathbb{Q}_\infty/\mathbb{Q}$ denotes the cyclotomic $\mathbb{Z}_p$-extension and $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. Let $\widehat{\Gamma}$ denote the set of $\overline{\mathbb{Q}}$-valued characters of Γ of finite order.

Recall also that an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ is fixed. For a positive integer m, let $\zeta_m \in \overline{\mathbb{Q}}$ be the element corresponding to $e^{2\pi\sqrt{-1}/m} \in \mathbb{C}$. We also fix an isomorphism $\mathbb{C} \simeq \mathbb{C}_p$. From this, we obtain an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Thus each character in $\widehat{\Gamma}$ is regarded both $\overline{\mathbb{Q}}_p$ and $\mathbb{C}$-valued.

As in Section 2, we fix a Néron differential $\omega \in \Gamma(E, \Omega^1_{E/\mathbb{Q}})$. Let ξ be the element of $\mathrm{SL}_2(\mathbb{Z})$ used in the construction of Kato's Euler system (and normalized as in (2.1.3)). Let Ω_ξ be the real period associated to (ω, ξ) (see (2.1.4)).

We fix a topological generator γ of Γ. Then we have a natural identification

$$\mathcal{O}_L[[\Gamma]] = \mathcal{O}_L[[\gamma - 1]].$$

Let $|-|_p : \mathbb{C}_p \to \mathbb{R}_{\geq 0}$ denote the p-adic absolute value normalized by $|p|_p = p^{-1}$. For a positive integer h, we define

$$\mathcal{H}_h := \left\{ \sum_{n=0}^{\infty} c_n(\gamma - 1)^n \in L[[\gamma - 1]] \;\middle|\; \lim_{n\to\infty} \frac{|c_n|_p}{n^h} = 0 \right\}$$

and

$$\mathcal{H}_\infty := \bigcup_h \mathcal{H}_h.$$

For any continuous character $\chi : \Gamma \to \overline{\mathbb{Q}}_p^\times$ and $f = \sum_n c_n(\gamma - 1)^n \in \mathcal{H}_\infty$, we can define a natural evaluation

$$\chi(f) := \sum_n c_n(\chi(\gamma)-1)^n \in \overline{\mathbb{Q}}_p.$$

It is known that there is a unique element (the 'p-adic L-function' of E)

$$\mathcal{L}_{S,p} = \mathcal{L}_{S,p,\alpha,\omega,\xi} \in \mathcal{H}_1$$

that has the following property: for any character $\chi \in \widehat{\Gamma}$ one has

$$\chi(\mathcal{L}_{S,p}) = \begin{cases} \left(1-\dfrac{1}{\alpha}\right)\left(1-\dfrac{1}{\beta}\right)^{-1} \dfrac{L_S(E,1)}{\Omega_\xi} & \text{if } \chi = 1, \\ \dfrac{\tau(\chi)}{\alpha^n}\dfrac{L_S(E,\chi^{-1},1)}{\Omega_\xi} & \text{if } \chi \text{ has conductor } p^n > 1. \end{cases}$$

Here in the latter case $\tau(\chi)$ denotes the Gauss sum

$$\tau(\chi) := \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})} \chi(\sigma)\zeta_{p^n}^{\sigma},$$

and $L_S(E,\chi^{-1},s)$ denotes the S-truncated Hasse–Weil L-function of E twisted by χ^{-1}. For the construction of $\mathcal{L}_{S,p}$ from Kato's Euler system, see Theorem 6.10 below.

Let $\mathcal{I} := (\gamma - 1)$ be the augmentation ideal of $\mathcal{H}_\infty$. For a non-negative integer a, we set

$$\mathcal{Q}^a := \mathcal{I}^a/\mathcal{I}^{a+1}.$$

Note that we have a natural identification

$$\mathcal{Q}^a = L \otimes_{\mathbb{Z}_p} Q^a.$$

We know the following 'order of vanishing' (which is actually a consequence of Proposition 4.4).

PROPOSITION 6.1 ([**23**, Theorem 18.4]). *Set $r := \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$. Then we have*

$$\mathcal{L}_{S,p} \in \begin{cases} \mathcal{I}^r & \text{if } p \text{ is good or non-split multiplicative,} \\ \mathcal{I}^{r+1} & \text{if } p \text{ is split multiplicative.} \end{cases}$$

6.2. The generalized Rubin formula.

Let $\mathcal{L}_{S,p}^{(r)}$ (resp. $\mathcal{L}_{S,p}^{(r+1)}$) denote the image of $\mathcal{L}_{S,p} \in \mathcal{I}^r$ (resp. $\mathcal{I}^{r+1}$) in $\mathcal{Q}^r$ (resp. $\mathcal{Q}^{r+1}$) when p is good or non-split multiplicative (resp. split multiplicative).

Recall some notations. Let

$$\langle -,- \rangle_p = \langle -,- \rangle_{p,\alpha} : E(\mathbb{Q}) \times (\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})) \otimes_{\mathbb{Z}_p} Q^{r-1} \to L \otimes_{\mathbb{Z}_p} Q^r = \mathcal{Q}^r$$

be the map induced by the p-adic height pairing (see (5.2.1)). Let $\log_\omega : E(\mathbb{Q}_p) \to \mathbb{Q}_p$ be the formal logarithm associated to the fixed Néron differential ω. Let

$$\kappa_\infty \in H^1(\mathbb{Z}_S, V) \otimes_{\mathbb{Z}_p} Q^{r-1} \simeq (\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})) \otimes_{\mathbb{Z}_p} Q^{r-1}$$

be the Iwasawa–Darmon derivative in Definition 4.5.

The following is a generalization of 'Rubin's formula' for the higher rank case.

THEOREM 6.2 (the generalized Rubin formula). *Under Hypothesis* 2.2, *we have the following.*

(i) *If p is good or non-split multiplicative, then for any $x \in E(\mathbb{Q})$ we have*

$$\langle x, \kappa_\infty \rangle_p = \left(1 - \frac{1}{\alpha}\right)^{-1} \left(1 - \frac{1}{\beta}\right) \log_\omega(x) \cdot \mathcal{L}_{S,p}^{(r)} \ \text{ in } \ \mathcal{Q}^r.$$

(ii) *If p is split multiplicative, then for any $x \in E(\mathbb{Q})$ we have*

$$\langle x, \kappa_\infty \rangle_p^{\mathrm{Sch}} \cdot \frac{1}{\mathrm{ord}_p(q_E)}(1 - \mathrm{rec}_p(q_E)) = \left(1 - \frac{1}{p}\right) \log_\omega(x) \cdot \mathcal{L}_{S,p}^{(r+1)} \ \text{ in } \ \mathcal{Q}^{r+1}.$$

Here $q_E \in \mathbb{Q}_p^\times$ denotes the p-adic Tate period of E and $\mathrm{rec}_p : \mathbb{Q}_p^\times \to \Gamma$ the local reciprocity map.

REMARK 6.3. When $r = 1$, we have $\kappa_\infty = z_{\mathbb{Q}}$ (see Remark 4.7), so Theorem 6.2(i) asserts

$$\langle x, z_{\mathbb{Q}} \rangle_p = \left(1 - \frac{1}{\alpha}\right)^{-1} \left(1 - \frac{1}{\beta}\right) \log_\omega(x) \cdot \mathcal{L}_{S,p}^{(1)} \ \text{ in } \ \mathcal{I}/\mathcal{I}^2.$$

When p is good ordinary, this formula is proved by Rubin [**36**, Theorem 1(ii)], which we call 'Rubin's formula' (following Nekovář [**32**, (11.3.14)]). (Note that '$L'_{\boldsymbol{z},\omega}(\mathbf{1})$' in [**36**, Theorem 1(ii)] corresponds to our $\left(1 - \frac{1}{\alpha}\right)\mathcal{L}_{S,p}^{(1)}$.) Thus Theorem 6.2(i) is regarded as a 'higher rank' generalization of Rubin's formula.

REMARK 6.4. The element

$$\frac{1}{\mathrm{ord}_p(q_E)}(1 - \mathrm{rec}_p(q_E)) \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} I/I^2$$

appearing in Theorem 6.2(ii) is essentially the '$\mathcal{L}$-invariant'. In fact, one checks that the image of this element under the isomorphism

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} I/I^2 \xrightarrow{\gamma-1 \mapsto \gamma} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Gamma \xrightarrow{\chi_{\mathrm{cyc}}} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} (1 + p\mathbb{Z}_p) \xrightarrow{\log_p} \mathbb{Q}_p$$

(see (5.3.2)) is the usual $\mathcal{L}$-invariant

$$\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}.$$

REMARK 6.5. When $r = 1$, Theorem 6.2(ii) is obtained by Venerucci [**44**, Theorem 12.31] and Büyükboduk [**12**, Theorem 3.22].

A proof of Theorem 6.2 will be given in Section 6.4. We state here some consequences of the theorem. Recall that $v_\xi \in \mathbb{Q}^\times$ is defined by $\Omega^+ = v_\xi \cdot \Omega_\xi$ (see (4.3.3)).

COROLLARY 6.6. *Conjecture* 4.15 *implies the p-adic Birch and Swinnerton-Dyer formula in* [**30**, Chapter II, Section 10]*, i.e.,*

$$\left(1-\frac{1}{\alpha}\right)^{-1}\left(1-\frac{1}{\beta}\right)\cdot \mathcal{L}_{S,p}^{(r)} = v_\xi \left(\prod_{\ell\in S\setminus\{\infty\}} L_\ell\right)\frac{\#Ш(E/\mathbb{Q})\cdot \mathrm{Tam}(E)}{\#E(\mathbb{Q})_{\mathrm{tors}}^2} R_p$$

if p is good or non-split multiplicative, and

$$\mathcal{L}_{S,p}^{(r+1)} = \frac{1}{\mathrm{ord}_p(q_E)}(1-\mathrm{rec}_p(q_E))\cdot v_\xi \left(\prod_{\ell\in S\setminus\{\infty,p\}} L_\ell\right)\frac{\#Ш(E/\mathbb{Q})\cdot \mathrm{Tam}(E)}{\#E(\mathbb{Q})_{\mathrm{tors}}^2} R_p^{\mathrm{Sch}}$$

if p is split multiplicative.

If $R_p \neq 0$ (resp. $R_p^{\mathrm{Sch}} \neq 0$), then the converse also holds when p is good or non-split multiplicative (resp. split multiplicative).

PROOF. We only treat the case when p is good or non-split multiplicative. The case when p is split multiplicative is treated similarly, by using Theorem 5.11.

Conjecture 4.15 asserts

$$\kappa_\infty = v_\xi \left(\prod_{\ell\in S\setminus\{\infty\}} L_\ell\right)\frac{\#Ш(E/\mathbb{Q})\mathrm{Tam}(E)}{\#E(\mathbb{Q})_{\mathrm{tors}}^2}\cdot R_\omega^{\mathrm{Boc}} \text{ in } (\mathbb{Q}_p\otimes_{\mathbb{Z}} E(\mathbb{Q}))\otimes_{\mathbb{Z}_p} Q^{r-1}.$$

Take $x \in E(\mathbb{Q})$ such that $\log_\omega(x) \neq 0$. Taking $\langle x, -\rangle_p$ to both sides, we obtain

$$\left(1-\frac{1}{\alpha}\right)^{-1}\left(1-\frac{1}{\beta}\right)\log_\omega(x)\cdot \mathcal{L}_{S,p}^{(r)} = v_\xi \left(\prod_{\ell\in S\setminus\{\infty\}} L_\ell\right)\frac{\#Ш(E/\mathbb{Q})\mathrm{Tam}(E)}{\#E(\mathbb{Q})_{\mathrm{tors}}^2}\log_\omega(x) R_p$$

by Theorems 6.2 and 5.6. Since $\log_\omega(x) \neq 0$, we can cancel it from both sides and obtain the desired formula.

If $R_p \neq 0$, then the map $y \mapsto (x \mapsto \langle x, y\rangle_p)$ is injective, and so the converse holds. □

Similarly, we also obtain the following.

COROLLARY 6.7. *Conjecture* 4.8 *implies the p-adic Beilinson formula, i.e.,*

$$\left(1-\frac{1}{\alpha}\right)^{-1}\left(1-\frac{1}{\beta}\right)\cdot \mathcal{L}_{S,p}^{(r)} = \frac{L_S^*(E,1)}{\Omega_\xi\cdot R_\infty} R_p \tag{6.2.1}$$

if p is good or non-split multiplicative, and

$$\mathcal{L}_{S,p}^{(r+1)} = \frac{1}{\mathrm{ord}_p(q_E)}(1-\mathrm{rec}_p(q_E))\cdot \frac{L_{S\setminus\{p\}}^*(E,1)}{\Omega_\xi\cdot R_\infty} R_p^{\mathrm{Sch}} \tag{6.2.2}$$

if p is split multiplicative.

If $R_p \neq 0$ (resp. $R_p^{\mathrm{Sch}} \neq 0$), then the converse also holds when p is good or non-split multiplicative (resp. split multiplicative).

PROOF. This follows by the same argument as the proof of Corollary 6.6, using Proposition 4.14. □

REMARK 6.8. When p is good and $r_{\mathrm{an}} = r = 1$, the formula (6.2.1) was proved by Perrin-Riou [**33**, Corollary 1.8] in the ordinary case, and by Kobayashi [**26**, Corollary 1.3] in the supersingular case. (It is essentially the 'p-adic Gross–Zagier formula'.) When p is split multiplicative and $r_{\mathrm{an}} = r = 0$, the formula (6.2.2) was first proved by Greenberg and Stevens [**20**] and then by Kobayashi [**25**] and by Kato, Tsuji and the second author (unpublished).

6.3. Review of the Coleman map.

As a preliminary of the proof of Theorem 6.2, we review the construction of the Coleman map. We follow the explicit construction due to Rubin [**37**, Appendix]. See also [**27**, Section 3].

We set

$$D := D_{\mathrm{crys}}(V).$$

Let φ denote the Frobenius operator acting on D. For a finite extension $K/\mathbb{Q}_p$, we set

$$D_K := K \otimes_{\mathbb{Q}_p} D.$$

Let

$$[-,-]_K : (K \otimes_{\mathbb{Q}_p} D_{\mathrm{dR}}(V)) \times D_K \to K$$

denote the natural pairing.

We use the following fact.

LEMMA 6.9 ([**23**, Theorem 16.6(1)]). *Set $L := \mathbb{Q}_p(\alpha)$. There exists a unique $\nu = \nu_{\alpha,\omega} \in D_L$ such that*

$$\varphi(\nu) = \alpha p^{-1}\nu = \beta^{-1}\nu \quad \textit{and} \quad [\omega, \nu]_L = 1.$$

Let $\mathbb{Q}_{n,p}$ denote the completion of $\mathbb{Q}_n$ at the unique prime lying above p. We set

$$L_n := L \cdot \mathbb{Q}_{n,p}.$$

Let $\nu \in D_L$ be as in Lemma 6.9 and set

$$\begin{aligned}\delta_n &:= \frac{1}{p^{n+1}} \mathrm{Tr}_{L(\mu_{p^{n+1}})/L_n} \left(\sum_{i=0}^{n} \zeta_{p^{n+1-i}} \varphi^{i-n-1}(\nu) + (1-\varphi)^{-1}(\nu) \right) \\ &= \frac{1}{\alpha^{n+1}} \mathrm{Tr}_{L(\mu_{p^{n+1}})/L_n} \left(\sum_{i=0}^{n} \frac{\zeta_{p^{n+1-i}} - 1}{\beta^i} + \frac{\beta}{\beta - 1} \right) \nu \in D_{L_n}. \end{aligned} \tag{6.3.1}$$

This element satisfies

$$\mathrm{Tr}_{L_{n+1}/L_n}(\delta_{n+1}) = \delta_n$$

and for any character χ of G_n

$$\sum_{\sigma\in G_n}\sigma(\delta_n)\chi(\sigma) = \begin{cases} \left(1-\dfrac{1}{\alpha}\right)\left(1-\dfrac{1}{\beta}\right)^{-1}\nu & \text{if } \chi = 1, \\ \dfrac{\tau(\chi)}{\alpha^m}\nu & \text{if } \chi \text{ has conductor } p^m > 1 \end{cases} \tag{6.3.2}$$

in $D_{L(\mu_{p^{n+1}})}$ (see [**37**, Lemma A.1] or [**27**, Lemma 3.1]).

As in Section 4.2, we set

$$H^i_n := H^i(\mathcal{O}_{\mathbb{Q}_n,S}, T) \quad \text{and} \quad \mathbb{H}^i := \varprojlim_n H^i_n.$$

We define a map

$$\mathrm{Col}_n : H^1_n \to L[G_n]$$

by

$$\mathrm{Col}_n(z) := \sum_{\sigma\in G_n} \mathrm{Tr}_{L_n/L}\big([\exp^*_n(z), \sigma\delta_n]_{L_n}\big)\sigma,$$

where

$$\exp^*_n = \exp^*_{\mathbb{Q}_{n,p},V} : H^1_n \to H^1(\mathbb{Q}_{n,p}, T) \to \mathbb{Q}_{n,p}\otimes_{\mathbb{Q}_p} D_{\mathrm{dR}}(V)$$

denotes the Bloch–Kato dual exponential map. This map induces a map on the inverse limit

$$\mathrm{Col} := \varprojlim_n \mathrm{Col}_n : \mathbb{H}^1 \to \mathcal{H}_\infty.$$

This is the definition of the Coleman map.

We set

$$t_{c,d} := cd(c-\sigma_c)(d-\sigma_d) \in \mathbb{Z}_p[[\Gamma]]. \tag{6.3.3}$$

Here $\sigma_a \in \Gamma$ is the restriction of the automorphism of $\mathbb{Q}(\mu_{p^\infty})$ characterized by $\zeta_{p^n}^{\sigma_a} = \zeta_{p^n}^a$ for every n.

The following result is well-known.

THEOREM 6.10 (Kato [**23**, Theorem 16.6(2)]). *We have*

$$\mathrm{Col}((_{c,d}z_n)_n) = t_{c,d}\cdot\mathcal{L}_{S,p}.$$

6.4. The proof of Theorem 6.2.

In this subsection, we prove Theorem 6.2.

6.4.1. We first establish several important preliminary results.

We initially suppose that p is good or non-split multiplicative, and give a proof of Theorem 6.2(i).

We shall use the derivative introduced by Nekovář in [**32**, Section 11.3.14], based on the idea of Rubin in [**36**].

With the notations in Section 5.1, we set

$$F^-V := \begin{cases} V/F^+V & \text{if } p \text{ is ordinary,} \\ \mathbb{D}^\dagger_{\mathrm{rig}}(V_L)/\mathbb{D}_\alpha & \text{if } p \text{ is supersingular.} \end{cases}$$

For $y \in \mathbb{H}^1$, we define 'Rubin's derivative'

$$\mathcal{D}(y) \in H^1(\mathbb{Q}_p, F^-V) \otimes_{\mathbb{Z}_p} I/I^2$$

as follows. (Compare the definition given by Nekovář in [**32**, Section 11.3.14], where the symbol 'Dx_{Iw}' is used.)

Suppose first that p is ordinary. We have a commutative diagram with exact rows and columns

$$\begin{array}{ccccc}
\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q},V)\otimes^{\mathsf{L}}_{\mathbb{Z}_p} I/I^2 & \longrightarrow & \mathsf{R}\Gamma(\mathbb{Z}_S,V)\otimes^{\mathsf{L}}_{\mathbb{Z}_p} I/I^2 & \longrightarrow & \mathsf{R}\Gamma(\mathbb{Q}_p,F^-V)\otimes^{\mathsf{L}}_{\mathbb{Z}_p} I/I^2 \\
\downarrow & & \downarrow & & \downarrow{\scriptstyle i} \\
\widetilde{\mathsf{R}\Gamma}_{f,\mathrm{Iw}}(\mathbb{Q},V)\otimes^{\mathsf{L}}_{\Lambda} \Lambda/I^2 & \longrightarrow & \mathsf{R}\Gamma_{\mathrm{Iw}}(\mathbb{Z}_S,V)\otimes^{\mathsf{L}}_{\Lambda} \Lambda/I^2 & \xrightarrow{\mathrm{loc}_p} & \mathsf{R}\Gamma_{\mathrm{Iw}}(\mathbb{Q}_p,F^-V)\otimes^{\mathsf{L}}_{\Lambda} \Lambda/I^2 \\
\downarrow & & \downarrow & & \downarrow \\
\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q},V) & \longrightarrow & \mathsf{R}\Gamma(\mathbb{Z}_S,V) & \longrightarrow & \mathsf{R}\Gamma(\mathbb{Q}_p,F^-V).
\end{array} \tag{6.4.1}$$

Here $\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q},V) := \widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q},T)\otimes^{\mathsf{L}}_{\mathbb{Z}_p}\mathbb{Q}_p$ and

$$\widetilde{\mathsf{R}\Gamma}_{f,\mathrm{Iw}}(\mathbb{Q},V) := \left(\varprojlim_n \widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q}_n,T)\right)\otimes^{\mathsf{L}}_{\mathbb{Z}_p}\mathbb{Q}_p.$$

$\mathsf{R}\Gamma_{\mathrm{Iw}}(\mathbb{Z}_S,V)$ and $\mathsf{R}\Gamma_{\mathrm{Iw}}(\mathbb{Q}_p,F^-V)$ are defined in a similar way.

We regard $y \in \mathbb{H}^1$ as an element of $H^1(\mathsf{R}\Gamma_{\mathrm{Iw}}(\mathbb{Z}_S,V)\otimes^{\mathsf{L}}_{\Lambda}\Lambda/I^2)$. Since y_0 lies in $\widetilde{H}^1_f(\mathbb{Q},V)$ (see (2.2.1)) and $H^0(\mathbb{Q}_p,F^-V)=0$, a diagram chasing shows that there exists a unique element $\mathcal{D}(y)\in H^1(\mathbb{Q}_p,F^-V)\otimes_{\mathbb{Z}_p} I/I^2$ such that

$$\mathrm{loc}_p(y) = i(\mathcal{D}(y)) \text{ in } H^1\big(\mathsf{R}\Gamma_{\mathrm{Iw}}(\mathbb{Q}_p,F^-V)\otimes^{\mathsf{L}}_{\Lambda}\Lambda/I^2\big).$$

This gives the definition of Rubin's derivative in this case.

When p is supersingular, Rubin's derivative is defined in the same way, by considering the commutative diagram with exact rows and columns

$$\begin{array}{ccccc}
\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q},V_L)\otimes^{\mathsf{L}}_{\mathbb{Z}_p} I/I^2 & \longrightarrow & \mathsf{R}\Gamma(\mathbb{Z}_S,V_L)\otimes^{\mathsf{L}}_{\mathbb{Z}_p} I/I^2 & \longrightarrow & \mathsf{R}\Gamma(\mathbb{Q}_p,F^-V)\otimes^{\mathsf{L}}_{\mathbb{Z}_p} I/I^2 \\
\downarrow & & \downarrow & & \downarrow \\
\widetilde{\mathsf{R}\Gamma}_{f,\mathrm{Iw}}(\mathbb{Q},V_L)\otimes^{\mathsf{L}}_{\mathcal{H}} \mathcal{H}/\mathcal{I}^2 & \longrightarrow & \mathsf{R}\Gamma(\mathbb{Z}_S,\overline{V}_L)\otimes^{\mathsf{L}}_{\mathcal{H}} \mathcal{H}/\mathcal{I}^2 & \longrightarrow & \mathsf{R}\Gamma_{\mathrm{Iw}}(\mathbb{Q}_p,F^-V)\otimes^{\mathsf{L}}_{\mathcal{H}} \mathcal{H}/\mathcal{I}^2 \\
\downarrow & & \downarrow & & \downarrow \\
\widetilde{\mathsf{R}\Gamma}_f(\mathbb{Q},V_L) & \longrightarrow & \mathsf{R}\Gamma(\mathbb{Z}_S,V_L) & \longrightarrow & \mathsf{R}\Gamma(\mathbb{Q}_p,F^-V).
\end{array}$$

Let

$$(-,-)_p : H^1_f(\mathbb{Q}_p,V)\times H^1(\mathbb{Q}_p,F^-V)\to H^2(\mathbb{Q}_p,L(1))\simeq L$$

be the pairing defined by the cup product. This pairing induces

$$(-,-)_p : E(\mathbb{Q})\times \left(H^1(\mathbb{Q}_p,F^-V)\otimes_{\mathbb{Z}_p} I/I^2\right)\to L\otimes_{\mathbb{Z}_p} I/I^2=\mathcal{I}/\mathcal{I}^2. \tag{6.4.2}$$

The following is an abstract version of Rubin's formula.

THEOREM 6.11 (Rubin, Nekovář). *Suppose that p is not split multiplicative. For any $x\in E(\mathbb{Q})$ and $y=(y_n)_n\in \varprojlim_n H^1_n=\mathbb{H}^1$, we have*

$$\langle x,y_0\rangle_p=(x,\mathcal{D}(y))_p \ \text{ in } \mathcal{I}/\mathcal{I}^2.$$

PROOF. This is proved in [**32**, Proposition 11.3.15]. We give a proof for the reader's convenience. We treat only the ordinary case, since the supersingular case is treated in a similar way.

Recall that the map $\widetilde{\beta}:\widetilde{H}^1_f(\mathbb{Q},V)\to \widetilde{H}^2_f(\mathbb{Q},V)\otimes_{\mathbb{Z}_p} I/I^2$ in (5.1.1) is defined to be (-1)-times the connecting homomorphism of the left vertical triangle of (6.4.1). Let $\delta: H^1(\mathbb{Q}_p,F^-V)\otimes_{\mathbb{Z}_p} I/I^2\to \widetilde{H}^2_f(\mathbb{Q},V)$ be the connecting homomorphism of the upper horizontal triangle of (6.4.1). Then, by the compatibility of connecting homomorphisms (see [**32**, Lemma 1.2.19]), we have

$$\widetilde{\beta}(y_0)=\delta(\mathcal{D}(y)).$$

We identify $\widetilde{H}^2_f(\mathbb{Q},V)=\widetilde{H}^1_f(\mathbb{Q},V)^*=\mathbb{Q}_p\otimes_{\mathbb{Z}} E(\mathbb{Q})^*$ by global duality. Then for any $x\in E(\mathbb{Q})$ we have

$$\widetilde{\beta}(y_0)(x)=\langle x,y_0\rangle_p$$

by the definition of the p-adic height pairing. On the other hand, by the compatibility between local and global duality, we have

$$\delta(\mathcal{D}(y))(x)=(x,\mathcal{D}(y))_p.$$

Thus we have

$$\langle x,y_0\rangle_p=(x,\mathcal{D}(y))_p. \qquad \square$$

We shall now apply Theorem 6.11 in our setting.

LEMMA 6.12. *Let* ${}_{c,d}\kappa_\infty \in H^1_0 \otimes_{\mathbb{Z}_p} Q^{r-1}$ *be the Iwasawa–Darmon derivative in Definition* 4.5. *Then there exists a unique* $w = (w_n)_n \in \varprojlim_n H^1_n = \mathbb{H}^1$ *such that*

$$ {}_{c,d}z_n = (\gamma - 1)^{r-1} w_n$$

for every n *and*

$$ {}_{c,d}\kappa_\infty = w_0 \otimes (\gamma - 1)^{r-1}.$$

PROOF. By the proof of Proposition 4.4, we have ${}_{c,d}z_\infty \in I^{r-1} \cdot \mathbb{H}^1$. Since $\mathbb{H}^1$ is a free Λ-module of rank one, there exists a unique $w \in \mathbb{H}^1$ such that ${}_{c,d}z_\infty = (\gamma - 1)^{r-1} w$. The description of ${}_{c,d}\kappa_\infty$ follows from (4.2.1). □

By Lemma 6.12, we can define the 'Rubin's derivative of the Iwasawa–Darmon derivative'

$$\mathcal{D}({}_{c,d}\kappa_\infty) := \mathcal{D}(w) \cdot (\gamma - 1)^{r-1} \in H^1(\mathbb{Q}_p, F^- V) \otimes_{\mathbb{Z}_p} Q^r.$$

Applying Theorem 6.11 to this element, we obtain the following.

COROLLARY 6.13. *For any* $x \in E(\mathbb{Q})$, *we have*

$$\langle x, {}_{c,d}\kappa_\infty \rangle_p = (x, \mathcal{D}({}_{c,d}\kappa_\infty))_p \ \text{ in } \ \mathcal{Q}^r,$$

where

$$(-,-)_p : E(\mathbb{Q}) \times \left(H^1(\mathbb{Q}_p, F^- V) \otimes_{\mathbb{Z}_p} Q^r \right) \to \mathcal{Q}^r$$

is the map induced by (6.4.2).

LEMMA 6.14. *Let* $y \in \mathbb{H}^1$. *Then we have*

$$\mathrm{Col}(y) \in \mathcal{I}$$

and

$$\mathrm{Col}(y) = (\exp_0(\delta_0), \mathcal{D}(y))_p \ \text{ in } \ \mathcal{I}/\mathcal{I}^2,$$

where $\exp_0 = \exp_{\mathbb{Q}_p, V} : D_L \to L \otimes_{\mathbb{Q}_p} H^1_f(\mathbb{Q}_p, V)$ *denotes the Bloch–Kato exponential map.*

PROOF. We shall show the first claim. By the construction of the Coleman map, it is sufficient to show that

$$\sum_{\sigma \in G_n} \mathrm{Tr}_{L_n/L}\left([\exp_n^*(y_n), \sigma\delta_n]_{L_n} \right) = 0$$

for every n. The left hand side is equal to $[\exp_0^*(y_0), \delta_0]_L$. Since y_0 lies in $H^1_f(\mathbb{Q}, V)$, we know that $\exp_0^*(y_0) = 0$ and so we have proved the first claim.

Next, we shall show the second claim. Note that, by construction, we have

$$\mathrm{Col}_n(y_n) = \sum_{\sigma \in G_n} (\exp_n(\delta_n), \sigma y_n)_{L_n} \sigma^{-1},$$

where $\exp_n : D_{L_n} \to H^1_f(L_n, V)$ denotes the Bloch–Kato exponential map and

$$(-,-)_{L_n} : H^1_f(L_n, V) \times H^1(\mathbb{Q}_{n,p}, F^- V) \to L$$

denotes the cup product pairing. Noting this, one verifies

$$\mathrm{Col}(y) = (\exp_0(\delta_0), \mathcal{D}(y))_p \text{ in } \mathcal{I}/\mathcal{I}^2$$

by the definition of $\mathcal{D}(y)$. □

6.4.2. Proof of Theorem 6.2(i). Let $w \in \mathbb{H}^1$ be the element in Lemma 6.12. We compute

$$\begin{aligned} t_{c,d} \cdot \mathcal{L}_{S,p} &= \mathrm{Col}((_{c,d}z_n)_n) \quad \text{(by Theorem 6.10)} \\ &= \mathrm{Col}(w) \cdot (\gamma - 1)^{r-1} \quad \text{(by Lemma 6.12)} \\ &\in \mathcal{I}^r \quad \text{(by Lemma 6.14).} \end{aligned}$$

Hence, in the quotient $\mathcal{Q}^r = \mathcal{I}^r/\mathcal{I}^{r+1}$, we compute

$$\begin{aligned} t_{c,d} \cdot \mathcal{L}^{(r)}_{S,p} &= (\exp_0(\delta_0), \mathcal{D}(w))_p \cdot (\gamma - 1)^{r-1} \quad \text{(by Lemma 6.14)} \\ &= (\exp_0(\delta_0), \mathcal{D}(_{c,d}\kappa_\infty))_p. \end{aligned}$$

By (6.3.2), note that

$$\delta_0 = \left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{\beta}\right)^{-1} \nu.$$

Since $[\omega, \nu]_L = 1$ by Lemma 6.9, we have

$$\left(1 - \frac{1}{\alpha}\right)^{-1}\left(1 - \frac{1}{\beta}\right) \log_\omega(x) \exp_0(\delta_0) = x \text{ in } H^1_f(\mathbb{Q}_p, V)$$

for any $x \in E(\mathbb{Q})$. Thus we have

$$\begin{aligned} \left(1 - \frac{1}{\alpha}\right)^{-1}\left(1 - \frac{1}{\beta}\right) \log_\omega(x) t_{c,d} \cdot \mathcal{L}^{(r)}_{S,p} &= (x, \mathcal{D}(_{c,d}\kappa_\infty))_p \\ &= \langle x, _{c,d}\kappa_\infty \rangle_p \quad \text{(by Corollary 6.13).} \end{aligned}$$

Upon multiplying both sides by $t_{c,d}^{-1}$ we obtain the desired formula.

This completes the proof of Theorem 6.2(i).

6.4.3. We now suppose that p is split multiplicative and prepare for the proof of Theorem 6.2(ii).

Note first that, by Tate's uniformization, we have an exact sequence of $G_{\mathbb{Q}_p}$-modules

$$0 \to \mathbb{Z}_p(1) \to T \to \mathbb{Z}_p \to 0. \tag{6.4.3}$$

This means that $F^+V \simeq \mathbb{Q}_p(1)$ and $F^-V := V/F^+V \simeq \mathbb{Q}_p$.

Since $H^0(\mathbb{Q}_p, F^-V)$ does not vanish in this case, Rubin's derivative $\mathcal{D}(y)$ is not determined uniquely, so we impose more condition to define it. Let

$$\rho_p : H^0(\mathbb{Q}_p, F^-V) \to H^1(\mathbb{Q}_p, F^-V) \otimes_{\mathbb{Z}_p} I/I^2$$

be the connecting homomorphism obtained from the right vertical exact triangle in (6.4.1). We know that

$$\mathrm{im}(\rho_p) = \langle \log_p \chi_{\mathrm{cyc}} \rangle \otimes_{\mathbb{Z}_p} I/I^2,$$

where we regard $\log_p \chi_{\mathrm{cyc}} : G_{\mathbb{Q}_p} \to \mathbb{Q}_p$ as an element of $H^1(\mathbb{Q}_p, F^-V) = H^1(\mathbb{Q}_p, \mathbb{Q}_p) = \mathrm{Hom}_{\mathrm{cont}}(G_{\mathbb{Q}_p}, \mathbb{Q}_p)$. (See the proof of [**44**, Lemma 15.1] for example.) Let

$$\pi_p : H^1(\mathbb{Q}_p, V) \otimes_{\mathbb{Z}_p} I/I^2 \to H^1(\mathbb{Q}_p, F^-V) \otimes_{\mathbb{Z}_p} I/I^2$$

be the map induced by $V \twoheadrightarrow F^-V$. Then one sees that $\mathrm{im}(\rho_p) \cap \mathrm{im}(\pi_p) = 0$ (since $\log_p(q_E) \neq 0$), by which one can take a unique element

$$\mathcal{D}(y) \in \mathrm{im}(\pi_p)$$

such that $\mathrm{loc}_p(y) = i(\mathcal{D}(y))$ in $H^1(\mathrm{R}\Gamma_{\mathrm{Iw}}(\mathbb{Q}_p, F^-V) \otimes^{\mathbb{L}}_{\Lambda} \Lambda/I^2)$. Compare Venerucci's construction [**44**, Lemma 15.1] (where I/I^2 is identified with $\mathbb{Z}_p$).

An analogue of Theorem 6.11 is as follows.

THEOREM 6.15. *Suppose that p is split multiplicative. For any $x \in E(\mathbb{Q})$ and $y = (y_n)_n \in \varprojlim_n H^1_n = \mathbb{H}^1$, we have*

$$\langle x, y_0 \rangle_p^{\mathrm{Sch}} = (x, \mathcal{D}(y))_p \ \text{ in } \ \mathbb{Q}_p \otimes_{\mathbb{Z}_p} I/I^2.$$

PROOF. We identify $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} I/I^2 = \mathbb{Q}_p$ via the isomorphism ℓ_p in (5.3.2). By the same argument as in Venerucci [**44**, Proposition 15.2], we have

$$\log_\omega(x) \cdot \mathcal{D}(y)(\mathrm{Fr}_p) = -\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)} \langle x, y_0 \rangle_p^{\mathrm{Sch}}.$$

(See also [**44**, (127)].) Here $\mathcal{D}(y)(\mathrm{Fr}_p)$ means the evaluation of $\mathcal{D}(y) \in H^1(\mathbb{Q}_p, \mathbb{Q}_p) = \mathrm{Hom}_{\mathrm{cont}}(G_{\mathbb{Q}_p}, \mathbb{Q}_p)$ at the arithmetic Frobenius Fr_p (this corresponds to $\mathrm{Der}_p(\boldsymbol{x})$ in [**44**, Section 15], where $\boldsymbol{x}$ corresponds to our y). Since $\mathcal{D}(y)(\mathrm{Fr}_p) = -\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)} \exp^*_\omega(\mathcal{D}(y))$ (see [**25**, (6)] or (6.4.4) below) and $\log_p(q_E) \neq 0$, we have

$$\log_\omega(x) \exp^*_\omega(\mathcal{D}(y)) = \langle x, y_0 \rangle_p^{\mathrm{Sch}}.$$

Since the left hand side is equal to $(x, \mathcal{D}(y))_p$, we obtain the desired formula. □

Theorem 6.15 immediately implies the following, which is an analogue of Corollary 6.13.

COROLLARY 6.16. *For any $x \in E(\mathbb{Q})$, we have*

$$\langle x, {}_{c,d}\kappa_\infty \rangle_p^{\mathrm{Sch}} = (x, \mathcal{D}({}_{c,d}\kappa_\infty))_p \ \text{ in } \ \mathbb{Q}_p \otimes_{\mathbb{Z}_p} Q^r.$$

Since E over $\mathbb{Q}_p$ is a Tate curve, we have an isomorphism $E(\mathbb{Q}_p) \simeq \mathbb{Q}_p^\times / \langle q_E \rangle$. We denote by λ_p the composite map

$$\lambda_p : \mathbb{Q}_p^\times \to (\mathbb{Q}_p^\times / \langle q_E \rangle) \otimes \mathbb{Q}_p \simeq E(\mathbb{Q}_p) \otimes \mathbb{Q}_p \to H^1(\mathbb{Q}_p, V)$$

where the final map is the Kummer map. This map λ_p also coincides with the composite $\mathbb{Q}_p^\times \to H^1(\mathbb{Q}_p, \mathbb{Q}_p(1)) = H^1(\mathbb{Q}_p, F^+V) \to H^1(\mathbb{Q}_p, V)$ where the first map is the Kummer map. Therefore, for any $a \in \mathbb{Q}_p^\times$ and $z \in H^1(\mathbb{Q}_p, V)$ we have

$$(\lambda_p(a), z)_p = (a, \pi_p(z))_{\mathbb{G}_m}$$

where $\pi_p : H^1(\mathbb{Q}_p, V) \to H^1(\mathbb{Q}_p, \mathbb{Q}_p)$ is the natural map induced by $V \twoheadrightarrow F^-V = \mathbb{Q}_p$, and $(-,-)_{\mathbb{G}_m}$ is the pairing induced by the cup product $H^1(\mathbb{Q}_p, \mathbb{Q}_p(1)) \times H^1(\mathbb{Q}_p, \mathbb{Q}_p) \to H^2(\mathbb{Q}_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$.

The following result explains how the $\mathcal{L}$-invariant occurs in our generalized version of Rubin's formula.

LEMMA 6.17. *For any $z \in H^1(\mathbb{Q}_p, V)$ we have*

$$(\lambda_p(p), z)_p \cdot (\gamma - 1) = (p, \pi_p(z))_{\mathbb{G}_m} \cdot (\gamma - 1) = -\frac{\log_p \chi_{\mathrm{cyc}}(\gamma)}{\mathrm{ord}_p(q_E)} \exp_\omega^*(z)(1 - \mathrm{rec}_p(q_E))$$

in $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} I/I^2$.

PROOF. We write $\log_{q_E} : (\mathbb{Q}_p^\times / \langle q_E \rangle) \otimes \mathbb{Q}_p \to \mathbb{Q}_p$ for the logarithm that vanishes on $\langle q_E \rangle$ and note that this coincides with the formal logarithm via the isomorphism $E(\mathbb{Q}_p) \simeq \mathbb{Q}_p^\times / \langle q_E \rangle$. We also write $\exp_{q_E}$ for the inverse of $\log_{q_E}$.

Then, by using the equality of functions

$$\log_{q_E} = \log_p - \frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)} \cdot \mathrm{ord}_p$$

(cf. the proof of [**45**, Corollary 3.7]), one computes that

$$\begin{aligned} \lambda_p(p) &= \lambda_p\big(\exp_{q_E}(\log_{q_E}(p))\big) \\ &= \lambda_p\left(\exp_{q_E}\left(-\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\right)\right) \\ &= -\exp_{\mathbb{Q}_p, V}\left(\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\nu\right) \end{aligned}$$

in $E(\mathbb{Q}_p)\otimes\mathbb{Q}_p$. Thus we have

$$(\lambda_p(p),z)_p=-\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\exp^*_\omega(z). \tag{6.4.4}$$

(See also [**25**, (6)].) The claim follows by noting

$$1-\mathrm{rec}_p(q_E)=\frac{\log_p(q_E)}{\log_p\chi_{\mathrm{cyc}}(\gamma)}\cdot(\gamma-1)\ \text{ in }\ \mathbb{Q}_p\otimes_{\mathbb{Z}_p}I/I^2. \qquad \square$$

Let U_n^1 be the group of principal local units in $\mathbb{Q}_{n,p}$. Let $(d_n)_n\in\varprojlim_n U_n^1$ be the system constructed by Kobayashi in [**25**, Section 2]. This system is related to our $(\delta_n)_n$ defined in (6.3.1) by

$$\delta_n=\log_p(d_n)\cdot\nu\ \text{ in }\ \mathbb{Q}_{n,p}\otimes_{\mathbb{Q}_p}D_{\mathrm{crys}}(V).$$

Since $d_0=1$, Hilbert's theorem 90 implies that there exists $x_n\in\mathbb{Q}_{n,p}^\times$ such that

$$d_n=\frac{\gamma x_n}{x_n}.$$

We regard $x_n\in H^1(\mathbb{Q}_{n,p},\mathbb{Z}_p(1))$ via the Kummer map. The element $\mathrm{Cor}_{\mathbb{Q}_{n,p}/\mathbb{Q}_p}(x_n)$ is well-defined in $H^1(\mathbb{Q}_p,\mathbb{Z}/p^n(1))$, i.e., independent of the choice of x_n. We define

$$d':=(\mathrm{Cor}_{\mathbb{Q}_{n,p}/\mathbb{Q}_p}(x_n))_n\in\varprojlim_n H^1(\mathbb{Q}_p,\mathbb{Z}/p^n(1))\simeq H^1(\mathbb{Q}_p,\mathbb{Z}_p(1)).$$

For each field $\mathbb{Q}_{n,p}$ with $n\geq 0$ we also write

$$(-,-)_{\mathbb{G}_m}:H^1(\mathbb{Q}_{n,p},\mathbb{Z}_p(1))\times H^1(\mathbb{Q}_{n,p},\mathbb{Z}_p)\to H^2(\mathbb{Q}_{n,p},\mathbb{Z}_p(1))\simeq\mathbb{Z}_p \tag{6.4.5}$$

for the pairing defined by the cup product. Let

$$\pi_p:H^1_n=H^1(\mathcal{O}_{\mathbb{Q}_n,S},T)\to H^1(\mathbb{Q}_{n,p},T)\to H^1(\mathbb{Q}_{n,p},\mathbb{Z}_p)$$

be the map induced by the surjection $T\twoheadrightarrow\mathbb{Z}_p$ in (6.4.3).

We define

$$\mathrm{Col}'_n:H^1_n\to\mathbb{Z}/p^n[G_n]$$

by

$$\mathrm{Col}'_n(z):=\sum_{\sigma\in G_n}(\sigma x_n,\pi_p(z))_{\mathbb{G}_m}\sigma$$

and set

$$\mathrm{Col}':=\varprojlim_n\mathrm{Col}'_n:\mathbb{H}^1\to\varprojlim_n\mathbb{Z}/p^n[G_n]\simeq\Lambda.$$

LEMMA 6.18.

(i) *The Coleman map* $\mathrm{Col} : \mathbb{H}^1 \to \Lambda$ *coincides with* $(\gamma^{-1} - 1) \cdot \mathrm{Col}'$.

(ii) *Let* $y \in \mathbb{H}^1$. *Then we have*

$$\mathrm{Col}'(y) \in I$$

and

$$\mathrm{Col}'(y) = (d', \mathcal{D}(y))_{\mathbb{G}_m} \ \text{ in } \ \mathbb{Q}_p \otimes_{\mathbb{Z}_p} I/I^2,$$

where

$$(-,-)_{\mathbb{G}_m} : H^1(\mathbb{Q}_p, \mathbb{Q}_p(1)) \times \left(H^1(\mathbb{Q}_p, \mathbb{Q}_p) \otimes_{\mathbb{Z}_p} I/I^2\right) \to \mathbb{Q}_p \otimes_{\mathbb{Z}_p} I/I^2$$

is induced by (6.4.5).

PROOF. Claim (i) follows directly from construction. (See also Kobayashi's computation of $\mathrm{Col}_n(z)$ in [**25**, p. 573].)

Claim (ii) is proved in the same way as Lemma 6.14 and so, for brevity, we omit the proof. □

6.4.4. Proof of Theorem 6.2(ii). Let $w \in \mathbb{H}^1$ be the element in Lemma 6.12. We compute

$$\begin{aligned} t_{c,d} \cdot \mathcal{L}_{S,p} &= \mathrm{Col}((_{c,d}z_n)_n) \quad \text{(by Theorem 6.10)} \\ &= \mathrm{Col}(w) \cdot (\gamma - 1)^{r-1} \quad \text{(by Lemma 6.12)} \\ &= \mathrm{Col}'(w) \cdot (\gamma^{-1} - 1)(\gamma - 1)^{r-1} \quad \text{(by Lemma 6.18(i))} \\ &\in I^{r+1} \quad \text{(by Lemma 6.18(ii))}. \end{aligned}$$

Thus, in $I^{r+1}/I^{r+2} = Q^{r+1}$, we further compute

$$\begin{aligned} t_{c,d} \cdot \mathcal{L}_{S,p}^{(r+1)} &= -\mathrm{Col}'(w) \cdot (\gamma - 1)^r \\ &= -(d', \mathcal{D}(w))_{\mathbb{G}_m} \cdot (\gamma - 1)^r \quad \text{(by Lemma 6.18(ii))}. \end{aligned}$$

Since

$$(d', \mathcal{D}(w))_{\mathbb{G}_m} = \left(1 - \frac{1}{p}\right)^{-1} (\log_p \chi_{\mathrm{cyc}}(\gamma))^{-1} (p, \mathcal{D}(w))_{\mathbb{G}_m}$$

(see Kobayashi [**25**, p. 574, line 2], note that '$\mathrm{N}x_n$' in [**25**] is congruent to d' modulo p^n), Lemma 6.17 implies that

$$-(d', \mathcal{D}(w))_{\mathbb{G}_m} \cdot (\gamma - 1)^r = \left(1 - \frac{1}{p}\right)^{-1} \exp_\omega^*(\mathcal{D}(w)) \cdot \frac{1}{\mathrm{ord}_p(q_E)} (1 - \mathrm{rec}_p(q_E)) \cdot (\gamma - 1)^{r-1}.$$

Note that, for any $x \in E(\mathbb{Q})$ and $y \in H^1(\mathbb{Q}_p, V)$, we have

$$\log_\omega(x) \exp^*_\omega(y) = (x, y)_p.$$

Hence we have

$$\begin{aligned}
&\left(1 - \frac{1}{p}\right) \log_\omega(x) t_{c,d} \cdot \mathcal{L}_{S,p}^{(r+1)} \\
&\quad = (x, \mathcal{D}(w))_p \cdot \frac{1}{\mathrm{ord}_p(q_E)} (1 - \mathrm{rec}_p(q_E)) \cdot (\gamma - 1)^{r-1} \\
&\quad = (x, \mathcal{D}({}_{c,d}\kappa_\infty))_p \cdot \frac{1}{\mathrm{ord}_p(q_E)} (1 - \mathrm{rec}_p(q_E)) \\
&\quad = \langle x, {}_{c,d}\kappa_\infty \rangle_p^{\mathrm{Sch}} \cdot \frac{1}{\mathrm{ord}_p(q_E)} (1 - \mathrm{rec}_p(q_E)) \quad \text{(by Corollary 6.16).}
\end{aligned}$$

Upon multiplying both sides by $t_{c,d}^{-1}$ we obtain the desired formula.

This thereby completes the proof of Theorem 6.2.

7. The Iwasawa main conjecture and descent theory.

The aim of this section is to directly relate Conjectures 4.8 and 4.15 with a natural main conjecture of Iwasawa theory. The main results in this section are Theorems 7.3 and 7.6.

As before, we always assume that p is odd and that $H^1(\mathbb{Z}_S, T)$ is $\mathbb{Z}_p$-free.

7.1. Review of the Iwasawa main conjecture.

We use the notations in Section 4.2.

We set

$$C_n := \mathsf{R}\,\mathrm{Hom}_{\mathbb{Z}_p}\big(\mathsf{R}\Gamma_c(\mathcal{O}_{\mathbb{Q}_n,S}, T^*(1)), \mathbb{Z}_p[-2]\big)$$

and $C_\infty := \varprojlim_n C_n$. Then we have a canonical isomorphism

$$H^0(C_\infty) \simeq \mathbb{H}^1$$

and an exact sequence

$$0 \to \mathbb{H}^2 \to H^1(C_\infty) \xrightarrow{f} \Lambda \otimes_{\mathbb{Z}_p} T^*(1)^{+,*} \to 0. \tag{7.1.1}$$

(See (4.1.1) and (4.1.2).) Let $Q(\Lambda)$ denote the quotient field of Λ. Kato proved that

$$Q(\Lambda) \otimes_\Lambda \mathbb{H}^i \begin{cases} \simeq Q(\Lambda) & \text{if } i = 1, \\ = 0 & \text{if } i = 2. \end{cases}$$

(See [**23**, Theorem 12.4].) Hence, we have a canonical isomorphism

$$Q(\Lambda) \otimes_\Lambda \det_\Lambda(C_\infty) \simeq Q(\Lambda) \otimes_\Lambda (\mathbb{H}^1 \otimes_{\mathbb{Z}_p} T^*(1)^+). \tag{7.1.2}$$

We set

$$ {}_{c,d}z_\infty := ({}_{c,d}z_n)_n \in \varprojlim_n H^1_n = \mathbb{H}^1 $$

and

$$ z_\infty := t_{c,d}^{-1} \cdot {}_{c,d}z_\infty \in Q(\Lambda) \otimes_\Lambda \mathbb{H}^1, $$

where $t_{c,d} \in \Lambda$ is as in (6.3.3). We then define

$$ \mathfrak{z}_\infty \in Q(\Lambda) \otimes_\Lambda \det_\Lambda(C_\infty) $$

to be the element corresponding to

$$ z_\infty \otimes e^+\delta(\xi) \in Q(\Lambda) \otimes_\Lambda (\mathbb{H}^1 \otimes_{\mathbb{Z}_p} T^*(1)^+) $$

under the isomorphism (7.1.2), where $\delta(\xi) \in \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathscr{H} \simeq T^*(1)$ is defined in Section 2.1.

Conjecture 7.1 (Iwasawa main conjecture). *We have*

$$ \langle \mathfrak{z}_\infty \rangle_\Lambda = \det_\Lambda(C_\infty). $$

Remark 7.2. Since Λ is a regular local ring, we see by [**22**, Chapter I, Proposition 2.1.5] that Conjecture 7.1 is equivalent to

$$ z_\infty \in \mathbb{H}^1 \quad \text{and} \quad \mathrm{char}_\Lambda(\mathbb{H}^1/\langle z_\infty \rangle_\Lambda) = \mathrm{char}_\Lambda(\mathbb{H}^2). $$

Thus Conjecture 7.1 is equivalent to [**23**, Conjecture 12.10] (by letting f in loc. cit. be the normalized newform corresponding to E). We prefer the formulation as in Conjecture 7.1 to the classical one using characteristic ideals as above, since one can formulate an equivariant Iwasawa main conjecture as a direct generalization of Conjecture 7.1. (See [**7**, Conjecture 3.1] in the case of Tate motives.)

7.2. Consequences of the Iwasawa main conjecture.
We now state main results of this section.

Theorem 7.3. *Assume Hypothesis* 2.2. *Then Conjecture* 7.1 (*Iwasawa main conjecture*) *implies Conjecture* 4.15 *up to* $\mathbb{Z}_p^\times$, *i.e., there exists* $u \in \mathbb{Z}_p^\times$ *such that*

$$ \kappa_\infty = u \cdot v_\xi \left(\prod_{\ell \in S \setminus \{\infty\}} L_\ell \right) \frac{\#Ш(E/\mathbb{Q}) \cdot \mathrm{Tam}(E)}{\#E(\mathbb{Q})^2_{\mathrm{tors}}} \cdot R_\omega^{\mathrm{Boc}} \quad \textit{in} \quad (\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})) \otimes_{\mathbb{Z}_p} Q^{r-1}. $$

Combining this theorem with Corollary 6.6, we immediately obtain the following.

Corollary 7.4. *Assume Hypothesis* 2.2. *Then Conjecture* 7.1 (*Iwasawa main conjecture*) *implies the p-adic Birch and Swinnerton-Dyer formula up to* $\mathbb{Z}_p^\times$, *i.e., there exists* $u \in \mathbb{Z}_p^\times$ *such that*

$$\left(1-\frac{1}{\alpha}\right)^{-1}\left(1-\frac{1}{\beta}\right)\cdot\mathcal{L}_{S,p}^{(r)}=u\cdot v_\xi\left(\prod_{\ell\in S\setminus\{\infty\}}L_\ell\right)\frac{\#Ш(E/\mathbb{Q})\cdot\mathrm{Tam}(E)}{\#E(\mathbb{Q})_{\mathrm{tors}}^2}R_p$$

if p is good or non-split multiplicative, and

$$\mathcal{L}_{S,p}^{(r+1)}=u\cdot\frac{1}{\mathrm{ord}_p(q_E)}(1-\mathrm{rec}_p(q_E))\cdot v_\xi\left(\prod_{\ell\in S\setminus\{\infty,p\}}L_\ell\right)\frac{\#Ш(E/\mathbb{Q})\cdot\mathrm{Tam}(E)}{\#E(\mathbb{Q})_{\mathrm{tors}}^2}R_p^{\mathrm{Sch}}$$

if p is split multiplicative.

Remark 7.5. Corollary 7.4 improves upon results of Schneider [**41**, Theorem 5] (good ordinary case), Jones [**21**, Theorem 3.1] (multiplicative case) and Perrin-Riou [**34**, Proposition 3.4.6] (good supersingular case) in which it is shown that the Iwasawa main conjecture and non-degeneracy of the p-adic height pairing together imply the p-adic Birch and Swinnerton-Dyer formula up to $\mathbb{Z}_p^\times$.

Theorem 7.6. *Assume Hypothesis* 2.2. *Assume also that*

- *Conjecture* 7.1 (*Iwasawa main conjecture*) *is valid,*
- *Conjecture* 4.8 (*Generalized Perrin-Riou Conjecture at infinite level*) *is valid, and*
- *the Bockstein regulator R_ω^{Boc} in Definition* 4.10 *does not vanish.*

Then the p-part of the Birch and Swinnerton-Dyer formula is valid so that there is an equality

$$L^*(E,1)\cdot\mathbb{Z}_p=\left(\#Ш(E/\mathbb{Q})[p^\infty]\cdot\mathrm{Tam}(E)\cdot\#E(\mathbb{Q})_{\mathrm{tors}}^{-2}\cdot\Omega^+\cdot R_\infty\right)\cdot\mathbb{Z}_p$$

of $\mathbb{Z}_p$-sublattices of $\mathbb{C}_p$.

Remark 7.7. Theorem 7.6 explains the precise link between the natural main conjecture of Iwasawa theory and the classical Birch and Swinnerton-Dyer formula, even in the case of additive reduction. We note also that this result is, in effect, an analogue of the main result [**7**, Theorem 5.2] of the current authors, where, roughly speaking, the following result is proved in the setting of the multiplicative group: if one assumes the validity of

- the Iwasawa main conjecture for $\mathbb{G}_m$ (cf. [**7**, Conjecture 3.1]),
- the Iwasawa–Mazur–Rubin–Sano conjecture for $\mathbb{G}_m$ (cf. [**7**, Conjecture 4.2]), and
- the injectivity of a certain Bockstein homomorphism (which is implied by the condition '(F)' in [**7**, Theorem 5.2]: see [**7**, Proposition 5.16]),

then the equivariant Tamagawa number conjecture for $\mathbb{G}_m$ is also valid.

7.3. The descent argument.

In the following, we assume both Hypothesis 2.2 and the validity of Conjecture 7.1.

7.3.1. A key commutative diagram. We shall first give quick proofs of Theorems 7.3 and 7.6 by using the following key result.

THEOREM 7.8. *Let $\boldsymbol{x}$ be a $\mathbb{Z}_p$-basis of $\bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}}$. Then there is a commutative diagram*

$$\begin{array}{ccccc} \det_\Lambda(C_\infty) & \xrightarrow{\Pi_\infty} & I^{r-1}\cdot\mathbb{H}^1 & & \\ & & & \searrow^{\mathcal{N}_\infty} & \\ \downarrow{\scriptstyle \mathrm{N}_\infty} & & & & H_0^1\otimes_{\mathbb{Z}_p} Q^{r-1} \\ & & & \nearrow_{\mathrm{Boc}_{\infty,\boldsymbol{x}}} & \\ \det_{\mathbb{Z}_p}(C_0) & \xrightarrow[\Pi_{\boldsymbol{x}}]{} & \bigwedge_{\mathbb{Z}_p}^r H_0^1 & & \end{array} \tag{7.3.1}$$

with the following properties:

(a) $\Pi_\infty(\mathfrak{z}_\infty) = z_\infty$;

(b) $\mathcal{N}_\infty(z_\infty) = \kappa_\infty$;

(c) $\langle \eta_{\boldsymbol{x}}^{\mathrm{Kato}} \rangle_{\mathbb{Z}_p} = \#H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \cdot \bigwedge_{\mathbb{Z}_p}^r H_0^1$, *where* $\eta_{\boldsymbol{x}}^{\mathrm{Kato}} := \Pi_{\boldsymbol{x}}(\mathrm{N}_\infty(\mathfrak{z}_\infty))$;

(d) $\langle \mathrm{Boc}_{\infty,\boldsymbol{x}}(\eta_{\boldsymbol{x}}^{\mathrm{Kato}}) \rangle_{\mathbb{Z}_p} = \mathbb{Z}_p \cdot v_\xi\big(\prod_{\ell\in S\setminus\{\infty\}} L_\ell\big) \#Ш(E/\mathbb{Q})[p^\infty]\mathrm{Tam}(E)\#E(\mathbb{Q})_{\mathrm{tors}}^{-2} \cdot R_\omega^{\mathrm{Boc}}$.

Admitting this, we give proofs of Theorems 7.3 and 7.6.

PROOF OF THEOREM 7.3. It is sufficient to show that

$$\langle \kappa_\infty \rangle_{\mathbb{Z}_p} = \mathbb{Z}_p \cdot v_\xi \left(\prod_{\ell\in S\setminus\{\infty\}} L_\ell \right) \#Ш(E/\mathbb{Q})[p^\infty]\mathrm{Tam}(E)\#E(\mathbb{Q})_{\mathrm{tors}}^{-2} \cdot R_\omega^{\mathrm{Boc}}.$$

By the commutativity of (7.3.1) and properties (a) and (b), we have

$$\kappa_\infty = \mathrm{Boc}_{\infty,\boldsymbol{x}}\big(\eta_{\boldsymbol{x}}^{\mathrm{Kato}}\big). \tag{7.3.2}$$

Hence the claim follows from the property (d). □

PROOF OF THEOREM 7.6. We assume Conjecture 4.8 and $R_\omega^{\mathrm{Boc}} \neq 0$, in addition to Hypothesis 2.2 and Conjecture 7.1. Recall that Conjecture 4.8 asserts the equality

$$\kappa_\infty = \mathrm{Boc}_{\infty,\boldsymbol{x}}\big(\eta_{\boldsymbol{x}}^{\mathrm{BSD}}\big).$$

Combining this with (7.3.2), we have

$$\mathrm{Boc}_{\infty,\boldsymbol{x}}\big(\eta_{\boldsymbol{x}}^{\mathrm{BSD}}\big) = \mathrm{Boc}_{\infty,\boldsymbol{x}}\big(\eta_{\boldsymbol{x}}^{\mathrm{Kato}}\big).$$

Since the non-vanishing of R_ω^{Boc} is equivalent to the injectivity of $\mathrm{Boc}_{\infty,\boldsymbol{x}}$ by construction, we have

$$\eta_{\boldsymbol{x}}^{\mathrm{BSD}} = \eta_{\boldsymbol{x}}^{\mathrm{Kato}}.$$

By the property (c) in Theorem 7.8, we have

$$\mathbb{Z}_p \cdot \eta_{\boldsymbol{x}}^{\mathrm{BSD}} = \#H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \cdot \bigwedge_{\mathbb{Z}_p}^{r} H_0^1.$$

By Proposition 2.6, this is equivalent to the p-part of the Birch and Swinnerton-Dyer formula, so we have completed the proof. □

The rest of this section is devoted to the proof of Theorem 7.8.

7.3.2. Definitions of maps. First, we give definitions of the maps $\Pi_\infty, \mathcal{N}_\infty, \mathrm{N}_\infty$ and $\Pi_{\boldsymbol{x}}$ in the diagram (7.3.1).

- The map

$$\Pi_\infty : \det_\Lambda(C_\infty) \to I^{r-1} \cdot \mathbb{H}^1$$

is induced by

$$Q(\Lambda) \otimes_\Lambda \det_\Lambda(C_\infty) \overset{(7.1.2)}{\simeq} Q(\Lambda) \otimes_\Lambda (\mathbb{H}^1 \otimes_{\mathbb{Z}_p} T^*(1)^+) \simeq Q(\Lambda) \otimes_\Lambda \mathbb{H}^1,$$

where the second isomorphism is induced by

$$T^*(1)^+ \simeq \mathbb{Z}_p;\ e^+\delta(\xi) \mapsto 1.$$

By Remark 7.2, the image of $\det_\Lambda(C_\infty)$ under this isomorphism is $\mathrm{char}_\Lambda(\mathbb{H}^2) \cdot \mathbb{H}^1$. Since $\mathrm{char}_\Lambda(\mathbb{H}^2) \subset I^{r-1}$, we see that the image of $\det_\Lambda(C_\infty)$ is contained in $I^{r-1} \cdot \mathbb{H}^1$ and thus Π_∞ is defined. By this construction, it is obvious that $\Pi_\infty(\mathfrak{z}_\infty) = z_\infty$, i.e., the property (a) of Theorem 7.8 holds.

- The construction of the map

$$\mathcal{N}_\infty : I^{r-1} \cdot \mathbb{H}^1 \to H_0^1 \otimes_{\mathbb{Z}_p} Q^{r-1}$$

is done in the same way as the construction of ${}_{c,d}\kappa_\infty$ from $({}_{c,d}z_n)_n$ in Section 4.2.1. See the discussion after Proposition 4.4. (In fact, $\mathcal{N}_\infty$ is defined to be the limit of the Darmon norm $\mathcal{N}_{\mathbb{Q}_n/\mathbb{Q}}$.) It is obvious that $\mathcal{N}_\infty(z_\infty) = \kappa_\infty$, i.e., the property (b) in Theorem 7.8 holds.

- The surjection

$$\mathrm{N}_\infty : \det_\Lambda(C_\infty) \twoheadrightarrow \det_{\mathbb{Z}_p}(C_0)$$

is defined to be the augmentation map

$$\det_\Lambda(C_\infty) \twoheadrightarrow \det_\Lambda(C_\infty) \otimes_\Lambda \mathbb{Z}_p \simeq \det_{\mathbb{Z}_p}(C_0),$$

where the last isomorphism follows from the fact $C_\infty \otimes_\Lambda^{\mathbb{L}} \mathbb{Z}_p \simeq C_0$.

- The map

$$\Pi_{\boldsymbol{x}} : \det_{\mathbb{Z}_p}(C_0) \to \bigwedge_{\mathbb{Z}_p}^{r} H_0^1$$

is induced by

$$\begin{aligned}\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \det_{\mathbb{Z}_p}(C_0) &\simeq \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \left(\det_{\mathbb{Z}_p}(H^0(C_0)) \otimes_{\mathbb{Z}_p} \det_{\mathbb{Z}_p}^{-1}(H^1(C_0))\right) \\ &\simeq \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \left(\bigwedge_{\mathbb{Z}_p}^{r} H_0^1 \otimes_{\mathbb{Z}_p} \bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}}^* \otimes_{\mathbb{Z}_p} T^*(1)^+\right) \\ &\simeq \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \bigwedge_{\mathbb{Z}_p}^{r} H_0^1,\end{aligned}$$

where the second isomorphism follows from (4.1.1) and (4.1.2), and the last isomorphism is induced by

$$\bigwedge_{\mathbb{Z}_p}^{r-1} H^2(\mathbb{Z}_S, T)_{\mathrm{tf}}^* \otimes_{\mathbb{Z}_p} T^*(1)^+ \simeq \mathbb{Z}_p;\ \boldsymbol{x}^* \otimes e^+\delta(\xi) \mapsto 1.$$

Since the image of $\det_{\mathbb{Z}_p}(C_0)$ under this isomorphism is $\#H^2(\mathbb{Z}_S, T)_{\mathrm{tors}} \cdot \bigwedge_{\mathbb{Z}_p}^{r} H_0^1$, the map $\Pi_{\boldsymbol{x}}$ is defined. This also shows that the property (c) in Theorem 7.8 holds.

7.3.3. The property (d). We have already seen that the properties (a), (b) and (c) in Theorem 7.8 are satisfied.

We shall now verify property (d), i.e., that there is an equality of $\mathbb{Z}_p$-lattices

$$\mathbb{Z}_p \cdot \left(\mathrm{Boc}_{\infty,\boldsymbol{x}}(\eta_{\boldsymbol{x}}^{\mathrm{Kato}})\right) = \mathbb{Z}_p \cdot c_E \cdot R_{\omega}^{\mathrm{Boc}},$$

where

$$c_E := v_\xi \cdot \left(\prod_{\ell \in S \setminus \{\infty\}} L_\ell\right) \cdot \#Ш(E/\mathbb{Q})[p^\infty] \cdot \mathrm{Tam}(E) \cdot \#E(\mathbb{Q})_{\mathrm{tors}}^{-2}.$$

One checks that the element $\mathrm{Boc}_{\infty,\boldsymbol{x}}(\eta_{\boldsymbol{x}}^{\mathrm{Kato}})$ is independent of the choice of a non-zero element $\boldsymbol{x} \in \bigwedge_{\mathbb{Q}_p}^{r-1} H^2(\mathbb{Z}_S, V)$. (Note that both $\mathrm{Boc}_{\infty,\boldsymbol{x}}$ and $\eta_{\boldsymbol{x}}^{\mathrm{Kato}}$ are defined for such $\boldsymbol{x}$ by linearity.) So we take $\boldsymbol{x}$ to be as in Section 4.3.2, by fixing a basis $\{x_1, \dots, x_r\}$ of $E(\mathbb{Q})_{\mathrm{tf}}$.

By the definition of $R_{\omega}^{\mathrm{Boc}}$ (see Definition 4.10), it is sufficient to show that

$$\left\langle \eta_{\boldsymbol{x}}^{\mathrm{Kato}} \right\rangle_{\mathbb{Z}_p} = \mathbb{Z}_p \cdot c_E \cdot \log_\omega(x_1) \cdot x_1 \wedge \cdots \wedge x_r. \tag{7.3.3}$$

By the property (c) and (2.5.2), we have

$$\left\langle \eta_{\boldsymbol{x}}^{\mathrm{Kato}} \right\rangle_{\mathbb{Z}_p} = \left\langle \eta_{\boldsymbol{x}}^{\mathrm{alg}} \right\rangle_{\mathbb{Z}_p}.$$

(Here $\eta_{\boldsymbol{x}}^{\mathrm{alg}}$ is defined in Definition 2.17, where the finiteness of $Ш(E/\mathbb{Q})$ is assumed. But we may define $\eta_{\boldsymbol{x}}^{\mathrm{alg}}$, replacing $Ш(E/\mathbb{Q})$ by $Ш(E/\mathbb{Q})[p^\infty]$ since we only consider the $\mathbb{Z}_p$-modules here. Then we need only the finiteness of $Ш(E/\mathbb{Q})[p^\infty]$.) On the other hand,

one checks in the same way as (4.3.2) that

$$\langle \eta_{\boldsymbol{x}}^{\mathrm{alg}} \rangle_{\mathbb{Z}_p} = \mathbb{Z}_p \cdot c_E \cdot \log_\omega(x_1) \cdot x_1 \wedge \cdots \wedge x_r.$$

From this, we obtain the desired equality (7.3.3). Hence we have proved that the property (d) holds.

7.4. The proof of Theorem 7.8.

In this subsection, we prove the commutativity of the diagram (7.3.1) and thus complete the proof of Theorem 7.8. Our argument is similar to [**6**, Lemma 5.22], [**7**, Lemma 5.17] and [**11**, Theorem 4.21].

Fix a non-negative integer n. It is sufficient to show the commutativity of the following 'n-th layer version' of (7.3.1):

$$\begin{array}{ccc} \det_{\mathbb{Z}_p[G_n]}(C_n) & \xrightarrow{\Pi_n} & I_n^{r-1} \cdot H_n^1 \\ \Big\downarrow{\scriptstyle \mathrm{N}_n} & & \searrow^{\mathcal{N}_n} \\ \det_{\mathbb{Z}_p}(C_0) & \xrightarrow[\Pi_{\boldsymbol{x}}]{} & \bigwedge^r_{\mathbb{Z}_p} H_0^1 \end{array} \qquad H_0^1 \otimes_{\mathbb{Z}_p} Q_n^{r-1}. \qquad (7.4.1)$$

We shall describe maps Π_∞, Π_n, $\Pi_{\boldsymbol{x}}$ and $\mathrm{Boc}_{n,\boldsymbol{x}}$ explicitly by choosing a useful representative of the complex C_∞. Then the commutativity of the diagram is checked by an explicit computation.

7.4.1. Choice of the representative. We make a similar argument to [**6**, Section 5.4] or [**11**, Proposition A.11].

One sees that the complex C_∞ is represented by

$$\mathbb{P} \xrightarrow{\psi} \mathbb{P},$$

where $\mathbb{P}$ is a free Λ-module of rank, say, d. We have an exact sequence

$$0 \to \mathbb{H}^1 \to \mathbb{P} \xrightarrow{\psi} \mathbb{P} \xrightarrow{\pi} H^1(C_\infty) \to 0. \qquad (7.4.2)$$

Also, setting $P_n := \mathbb{P} \otimes_\Lambda \mathbb{Z}_p[G_n]$, we have an exact sequence

$$0 \to H_n^1 \to P_n \xrightarrow{\psi_n} P_n \xrightarrow{\pi_n} H^1(C_n) \to 0. \qquad (7.4.3)$$

Let $\{b_1, \ldots, b_d\}$ be a basis of $\mathbb{P}$. We denote the image of b_i in P_n by $b_{i,n}$. We set

$$x_i := \pi(b_i) \in H^1(C_\infty) \quad \text{and} \quad x_{i,n} := \pi_n(b_{i,n}) \in H^1(C_n).$$

By the argument of [**11**, Proposition A.11(i)], one may assume

(i) $f(x_1) = 1 \otimes e^+\delta(\xi)^*$, where $f : H^1(C_\infty) \to \Lambda \otimes_{\mathbb{Z}_p} T^*(1)^{+,*}$ is as in (7.1.1);

(ii) $\langle x_2, \dots, x_d \rangle_\Lambda = \mathbb{H}^2 \subset H^1(C_\infty)$;

(iii) $\{x_{2,0}, \dots, x_{r,0}\}$ is a $\mathbb{Z}_p$-basis of $H^2(\mathbb{Z}_S, T)_{\mathrm{tf}} \subset H^1(C_0)$.

We set

$$\psi_i := b_i^* \circ \psi : \mathbb{P} \to \Lambda$$

and

$$\psi_{i,n} := b_{i,n}^* \circ \psi_n : P_n \to \mathbb{Z}_p[G_n].$$

Note that the property (iii) implies that

$$\operatorname{im} \psi_{i,n} \subset I_n \text{ for every } 1 < i \leq r. \tag{7.4.4}$$

7.4.2. Explicit descriptions of $\boldsymbol{\Pi_\infty}$, $\boldsymbol{\Pi_n}$ and $\boldsymbol{\Pi_x}$. With the above representative of C_∞, we have an identification

$$\det_\Lambda(C_\infty) = \bigwedge_\Lambda^d \mathbb{P} \otimes_\Lambda \bigwedge_\Lambda^d \mathbb{P}^*.$$

We define a map

$$\Pi_\infty : \bigwedge_\Lambda^d \mathbb{P} \otimes_\Lambda \bigwedge_\Lambda^d \mathbb{P}^* \to \mathbb{P}$$

by

$$a \otimes (b_1^* \wedge \cdots \wedge b_d^*) \mapsto (-1)^{d-1} \left(\bigwedge_{1<i\leq d} \psi_i \right)(a). \tag{7.4.5}$$

(See [**6**, Section 4.1] for the construction of the map $\bigwedge_{1<i\leq d} \psi_i$.) We denote this map by Π_∞, since it coincides with Π_∞ defined in Section 7.3.2 (see [**6**, Lemma 4.3]). In particular, its image is contained in $I^{r-1} \cdot \mathbb{H}^1$. (We regard $\mathbb{H}^1 \subset \mathbb{P}$ via (7.4.2).)

Similarly, we have an identification

$$\det_{\mathbb{Z}_p[G_n]}(C_n) = \bigwedge_{\mathbb{Z}_p[G_n]}^d P_n \otimes_{\mathbb{Z}_p[G_n]} \bigwedge_{\mathbb{Z}_p[G_n]}^d P_n^*$$

and we define a map

$$\Pi_n : \bigwedge_{\mathbb{Z}_p[G_n]}^d P_n \otimes_{\mathbb{Z}_p[G_n]} \bigwedge_{\mathbb{Z}_p[G_n]}^d P_n^* \to P_n$$

by

$$a \otimes (b_{1,n}^* \wedge \cdots \wedge b_{d,n}^*) \mapsto (-1)^{d-1} \left(\bigwedge_{1<i\leq d} \psi_{i,n} \right)(a). \tag{7.4.6}$$

It is clear by construction that the inverse limit $\varprojlim_n \Pi_n$ coincides with Π_∞. Since the image of Π_∞ is contained in $I^{r-1} \cdot \mathbb{H}^1$, we see that the image of Π_n is contained in $I_n^{r-1} \cdot H_n^1$.

Finally, we give an explicit description of $\Pi_{\boldsymbol{x}}$. Here we take

$$\boldsymbol{x} := x_{2,0} \wedge \cdots \wedge x_{r,0}.$$

We have an identification

$$\det_{\mathbb{Z}_p}(C_0) = \bigwedge_{\mathbb{Z}_p}^{d} P_0 \otimes_{\mathbb{Z}_p} \bigwedge_{\mathbb{Z}_p}^{d} P_0^*.$$

We define a map

$$\Pi_{\boldsymbol{x}} : \bigwedge_{\mathbb{Z}_p}^{d} P_0 \otimes_{\mathbb{Z}_p} \bigwedge_{\mathbb{Z}_p}^{d} P_0^* \to \bigwedge_{\mathbb{Z}_p}^{r} P_0$$

by

$$a \otimes (b_{1,0}^* \wedge \cdots \wedge b_{d,0}^*) \mapsto (-1)^{r(d-r)} \left(\bigwedge_{r<i\leq d} \psi_{i,0} \right)(a). \tag{7.4.7}$$

This map coincides with $\Pi_{\boldsymbol{x}}$ defined in Section 7.3.2 (by [**6**, Lemma 4.3]). In particular, its image is contained in $\bigwedge_{\mathbb{Z}_p}^{r} H_0^1$.

7.4.3. Explicit Bockstein maps. We shall describe the Bockstein regulator map $\mathrm{Boc}_{n,\boldsymbol{x}}$ explicitly.

For an integer i with $1 < i \leq r$, we define a map

$$\beta_{i,n} : P_0 \to I_n/I_n^2$$

by

$$\beta_{i,n}(a) := \psi_{i,n}(\tilde{a}) \pmod{I_n^2},$$

where for $a \in P_0$ we take an element $\tilde{a} \in P_n$ such that $\sum_{\sigma\in G_n} \sigma(\tilde{a}) = a$ (we regard $P_0 \subset P_n$ by identifying P_0 with $P_n^{G_n}$). Note that $\psi_{i,n}(\tilde{a}) \in I_n$ by (7.4.4) and its image in I_n/I_n^2 is independent of the choice of $\tilde{a}$. Hence the map $\beta_{i,n}$ is well-defined.

Let $\beta_{\mathbb{Q}_n} : H_0^1 \to H^2(\mathbb{Z}_S, T)_{\mathrm{tf}} \otimes_{\mathbb{Z}_p} I_n/I_n^2$ be the Bockstein map defined in (2.3.2). One checks by the definition of the connecting homomorphism that

$$-\beta_{i,n} = x_{i,0}^* \circ \beta_{\mathbb{Q}_n} \text{ on } H_0^1.$$

From this, we see that the map

$$\mathrm{Boc}_{n,\boldsymbol{x}} := (-1)^{r-1} \bigwedge_{1<i\leq r} \beta_{i,n} : \bigwedge_{\mathbb{Z}_p}^{r} P_0 \to P_0 \otimes_{\mathbb{Z}_p} Q_n^{r-1} \tag{7.4.8}$$

coincides with $\mathrm{Boc}_{n,\boldsymbol{x}} = \mathrm{Boc}_{\mathbb{Q}_n,\boldsymbol{x}}$ defined in Section 2.3 on $\bigwedge_{\mathbb{Z}_p}^{r} H_0^1$.

7.4.4. Completion of the proof. We prove the commutativity of (7.4.1). We may assume $\boldsymbol{x} = x_{2,0} \wedge \cdots \wedge x_{r,0}$.

In view of the explicit descriptions (7.4.6), (7.4.7) and (7.4.8), it is sufficient to prove that

$$(-1)^{d-1}\mathcal{N}_n \circ \left(\bigwedge\nolimits_{1<i\le d} \psi_{i,n}\right)(b_{1,n}\wedge\cdots\wedge b_{d,n})$$
$$= (-1)^{r-1+r(d-r)}\left(\bigwedge\nolimits_{1<i\le r} \beta_{i,n}\right)\circ\left(\bigwedge\nolimits_{r<i\le d} \psi_{i,0}\right)(b_{1,0}\wedge\cdots\wedge b_{d,0}). \tag{7.4.9}$$

By computation, we have

$$\left(\bigwedge\nolimits_{1<i\le d} \psi_{i,n}\right)(b_{1,n}\wedge\cdots\wedge b_{d,n}) = \sum_{k=1}^{d}(-1)^{k+1}\det(\psi_{i,n}(b_{j,n}))_{j\neq k}\cdot b_{k,n}$$

(see [**6**, Proposition 4.1]) and so

$$\mathcal{N}_n \circ \left(\bigwedge\nolimits_{1<i\le d} \psi_{i,n}\right)(b_{1,n}\wedge\cdots\wedge b_{d,n})$$
$$= \sum_{k=1}^{d}(-1)^{k+1} b_{k,0}\otimes\det(\psi_{i,n}(b_{j,n}))_{j\neq k} \text{ in } P_0\otimes_{\mathbb{Z}_p} Q_n^{r-1}.$$

By noting

$$\psi_{i,n}(b_{j,n}) \equiv \psi_{i,0}(b_{j,0}) \pmod{I_n} \text{ for every } r<i\le d,$$

we compute

$$\left(\bigwedge\nolimits_{1<i\le r} \beta_{i,n}\right)\circ\left(\bigwedge\nolimits_{r<i\le d} \psi_{i,0}\right)(b_{1,0}\wedge\cdots\wedge b_{d,0})$$
$$= (-1)^{(r-1)(d-r)}\sum_{k=1}^{d}(-1)^{k+1} b_{k,0}\otimes\det(\psi_{i,n}(b_{j,n}))_{j\neq k} \text{ in } P_0\otimes_{\mathbb{Z}_p} Q_n^{r-1}.$$

Since we have

$$(-1)^{r-1+r(d-r)+(r-1)(d-r)} = (-1)^{d-1},$$

we therefore obtain the desired equality (7.4.9).

Acknowledgements. The third author would like to thank Kazim Büyükboduk for helpful discussions, especially about Rubin's formula. The authors would like to thank Takenori Kataoka for discussions with him and for his comments on the first draft of this paper, which were very helpful. The authors also would like to thank Christian Wuthrich for carefully reading the manuscript and giving them helpful comments.

References

[1] K. Barré-Sirieix, G. Diaz, F. Gramain and G. Philibert, Une preuve de la conjecture de Mahler-Manin, Invent. Math., **124** (1996), 1–9.

[2] D. Benois, p-adic heights and p-adic Hodge theory, Mém. Soc. Math. Fr. (N.S.), **167** (2021), vi+135 pp.

[3] D. Benois and K. Büyükboduk, On the exceptional zeros of p-non-ordinary p-adic L-functions and a conjecture of Perrin-Riou, Trans. Amer. Math. Soc., **376** (2023), 231–284.

[4] M. Bertolini, H. Darmon and R. Venerucci, Heegner points and Beilinson–Kato elements: a conjecture of Perrin-Riou, Adv. Math., **398** (2022), paper no. 108172.

[5] D. Burns and M. Flach, Tamagawa numbers for motives with (non-commutative) coefficients, Doc. Math., **6** (2001), 501–570.
[6] D. Burns, M. Kurihara and T. Sano, On zeta elements for $\mathbb{G}_m$, Doc. Math., **21** (2016), 555–626.
[7] D. Burns, M. Kurihara and T. Sano, On Iwasawa theory, zeta elements for $\mathbb{G}_m$ and the equivariant Tamagawa number conjecture, Algebra Number Theory, **11** (2017), 1527–1571.
[8] D. Burns, M. Kurihara and T. Sano, On Stark elements of arbitrary weight and their p-adic families, In: Development of Iwasawa Theory—the Centennial of K. Iwasawa's Birth, Adv. Stud. Pure Math., **86**, 2020, 113–140.
[9] D. Burns, M. Kurihara and T. Sano, On derivatives of Kato's Euler system and the Mazur–Tate Conjecture, submitted for publication, arXiv:2103.11535.
[10] D. Burns, R. Sakamoto and T. Sano, On the theory of higher rank Euler, Kolyvagin and Stark systems, III: applications, preprint, arXiv:1902.07002.
[11] D. Burns and T. Sano, On the theory of higher rank Euler, Kolyvagin and Stark systems, Int. Math. Res. Not. IMRN, **2021** (2021), 10118–10206.
[12] K. Büyükboduk, On Nekovář's heights, exceptional zeros and a conjecture of Mazur–Tate–Teitelbaum, Int. Math. Res. Not. IMRN, **2016** (2016), 2197–2237.
[13] K. Büyükboduk, Beilinson–Kato and Beilinson–Flach elements, Coleman–Rubin–Stark classes, Heegner points and a conjecture of Perrin-Riou, In: Development of Iwasawa Theory—the Centennial of K. Iwasawa's Birth, Adv. Stud. Pure Math., **86**, 2020, 141–193.
[14] K. Büyükboduk, R. Pollack and S. Sasaki, p-adic Gross–Zagier formula at critical slope and a conjecture of Perrin-Riou, preprint, arXiv:1811.08216.
[15] H. Darmon, A refined conjecture of Mazur–Tate type for Heegner points, Invent. Math., **110** (1992), 123–146.
[16] H. Darmon, Thaine's method for circular units and a conjecture of Gross, Canad. J. Math., **47** (1995), 302–317.
[17] T. Fukaya and K. Kato, A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory, In: Proceedings of the St. Petersburg Mathematical Society, Volume XII, Amer. Math. Soc. Transl. Ser. 2, **219**, 2006, 1–85.
[18] T. Fukaya and K. Kato, On conjectures of Sharifi, preprint, 2012.
[19] R. Greenberg, Iwasawa theory for p-adic representations, In: Algebraic Number Theory, Adv. Stud. Pure Math., **17**, Academic Press, Boston, MA, 1989, 97–137.
[20] R. Greenberg and G. Stevens, p-adic L-functions and p-adic periods of modular forms, Invent. Math., **111** (1993), 407–447.
[21] J. W. Jones, Iwasawa L-functions for multiplicative abelian varieties, Duke Math. J., **59** (1989), 399–420.
[22] K. Kato, Lectures on the approach to Iwasawa theory for Hasse–Weil L-functions via B_{dR}. Part I, In: Arithmetic Algebraic Geometry, (ed. E. Ballico), Lecture Notes in Math., **1553**, Springer, New York, 1993, 50–163.
[23] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, Cohomologies p-adiques et applications arithmétiques. III, Astérisque, **295** (2004), 117–290.
[24] G. Kings, The equivariant Tamagawa number conjecture and the Birch–Swinnerton-Dyer conjecture, In: Arithmetic of L-functions, IAS/Park City Math. Ser., **18**, Amer. Math. Soc., Providence, RI, 2011, 315–349.
[25] S. Kobayashi, An elementary proof of the Mazur–Tate–Teitelbaum conjecture for elliptic curves, Doc. Math., **Extra Vol.** (2006), 567–575.
[26] S. Kobayashi, The p-adic Gross–Zagier formula for elliptic curves at supersingular primes, Invent. Math., **191** (2013), 527–629.
[27] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, Invent. Math., **149** (2002), 195–224.
[28] B. Mazur and K. Rubin, Refined class number formulas for $\mathbb{G}_m$, J. Théor. Nombres Bordeaux, **28** (2016), 185–211.
[29] B. Mazur and J. Tate, Refined conjectures of the "Birch and Swinnerton-Dyer type", Duke Math. J., **54** (1987), 711–750.
[30] B. Mazur, J. Tate and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. Math., **84** (1986), 1–48.

[31] J. Nekovář, On p-adic height pairings, In: Séminaire de Théorie des Nombres, Paris, 1990–1991, Progr. Math., **108**, Birkhäuser Boston, Boston, 1993, 127–202.
[32] J. Nekovář, Selmer complexes, Astérisque, **310** (2006).
[33] B. Perrin-Riou, Points de Heegner et dérivées de fonctions L p-adiques, Invent. Math., **89** (1987), 455–510.
[34] B. Perrin-Riou, Fonctions L p-adiques d'une courbe elliptique et points rationnels, Ann. Inst. Fourier (Grenoble), **43** (1993), 945–995.
[35] J. Pottharst, Analytic families of finite slope Selmer groups, Algebra Number Theory, **7** (2013), 1571–1612.
[36] K. Rubin, Abelian varieties, p-adic heights and derivatives, In: Algebra and Number Theory (Essen, 1992), Walter de Gruyter, Berlin, 1994, 247–266.
[37] K. Rubin, Euler systems and modular elliptic curves, In: Galois Representations in Arithmetic Algebraic Geometry, London Math. Soc. Lecture Note Ser., **254**, Cambridge Univ. Press, 1998, 351–367.
[38] R. Sakamoto, The theory of Kolyvagin systems for $p = 3$, preprint.
[39] T. Sano, Refined abelian Stark conjectures and the equivariant leading term conjecture of Burns, Compositio Math., **150** (2014), 1809–1835.
[40] P. Schneider, p-adic height pairings I, Invent. Math., **69** (1982), 401–409.
[41] P. Schneider, Iwasawa L-functions of varieties over algebraic number fields. A first approach, Invent. Math., **71** (1983), 251–293.
[42] A. J. Scholl, An introduction to Kato's Euler systems, In: Galois Representations in Arithmetic Algebraic Geometry, (eds. A. J. Scholl and R. L. Taylor), London Math. Soc. Lecture Note Ser., **254**, Cambridge Univ. Press, 1998, 379–460.
[43] D. Solomon, On a construction of p-units in abelian fields, Invent. Math., **109** (1992), 329–350.
[44] R. Venerucci, p-adic regulators and p-adic families of modular forms, Ph.D. thesis, Univ. degli Studi di Milano, (2013).
[45] R. Venerucci, Exceptional zero formulae and a conjecture of Perrin-Riou, Invent. Math., **203** (2016), 923–972.

David Burns
Department of Mathematics
King's College London
London WC2R 2LS, U.K.
E-mail: david.burns@kcl.ac.uk

Masato Kurihara
Department of Mathematics
Keio University
3-14-1 Hiyoshi, Kohoku-ku
Yokohama 223-8522, Japan
E-mail: kurihara@math.keio.ac.jp

Takamichi Sano
Department of Mathematics
Osaka Metropolitan University
3-3-138 Sugimoto, Sumiyoshi-ku
Osaka 558-8585, Japan
E-mail: tsano@omu.ac.jp