Université Grenoble Alpes

ANNALES DE L'INSTITUT FOURIER

Kazuto Ota

On the rank-part of the Mazur–Tate refined conjecture for higher weight modular forms

Tome 73, n° 3 (2023), p. 1319-1364.

https://doi.org/10.5802/aif.3557

Ann. Inst. Fourier, Grenoble
73, 3 (2023) 1319-1364

ON THE RANK-PART OF THE MAZUR–TATE REFINED CONJECTURE FOR HIGHER WEIGHT MODULAR FORMS

by Kazuto OTA (*)

Abstract. — Under some assumptions, we prove the rank-part of the Mazur–Tate refined conjecture of BSD type. More concretely, we prove that the rank of the Selmer group of an elliptic modular form is less than or equal to the order of zeros of Mazur–Tate elements, or modular elements, which are elements in certain group rings constructed from special values of the associated L-function. Our main result is regarded as a generalization of our previous work on elliptic curves.

Résumé. — Sous certaines hypothèses, on prouve la partie rang de la conjecture précisée de Mazur–Tate de type BSD. Plus concrètement, on prouve que le rang du groupe de Selmer d'une forme modulaire elliptique est inférieur ou égal à l'ordre des zéros des éléments de Mazur–Tate, qui sont des éléments de certains algèbres de groupes construits à partir de valeurs spéciales de la fonction L associée. Notre résultat principal est considéré comme une généralisation de nos travaux antérieurs sur les courbes elliptiques.

1. Introduction

In an earlier paper [26], under relatively mild assumptions we proved the rank-part of the Mazur–Tate refined conjecture for elliptic curves (cf. [22]). The aim of this paper is to generalize the previous work to modular forms of higher weight.

To state our main result, we fix some notation. Let $f(\tau) \in S_k(\Gamma_0(N))$ be a normalized eigen newform of even weight k for $\Gamma_0(N)$, whose q-expansion

Keywords: Mazur–Tate refined conjectures, elliptic modular forms, p-adic L-functions.
2020 *Mathematics Subject Classification:* 11G40, 11F11, 11R23.
(*) This research was supported by KAKENHI 17K14173. This research was also supported in part by KAKENHI 26247004, as well as the JSPS Core-to-Core program "Foundation of a Global Research Cooperative Center in Mathematics focused on Number Theory and Geometry" and the KiPAS program 2013–2018 of the Faculty of Science and Technology at Keio University.

we denote by $\sum_{n\geqslant 1} a_n q^n$. Let p be a prime not dividing $2N$, and fix embeddings $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ and $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Let $F_\mathfrak{p}$ be the completion of the Hecke field $F = \mathbb{Q}(a_n; n \geqslant 1)$ at the prime $\mathfrak{p} \mid p$ induced by ι_p. We denote by $V_f \cong F_\mathfrak{p}^{\oplus 2}$ the Galois representation attached to f (cf. Section 2.1). Let T_f be an $\mathscr{O}_\mathfrak{p}$-lattice of V_f stable under the $G_\mathbb{Q}$-action, where $\mathscr{O}_\mathfrak{p}$ denotes the ring of integers in $F_\mathfrak{p}$. We denote by $\rho_f : G_\mathbb{Q} \to \mathrm{Aut}_{\mathscr{O}_\mathfrak{p}}(T_f)$ the associated representation. We put $A = T_f(k/2) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, where $(k/2)$ denotes the $k/2$-th Tate twist. We assume the following (see Remark 1.2 for the validity of the assumption).

Assumption A.

(1) $\mathrm{H}^0(\mathbb{Q}_p, A[\mathfrak{p}]) = \{0\}$.
(2) *Fixing an $\mathscr{O}_\mathfrak{p}$-basis of T_f, we have*

$$\mathrm{Im}(\rho_f) \supseteq \left\{ g \in \mathrm{GL}_2(\mathbb{Z}_\mathfrak{p}) \,\middle|\, \det(g) \in (\mathbb{Z}_p^\times)^{k-1} \right\}.$$

(3) *For each prime $l \mid N$, either* $\mathrm{H}^0(\mathbb{Q}_l, A)$ *or* $\mathrm{H}^1\left(\mathbb{F}_l, \mathrm{H}^0(\mathbb{Q}_l^{\mathrm{ur}}, A)/(\mathrm{div.})\right)$ *is the zero module, where* (div.) *denotes the maximal divisible part.*

In this section, for simplicity we assume that $F_\mathfrak{p}/\mathbb{Q}_p$ is unramified and that if f is ordinary (i.e. $a_p \in \mathscr{O}_\mathfrak{p}^\times$) then $a_p \in \mathbb{Z}_p$ and $a_p \not\equiv 1 \bmod p$ (those assumptions are imposed to verify Assumptions B and C). For a positive integer S, we put $\zeta_S = e^{2\pi i/S}$ (the S-th root of unity) and denote by Γ_S the p-Sylow subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_S)/\mathbb{Q})$. We denote by $\theta_S \in \mathscr{O}_\mathfrak{p}[\Gamma_S]$ the Mazur–Tate element (cf. Definition 2.3) which interpolates algebraic parts of the special values $L(f, \chi, k/2)$ for Dirichlet characters $\chi : \Gamma_S \to \overline{\mathbb{Q}}^\times$. We put $r_f = \mathrm{corank}_{\mathscr{O}_\mathfrak{p}}(\mathrm{Sel}(\mathbb{Q}, A))$, where $\mathrm{Sel}(\mathbb{Q}, A)$ is the Bloch–Kato Selmer group. The following is the main result (see Theorems 7.2 and 7.4 for the general case).

Theorem 1.1. — *Let S be a positive integer relatively prime to pN such that for each prime $l \mid S$,*

$$\mathrm{H}^0(\mathbb{Q}_l, A[\mathfrak{p}]) \text{ is isomorphic to } \mathscr{O}_\mathfrak{p}/\mathfrak{p} \text{ or } \{0\}. \tag{1.1}$$

Let n be a non-negative integer. Assume at least one of the following two conditions holds.

(a) *We have $n \leqslant 2$, and for every prime $l \mid S$ we have $p^2 \nmid (l-1)$.*
(b) *The p-parity conjecture holds, that is,* $\mathrm{ord}_{s=k/2}(L(f,s)) \equiv r_f \bmod 2$.

Then, we have

$$\theta_{Sp^n} \in I_{Sp^n}^{\min\{r_f, p\}},$$

where I_{Sp^n} denotes the augmentation ideal of $\mathscr{O}_\mathfrak{p}[\Gamma_{Sp^n}]$.

Remark 1.2.

(1) Even in the case where $F = \mathbb{Q}$ and $k = 2$ (i.e. the newform f corresponds to an elliptic curve over $\mathbb{Q}$), the theorem above is still stronger than [26, Theorem 5.17]. The reason is that in loc. cit. we considered θ_{Sp^n} with $n \leqslant 1$, assuming that p did not divide the product of Tamagawa factors, which is slightly stronger than Assumption A (3).

(2) If either f corresponds to an elliptic curve or f is ordinary, then the p-parity conjecture holds (cf. [11, 25]).

(3) By Ribet [30], if f has no complex multiplication, then for almost all primes p, Assumption A (2) is verified.

(4) By Chebotarev's density theorem, the density of primes l satisfying (1.1) is greater than or equal to $1 - \left((p^3 - p)|(\mathbb{F}_p^\times)^{k-1}|\right)^{-1}$ (cf. Proposition 3.9).

(5) See Proposition 3.7 for Assumption A (1). For $l \mid N$, if $a_l = 0$ and $p \geqslant 5$, then $\mathrm{H}^0(\mathbb{Q}_l^{\mathrm{ur}}, A[\mathfrak{p}]) = 0$ (cf. Proposition 3.8).

(6) We mention known results related to the theorem for $k > 2$ (see [26, §1] for $k = 2$). Kato's result [13] on the p-adic BSD conjecture implies that if f is ordinary, then for $n \geqslant 0$, $\theta_{p^n} \in I_{p^n}^{r_f}$. In the case where f is non-ordinary, an unpublished work of Emerton–Pollack–Weston implies that $\theta_{p^n} \in I_{p^n}^{r_f}$. Results of Kurihara also imply that if f is ordinary, then $\theta_{Sp^n} \in I_{Sp^n}^{r_f}$ for general S relatively prime to pN, under assumptions including the validity of $\mu = 0$ conjectures and the non-existence of finite submodules of Iwasawa modules associated to Selmer groups (see [17] for the details).

(7) The Mazur–Tate refined conjecture which we consider is over cyclotomic extensions. There are also works on anticylotomic extensions (cf. [8, 12, 14, 20]).

Our proof of Theorem 1.1 is similar to that of [26, Theorem 5.17] (cf. [26, §1.3]). The key ingredients of the previous proof were the following: (a) modification of Darmon's argument on Heegner points in [8] to Kato's Euler system, (b) construction of local points (as in [15, 16, 27]) of elliptic curves relating Mazur–Tate elements with Kato's Euler system via cup products.

Compared to the proof of [26, Theorem 5.17], one of the new parts of this paper is that we slightly refine the argument on derivatives of Euler systems so that we can consider θ_{Sp^n} with $n \geqslant 2$ (cf. Section 5). Another part is that by using Perrin-Riou's theory, we generalize local points of Otsuki [27] to modular forms of higher weight (cf. Section 6).

Considering $\{\theta_{Sp^n}\}_{n\geqslant 1}$ leads us to the following result on the p-adic L-functions which also interpolate special values of the L-functions twisted by characters whose conductor are divisible by integers prime to p.

Theorem 1.3 (Corollary 7.5). — *With the same notation and assumption as in Theorem 1.1, assume further that f is ordinary. Let $\mathscr{L}_{p,S,\alpha}(f) \in \mathscr{O}_{\mathfrak{p}}[\![G_\infty]\!][\Gamma_S]$ denote the p-adic L-function (see Proposition 6.13 and Remark 6.14(1) for the details), where $G_\infty = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$. Then,*

$$\mathscr{L}_{p,S,\alpha}(f) \in I_{\infty,S,k/2}^{\min\{r_f,p\}},$$

where $I_{\infty,S,k/2} \subseteq \mathscr{O}_{\mathfrak{p}}[\![G_\infty]\!][\Gamma_S]$ denotes the kernel of the homomorphism of $\mathscr{O}_{\mathfrak{p}}$ algebras $\mathscr{O}_{\mathfrak{p}}[\![G_\infty]\!][\Gamma_S] \to \mathscr{O}_{\mathfrak{p}}$ induced by the product $\kappa_{\mathrm{cyc}}^{k/2} \cdot \mathbf{1}_S$. Here, $\kappa_{\mathrm{cyc}} : G_\infty \xrightarrow{\sim} \mathbb{Z}_p^\times$ denotes the p-adic cyclotomic character, and $\mathbf{1}_S$ denotes the trivial character of Γ_S.

Remark 1.4.

(1) We note that the work of Kato [13] and Kurihara [17] mentioned in Remark 1.2(6) also imply similar results under their corresponding setting explained above.
(2) The elements θ_S and $\mathscr{L}_{p,S,\alpha}(f)$ rely on the choice of periods $\Omega^\pm$, which are independent of S. We briefly explain our choice. Throughout this paper, we first fix an element $\delta_f = \delta_f^+ + \delta_f^-$ of V_f which is *good* for T_f in the sense of [13, §17.5] (see also Definition 2.1), and the data δ_f specifies Kato's Euler system. Fixing δ_f, the choice of periods is essentially equivalent to that of a nonzero element $\omega \in \mathrm{Fil}^1 D_{\mathrm{cris}}(V_f)$ (cf. Definition 2.1 or [13, Theorem 16.2]). We choose ω so that by Perrin-Riou's theory (cf. [28]) we may obtain a system of certain *integral* maps (regarded as analogues of Coleman maps), by which we connect Kato's Euler system to the Mazur–Tate elements (cf. (7.1)). We refer the reader to Definition 6.6 for details. We note that in the good ordinary case, by [13, §17], we may take ω to be *good* for T_f in the sense of [13, §17.5]. We also note that since our ω may not be necessarily the differential form associated to f under the canonical isomorphism from the f-part of the de Rham cohomology group of $X_1(N)$ to $D_{\mathrm{cris}}(V_f)$, the μ-invariant of our $\mathscr{L}_{p,1,\alpha}(f)$ may differ from those of the p-adic L-functions associated to so-called canonical periods.

We also prove a result on exceptional zeros of Mazur–Tate elements. We refer the reader to Theorem 7.3 for the details.

Acknowledgements

The author is grateful to Shinichi Kobayashi for discussion and for sharing his insight about Perrin-Riou's theory. He would like to thank Chan-Ho Kim and Tatsuya Ohshita for discussion on cohomology groups attached to modular forms. He also thanks Kâzim Büyükboduk for a useful comment on the Selmer groups. Thanks are also due to the referee for valuable comments.

2. Mazur–Tate elements

In this section, we fix the notation and recall Mazur–Tate elements.

2.1. Setup

Let $f(\tau) \in S_k(\Gamma_0(N))$ be a normalized eigen newform of even weight k, whose q-expansion we denote by $\sum_{n\geqslant 1} a_n q^n$. We assume that f has no complex multiplication. Let p be a prime not dividing $2N$, and fix embeddings $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ and $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. We denote by F the Hecke field $\mathbb{Q}(a_n; n \geqslant 1)$ and write $\mathscr{O}$ for the ring of integers in F. Let $\mathfrak{p}$ be the prime of F above p induced by ι_p. Let $F_\mathfrak{p}$ be the completion of F at $\mathfrak{p}$ and $\mathscr{O}_\mathfrak{p}$ the ring of integers in $F_\mathfrak{p}$. For a commutative F-algebra R, we let $V_R(f)$ be the free R-module of rank two that is introduced in [13, §6.3] and is constructed from cohomology groups of modular curves. Then, $V_f := V_{F_\mathfrak{p}}(f)$ has an action of $G_\mathbb{Q}$ (cf. [13, §8.3]) and is isomorphic to Deligne's Galois representation associated to f, where we denote by G_L the absolute Galois group of a perfect field L. We recall that for a prime $l \nmid pN$,

$$\det(1 - \mathrm{Fr}_l^{-1} X | V_f) = 1 - a_l X + l^{k-1} X^2,$$

where Fr_l is the arithmetic Frobenius at l. Let T_f be an $\mathscr{O}_\mathfrak{p}$-lattice of V_f stable under the $G_\mathbb{Q}$-action such that

$$T_f \subseteq V_{\mathscr{O}_\mathfrak{p}}(f), \quad \frac{1}{\varpi} T_f \not\subseteq V_{\mathscr{O}_\mathfrak{p}}(f),$$

where $\varpi \in \mathscr{O}_\mathfrak{p}$ denotes a uniformizer, and we refer the reader to [13, §8.3] for $V_{\mathscr{O}_\mathfrak{p}}(f)$. If we put $\mathscr{O}_{F,(p)} = F \cap \mathscr{O}_\mathfrak{p}$, then the intersection $T_f \cap V_F(f)^\pm$ inside $V_{F_\mathfrak{p}}(f)$ is an $\mathscr{O}_{F,(p)}$-module free of rank one, where $V_F(f)^\pm$ denotes the eigenspace with eigenvalue ± 1 of the complex conjugation. Let $S(f)$

be the F-vector subspace of $S_k(\Gamma_0(N))$ generated by f. Then, we have the period map of f

$$\mathrm{per}_f : S(f) \to V_{\mathbb{C}}(f)$$

as in [13, §6.3].

Definition 2.1. — *Throughout this paper, we fix an $\mathscr{O}_{F,(p)}$-basis $\delta_f^{\pm}$ of $T_f \cap V_F(f)^{\pm}$. For a non-zero element ω of $S(f)$, we define periods $\Omega_\omega^{\pm} \in \mathbb{C}^\times$ by*

$$\mathrm{per}_f(\omega) = \Omega_\omega^+ \delta_f^+ + \Omega_\omega^- \delta_f^-.$$

2.2. Mazur–Tate elements

Let $L(f,s) = \sum_{n\geqslant 1} a_n n^{-s}$ be the L-function attached to f. For a Dirichlet character χ, we put $L(f,\chi,s) = \sum_{n\geqslant 1} \chi(n) a_n n^{-s}$. Let ω be a non-zero element of $S(f)$. Then, for $1 \leqslant i \leqslant k-1$, $(2\pi\sqrt{-1})^{k-i-1} L(f,\chi,i)/\Omega_\omega^{\pm} \in F(\chi)$, where $\pm$ corresponds to the sign of $(-1)^{k-i-1}\chi(-1) = (-1)^{i-1}\chi(-1)$.

For a polynomial $P(z) \in \mathbb{C}[z]$ whose degree is at most $k-2$ and for $a, S \in \mathbb{Q}$ with $S > 0$, we denote by $\lambda(f, P(z); -a, S) \in \mathbb{C}$ the modular symbol as in [23, §3]. By [23, (8.6)] for a Dirichlet character χ of conductor S and $1 \leqslant i \leqslant k-1$,

$$\sum_{a\in(\mathbb{Z}/S\mathbb{Z})^\times} \lambda(f, z^{i-1}; -a, S)\chi(a) = S^{i-1}(i-1)!\tau(\chi)\frac{L(f,\chi^{-1},i)}{(-2\pi\sqrt{-1})^{i-1}}, \tag{2.1}$$

where we define $\tau(\chi) = \sum_{\gamma\in G_S} \chi(\gamma)\zeta_S^{\gamma}$. For $a \in \mathbb{Z}$, a positive integer S and $1 \leqslant i \leqslant k-1$, we define $[a/S]_{i,\omega}^{\pm} \in F$ by

$$\left[\frac{a}{S}\right]_{i,\omega}^{\pm} = (-2\pi\sqrt{-1})^{k-2}\frac{\lambda(f, z^{i-1}; -a, S) \pm (-1)^{i-1}\lambda(f, z^{i-1}; a, S)}{2\Omega_\omega^{\pm}}.$$

Then, we have $[-a/S]_{i,\omega}^{\pm} = \pm(-1)^{i-1}[a/S]_{i,\omega}^{\pm}$. We define

$$\vartheta_{S,i,\omega} = \sum_{a\in(\mathbb{Z}/S\mathbb{Z})^\times}\left(\left[\frac{a}{S}\right]_{i,\omega}^{+} + \left[\frac{a}{S}\right]_{i,\omega}^{-}\right)\mathrm{Fr}_a \in F[G_S],$$

where $G_S = \mathrm{Gal}(\mathbb{Q}(\zeta_S)/\mathbb{Q})$, and $\mathrm{Fr}_a \in G_S$ denotes the element such that $\mathrm{Fr}_a(\zeta_S) = \zeta_S^a$.

For $n \mid m$ and a commutative ring R, we denote by $\pi_{m/n} : R[G_m] \to R[G_n]$ the homomorphism of R-algebras induced by the natural surjection $G_m \to G_n$. We also denote by $\nu_{m,n}$ the R-linear map $R[G_n] \to R[G_m]$ induced by

$$\sigma \mapsto \sum_{\tau\in G_m,\ \tau\mapsto\sigma} \tau \quad \text{for } \sigma \in G_n.$$

Proposition 2.2.

(1) *Let S be a positive integer and l a prime. Then,*

$$\pi_{Sl/S}(\vartheta_{Sl,i,\omega}) = \begin{cases} -\operatorname{Fr}_l l^{i-1}(1 - a_l l^{1-i}\operatorname{Fr}_l^{-1} + \epsilon(l) l^{k-2i}\operatorname{Fr}_l^{-2})\vartheta_{S,i,\omega} & (l \nmid S), \\ a_l\vartheta_{S,i,\omega} - \epsilon(l) l^{k-2}\nu_{S,Sl}(\vartheta_{S/l,i,\omega}) & (l \mid S), \end{cases}$$

where ϵ is the trivial Dirichlet character modulo N.

(2) *For a character χ of G_S with conductor S, we have*

$$\chi(\vartheta_{S,i,\omega}) = S^{i-1}(i-1)!\tau(\chi)(-2\pi\sqrt{-1})^{k-i-1}\frac{L(f,\chi^{-1},i)}{\Omega_\omega^\pm},$$

where the sign $\pm$ denotes that of $(-1)^{k-i-1}\chi(-1)$.

Proof.

(1). — We put

$$\Theta_S^\pm = \sum_{a\in(\mathbb{Z}/S\mathbb{Z})^\times} \lambda(f, z^{i-1}; \pm a, S)\operatorname{Fr}_a \in \mathbb{C}[G_S].$$

Then,

$$\pi_{Sl/S}(\Theta_{Sl}^\pm) = \sum_{a\in(\mathbb{Z}/S\mathbb{Z})^\times}\ \sum_{\substack{b\in(\mathbb{Z}/Sl\mathbb{Z})^\times \\ b\equiv a \bmod S}} \lambda(f, z^{i-1}; \pm b, Sl)\operatorname{Fr}_a. \tag{2.2}$$

We first consider the case where $l \nmid S$. Let $x, y \in \mathbb{Z}$ such that $xS + ly = 1$. For an integer a relatively prime to S, we put $e_a = ayl$, whose image in $\mathbb{Z}/Sl\mathbb{Z}$ is a unique element such that $e_a \equiv a \bmod S$ and $e_a \equiv 0 \bmod l$. By [23, (3.1) and §4], we have

$$\begin{aligned}
&\sum_{\substack{b\in(\mathbb{Z}/Sl\mathbb{Z})^\times \\ b\equiv a \bmod S}} \lambda(f, z^{i-1}; \pm b, Sl) \\
&= \sum_{\substack{b\in\mathbb{Z}/Sl\mathbb{Z} \\ b\equiv a \bmod S}} \lambda(f, z^{i-1}; \pm b, Sl) - \lambda(f, z^{i-1}; \pm e_a, Sl) \\
&= \sum_{u=0}^{l-1} \lambda(f, z^{i-1}; \pm a - uS, Sl) - \lambda(f, z^{i-1}; \pm ayl, Sl) \\
&= a_l\lambda(f, z^{i-1}; \pm a, S) - \epsilon(l) l^{k-2}\lambda(f, z^{i-1}; \pm a, S/l) - \lambda(f, z^{i-1}; \pm ayl, Sl) \\
&= a_l\lambda(f, z^{i-1}; \pm a, S) - \epsilon(l) l^{k-2}\lambda(f, (z/l)^{i-1}; \pm al, S) \\
&\qquad - \lambda(f, l^{i-1}(z/l)^{i-1}; \pm ayl, Sl) \\
&= a_l\lambda(f, z^{i-1}; \pm a, S) - \epsilon(l) l^{k-1-i}\lambda(f, z^{i-1}; \pm al, S) - l^{i-1}\lambda(f, z^{i-1}; \pm ay, S).
\end{aligned}$$

By (2.2) and noting that $yl \equiv 1 \mod S$, we have

$$\begin{aligned}\pi_{Sl/S}(\Theta_S^{\pm}) &= (a_l - \epsilon(l)l^{k-1-i}\operatorname{Fr}_l^{-1} - l^{i-1}\operatorname{Fr}_l)\Theta_S^{\pm} \\ &= -\operatorname{Fr}_l(l^{i-1} - a_l\operatorname{Fr}_l^{-1} + \epsilon(l)l^{k-1-i}\operatorname{Fr}_l^{-2})\Theta_S^{\pm},\end{aligned}$$

which implies the assertion (1) in the case where $l \nmid S$.

We next assume that $l \mid S$. Then, by [23, §4] we have

$$\begin{aligned}\sum_{\substack{b\in(\mathbb{Z}/Sl\mathbb{Z})^\times \\ b\equiv a \bmod S}} \lambda(f, z^{i-1}; \pm b, Sl) &= \sum_{u=0}^{l-1}\lambda(f, z^{i-1}; \pm a - uS, Sl) \\ &= a_l\lambda(f, z^{i-1}; \pm a, S) - \epsilon(l)l^{k-2}\lambda(f, z^{i-1}; \pm a, S/l).\end{aligned}$$

By (2.2) we have

$$\begin{aligned}&\pi_{S\ell/S}(\Theta_{S\ell}^{\pm}) \\ &\quad= \sum_{a\in(\mathbb{Z}/S\mathbb{Z})^\times}\big(a_l\lambda(f, z^{i-1}; \pm a, S) - \epsilon(l)l^{k-2}\lambda(f, z^{i-1}; \pm a, S/l)\big)\operatorname{Fr}_a \\ &\quad= \sum_{a\in(\mathbb{Z}/S\mathbb{Z})^\times} a_l\lambda(f, z^{i-1}; \pm a, S)\operatorname{Fr}_a \\ &\qquad\quad - \epsilon(l)l^{k-2}\sum_{a\in(\mathbb{Z}/Sl^{-1}\mathbb{Z})^\times}\sum_{\substack{b\in(\mathbb{Z}/S\mathbb{Z})^\times \\ b\mapsto a}}\lambda(f, z^{i-1}; \pm a, S/l)\operatorname{Fr}_b \\ &\quad= a_\ell\Theta_S^{\pm} - \epsilon(l)l^{k-2}\nu_{S,S\ell}(\Theta_{S/\ell}^{\pm}),\end{aligned}$$

which implies the assertion (1).

(2). — It follows from (2.1) and straightforward computation. □

Definition 2.3. — *For a positive integer S, we denote by Γ_S the p-Sylow subgroup of G_S. For $1 \leqslant i \leqslant k-1$ and $\omega \in S(f) \setminus \{0\}$, we define the* Mazur–Tate element *$\theta_{S,i,\omega}$ of $F[\Gamma_S]$ as the image of $\vartheta_{S,i,\omega}$ in $F[\Gamma_S]$. We put $\theta_{S,\omega} = \theta_{S,\frac{k}{2},\omega}$.*

Conjecture 2.4. — *Let $S > 0$, and suppose that ω is a non-zero element of $S(f)$ such that $\theta_{S,\omega} \in \mathscr{O}_{F,(p)}[\Gamma_S]$. Then, $\theta_{S,\omega} \in I_S^{r_f}$, where we recall that r_f is the $\mathscr{O}_\mathfrak{p}$-corank of the Bloch–Kato Selmer group $\mathrm{Sel}(\mathbb{Q}, T_f(k/2) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$.*

2.3. Functional equation of Mazur–Tate elements

We recall the functional equation of Mazur–Tate elements, which plays an important role in the proof of Theorem 1.1 with the assumption that the p-parity conjecture holds.

Let w_N be the operator on $S_k(\Gamma_0(N))$ defined as $g(\tau) \mapsto \frac{N^{k/2}}{(N\tau)^k} g\left(\frac{-1}{N\tau}\right)$. Then there exists $\varepsilon_f \in \{\pm 1\}$ such that $w_N(f) = \varepsilon_f f$. It is known that

$$(-1)^{\frac{k}{2}} \varepsilon_f = (-1)^{\mathrm{ord}_{s=k/2}(L(f,s))} \tag{2.3}$$

(see [10, Theorem 5.10.2] for example). Let S be a positive integer relatively prime to N. To simplify the notation, we put $[a/S]^{\pm} = [a/S]^{\pm}_{\frac{k}{2},\omega}$, $\vartheta_S = \vartheta_{S,k/2,\omega}$, and $\theta_S = \theta_{S,k/2,\omega}$. By [23, Chapter 1, §6], for an integer a relatively prime to S, we have

$$\left[\frac{a}{S}\right]^{\pm} = (-1)^{k/2} \varepsilon_f \left[\frac{a'}{S}\right]^{\pm}, \tag{2.4}$$

where a' is any integer satisfying $a'aN \equiv -1 \bmod S$. Let ι be the homomorphism of $F_{\mathfrak{p}}$-algebras $F_{\mathfrak{p}}[G_S] \to F_{\mathfrak{p}}[G_S]$ sending $\sigma \in G_S$ to σ^{-1}. We have the *functional equation* of θ_S as follows.

Proposition 2.5. — *For a positive integer S relatively to N,*

$$\vartheta_S = (-1)^{\frac{k}{2}} \varepsilon_f \operatorname{Fr}_{-N}^{-1} \iota(\vartheta_S), \quad \theta_S = (-1)^{\frac{k}{2}} \varepsilon_f \operatorname{Fr}_{-N}^{-1} \iota(\theta_S).$$

Proof. — Since θ_S is the image of ϑ_S under $F_{\mathfrak{p}}[G_S] \to F_{\mathfrak{p}}[\Gamma_S]$, the second equality follows from the first one, which follows from the computation

$$\begin{aligned}(-1)^{k/2}\varepsilon_f \operatorname{Fr}_{-N}^{-1} \iota(\vartheta_S) &= (-1)^{k/2}\varepsilon_f \operatorname{Fr}_{-N}^{-1} \sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \left(\left[\frac{a}{S}\right]^+ + \left[\frac{a}{S}\right]^-\right) \operatorname{Fr}_a^{-1} \\ &= (-1)^{k/2}\varepsilon_f \sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \left(\left[\frac{a}{S}\right]^+ + \left[\frac{a}{S}\right]^-\right) \operatorname{Fr}_{-aN}^{-1} \\ &\overset{\text{(a)}}{=} \sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \left(\left[\frac{a'}{S}\right]^+ + \left[\frac{a'}{S}\right]^-\right) \operatorname{Fr}_{a'} = \vartheta_S.\end{aligned}$$

Here, the equation (a) follows from (2.4). □

3. Preliminaries on Galois cohomology

In the rest of this paper, we write

$$T = T_f(k/2), \quad V = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, \quad A = \operatorname{Hom}(T, F_{\mathfrak{p}}/\mathscr{O}_{\mathfrak{p}}(1)) \cong V/T,$$

where the last isomorphism is due to the natural $G_{\mathbb{Q}}$-equivariant isomorphism $\mathrm{Hom}_{\mathfrak{p}}(V_f, F_{\mathfrak{p}}) \cong V_f(k-1)$ induced by the Poincaré duality. The aim of this section is to review some basic properties of associated Galois cohomology groups.

3.1. Global cohomology groups

Lemma 3.1. — *Under Assumption A (2), for a finite abelian p-extension K of $\mathbb{Q}$, the restriction $\bar{\rho}|_{G_K}$ of the residual representation $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{Aut}_{k_{\mathfrak{p}}}(T \otimes k_{\mathfrak{p}})$ is absolutely irreducible as a G_K-module, where $k_{\mathfrak{p}}$ is the residue filed of $\mathscr{O}_{\mathfrak{p}}$.*

Proof. — Since T is free of rank two and $k_{\mathfrak{p}}$ is of odd characteristic, we are reduced to showing that the image of $\bar{\rho} : G_K \to \mathrm{Aut}_{k_{\mathfrak{p}}}(T \otimes k_{\mathfrak{p}}) \cong \mathrm{GL}_2(k_{\mathfrak{p}})$ contains $a_1 \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $a_2 \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ for some $a_1, a_2 \in k_{\mathfrak{p}}^{\times}$. Since $k-1$ is odd and $|\mathbb{F}_p^{\times}|$ is even, we have $-1 \in (\mathbb{F}_p^{\times})^{k-1} \neq \{1\}$. Hence, by Assumption A (2), $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ are contained in the image of $\bar{\rho}_f(G_{\mathbb{Q}})$, where $\bar{\rho}_f : G_{\mathbb{Q}} \to \mathrm{Aut}(T_f \otimes k_{\mathfrak{p}}) \cong \mathrm{GL}_2(k_{\mathfrak{p}})$ is the residual representation of ρ_f. Since $[K : \mathbb{Q}]$ is odd and since the orders of the matrices above are powers of two, they are contained in $\bar{\rho}_f(G_K)$. By the Chebotarev density, there exist primes $\mathfrak{l}_1$ and $\mathfrak{l}_2$ of K relatively prime to pN such that $\bar{\rho}_f(\mathrm{Fr}_{\mathfrak{l}_1}) = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $\bar{\rho}_f(\mathrm{Fr}_{\mathfrak{l}_2}) = \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, where $\mathrm{Fr}_{\mathfrak{l}_i}$ are the arithmetic Frobenius at $\mathfrak{l}_i$. Since $T \otimes k_{\mathfrak{p}} = (T_f \otimes k_{\mathfrak{p}})(k/2)$, by putting $a_i = \kappa_{\mathrm{cyc}}^{k/2}(\mathrm{Fr}_{\mathfrak{l}_i})$, we deduce the lemma. □

Proposition 3.2. — *Under Assumption A (2), for a power $\mathfrak{q}$ of $\mathfrak{p}$ and a finite abelian p-extension K of $\mathbb{Q}$, we have $\mathrm{H}^0(K, T/\mathfrak{q}) = \{0\}$, and the restriction map induces an isomorphism $\mathrm{H}^1(\mathbb{Q}, T/\mathfrak{q}) \cong \mathrm{H}^0(K/\mathbb{Q}, \mathrm{H}^1(K, T/\mathfrak{q}))$.*

Proof. — By Lemma 3.1, $\mathrm{H}^0(K, T/\mathfrak{p}) = \{0\}$. Then the proposition follows from the inflation-restriction sequence. □

3.2. Selmer groups

If l is a prime and if K is a finite extension of $\mathbb{Q}_l$, then we put

$$\mathrm{H}^1_{\mathrm{f}}(K, V) = \begin{cases} \mathrm{Ker}\left(\mathrm{H}^1(K, V) \to \mathrm{H}^1(K, V \otimes_{\mathbb{Q}_p} B_{\mathrm{cris}})\right) & (l = p), \\ \mathrm{H}^1_{\mathrm{ur}}(K, V) & (l \neq p), \end{cases}$$

where $\mathrm{H}^1_{\mathrm{ur}}(K, -) := \mathrm{Ker}(\mathrm{H}^1(K, -) \to \mathrm{H}^1(K^{\mathrm{ur}}, -))$. Here K^{ur} is the maximal unramified extension of K. We denote by $\mathrm{H}^1_{\mathrm{f}}(K, T)$ the preimage of

$\mathrm{H}^1_{\mathrm{f}}(K,V)$ under the natural map $\mathrm{H}^1(K,T)\to\mathrm{H}^1(K,V)$, and we denote by $\mathrm{H}^1_{\mathrm{f}}(K,T/\mathfrak{p}^n)$ the image of $\mathrm{H}^1_{\mathrm{f}}(K,T)$ under the natural map $\mathrm{H}^1(K,T)\to\mathrm{H}^1(K,T/\mathfrak{p}^n)$. We also denote by $\mathrm{H}^1_{\mathrm{f}}(K,A)$ the image of $\mathrm{H}^1_{\mathrm{f}}(K,V)$ under the natural map $\mathrm{H}^1(K,V)\to\mathrm{H}^1(K,A)$. We recall that $\mathrm{H}^1_{\mathrm{f}}(K,A)$ coincides with the orthogonal complement of $\mathrm{H}^1_{\mathrm{f}}(K,T)$ under the perfect pairing

$$\mathrm{H}^1(K,T)\times\mathrm{H}^1(K,A)\to\mathrm{H}^2(K,F_{\mathfrak{p}}/\mathscr{O}_{\mathfrak{p}}(1))=F_{\mathfrak{p}}/\mathscr{O}_{\mathfrak{p}}.$$

We denote by $\mathrm{H}^1_{\mathrm{f}}(K,A[\mathfrak{p}^n])$ the preimage of $\mathrm{H}^1_{\mathrm{f}}(K,A)$ under $\mathrm{H}^1(K,A[\mathfrak{p}^n])\to\mathrm{H}^1(K,A)$. For $M\in\{V,T,A,A[\mathfrak{p}^m],T/\mathfrak{p}^m\}$, we put

$$\mathrm{H}^1_{/\mathrm{f}}(K,M)=\frac{\mathrm{H}^1(K,M)}{\mathrm{H}^1_{\mathrm{f}}(K,M)}.$$

For a finite extension L of $\mathbb{Q}$ and a place λ of L, we denote by $\mathrm{loc}_\lambda:\mathrm{H}^1(L,M)\to\mathrm{H}^1(L_\lambda,M)$ the localization map, where L_λ denotes the completion at λ. We define $\mathrm{loc}_{/\mathrm{f},\lambda}$ as the composite

$$\mathrm{loc}_{/\mathrm{f},\lambda}:\mathrm{H}^1(L,M)\xrightarrow{\mathrm{loc}_\lambda}\mathrm{H}^1(L_\lambda,M)\to\mathrm{H}^1_{/\mathrm{f}}(L_\lambda,M).$$

Definition 3.3. — *Let M be one of $A,T,V,A[\mathfrak{p}^n]$ and $T/\mathfrak{p}^n$. We define the Selmer group* $\mathrm{Sel}(\mathbb{Q},M)$ *by*

$$\mathrm{Sel}(\mathbb{Q},M)=\mathrm{Ker}\left(\mathrm{H}^1(\mathbb{Q},M)\xrightarrow{\prod\mathrm{loc}_{/\mathrm{f},l}}\prod_{l:\mathrm{primes}}\mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}_l,M)\right),$$

and for a positive integer S we define a subgroup $\mathrm{H}^1_{\mathrm{f},S}(\mathbb{Q},M)$ of $\mathrm{Sel}(\mathbb{Q},M)$ *by*

$$\mathrm{H}^1_{\mathrm{f},S}(\mathbb{Q},M)=\mathrm{Ker}\left(\mathrm{Sel}(\mathbb{Q},M)\to\bigoplus_{l\mid S}\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l,M)\right),\tag{3.1}$$

where l ranges over all the primes dividing S.

3.3. Local cohomology groups

For a finite extension L of $\mathbb{Q}$ or $\mathbb{Q}_l$ for some prime l, and for $n\geqslant 0$, by taking Galois cohomology of the exact sequence

$$0\to A[\mathfrak{p}^n]\to A\xrightarrow{\times\varpi^n}A\to 0,$$

where ϖ is a uniformizer of $F_{\mathfrak{p}}$, we have that the natural homomorphism $\iota_n:\mathrm{H}^1(L,A[\mathfrak{p}^n])\to\mathrm{H}^1(L,A)[\mathfrak{p}^n]$ is surjective, and $\mathrm{Ker}(\iota_n)\cong\mathrm{H}^0(L,A)/\mathfrak{p}^n$.

Lemma 3.4. — *Let $l\neq p$ be a prime. Then, the following assertions hold.*

(1) $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l, V) = \{0\}$.
(2) *For* $n \geqslant 0$, *we have* $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l, A[\mathfrak{p}^n]) \cong \mathrm{H}^0(\mathbb{Q}_l, A)/\mathfrak{p}^n$. *In particular, if* $\mathrm{H}^0(\mathbb{Q}_l, A[\mathfrak{p}]) = \{0\}$, *then* $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l, A[\mathfrak{p}^n]) = \{0\}$.

Proof. — The assertion (1) is proved by combining [31, Corollary 1.3.3] and [24, Proposition 3.1]. By (1), we have

$$\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l, A[\mathfrak{p}^n]) = \mathrm{Ker}\left(\mathrm{H}^1(\mathbb{Q}_l, A[\mathfrak{p}^n]) \to \mathrm{H}^1(\mathbb{Q}_l, A)\right),$$

which is isomorphic to $\mathrm{H}^0(\mathbb{Q}_l, A)/\mathfrak{p}^n$. □

Lemma 3.5. — *The following hold.*

(1) *We have* $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_p, A) \cong F_{\mathfrak{p}}/\mathscr{O}_{\mathfrak{p}}$.
(2) *If* $\mathrm{H}^0(\mathbb{Q}_p, A[\mathfrak{p}]) = \{0\}$, *then* $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_p, A[\mathfrak{p}^n]) \cong \mathscr{O}_{\mathfrak{p}}/\mathfrak{p}^n$.

Proof.

(1). — By [7, Theorem 4.1],

$$\dim_{F_{\mathfrak{p}}}\left(\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_p, V)\right) = \dim_{F_{\mathfrak{p}}}(D_{\mathrm{cris}}(V)/\,\mathrm{Fil}^0(D_{\mathrm{cris}}(V))) = 1,$$

and hence $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_p, A) \cong F_{\mathfrak{p}}/\mathscr{O}_{\mathfrak{p}}$.

(2). — If $\mathrm{H}^0(\mathbb{Q}_p, A[\mathfrak{p}]) = \{0\}$, then $\iota_n : \mathrm{H}^1(\mathbb{Q}_p, A[\mathfrak{p}^n]) \to \mathrm{H}^1(\mathbb{Q}_p, A)[\mathfrak{p}^n]$ is an isomorphism. Hence, by (1), we have $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_p, A[\mathfrak{p}^n]) \cong \mathscr{O}_{\mathfrak{p}}/\mathfrak{p}^n$. □

Lemma 3.6. — *Assume that* $\mathrm{H}^0(\mathbb{Q}, A[\mathfrak{p}]) = \mathrm{H}^0(\mathbb{Q}_p, A[\mathfrak{p}]) = \{0\}$. *Then, for* $n \geqslant 0$, ι_n *induces an isomorphism* $\mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q}, A[\mathfrak{p}^n]) \cong \mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q}, A)[\mathfrak{p}^n]$.

Proof. — Under the assumption that $\mathrm{H}^0(\mathbb{Q}_p, A[\mathfrak{p}]) = \{0\}$, we have that our Selmer groups $\mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q}, A[\mathfrak{p}])$ and $\mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q}, A)$ coincide with $\mathrm{H}^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}, A[\mathfrak{p}])$ and $\mathrm{H}^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}, A)$ in [21], respectively. Here, $\mathcal{F}^*_{\mathrm{can}}$ is the Selmer structure on $A \cong \mathrm{Hom}(T, \mu_{p^\infty})$ induced by the canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ on T, explained in [21, Definition 3.2.1]. Then, the lemma follows from [21, Lemma 3.5.3] (Although slightly stronger assumptions are assumed in loc. cit., one sees that we only need to assume that $\mathrm{H}^0(\mathbb{Q}, A[\mathfrak{p}]) = 0$ in order to prove the lemma). □

The following two propositions give examples on the vanishing of local cohomology groups.

Proposition 3.7. — *Assume at least one of the following three assumptions holds.*

(a) *The modular form* f *is ordinary (i.e.* $a_p \in \mathscr{O}_{\mathfrak{p}}^{\times}$*), and* $a_p \not\equiv 1 \bmod \mathfrak{p}$.
(b) *The modular form* f *is ordinary, and* k *is congruent to neither* 0 *nor* 2 *modulo* $2(p-1)$.

(c) *We have* $\mathrm{ord}_p(a_p) > \lfloor (k-2)/(p-1) \rfloor$, *where* $\lfloor x \rfloor$ *denotes the maximal integer* m *such that* $m \leqslant x$, *and* ord_p *denotes the additive valuation on* $\mathbb{C}_p$ *such that* $\mathrm{ord}_p(p) = 1$ *(we regard* $\mathrm{ord}_p(0) = \infty$*).*

Then, $\mathrm{H}^0(\mathbb{Q}_p, A) = \{0\}$.

Proof. — It suffices to show that $\mathrm{H}^0(\mathbb{Q}_p, T/\mathfrak{p}) = 0$. Assume first that f is ordinary. Then, $G_{\mathbb{Q}_p}$ acts on $T_\mathfrak{p} \cong k_\mathfrak{p}^{\oplus 2}$ by

$$\begin{bmatrix} \overline{\kappa}_{\mathrm{cyc}}^{k/2} \lambda^{-1} & * \\ 0 & \overline{\kappa}_{\mathrm{cyc}}^{(2-k)/2} \lambda \end{bmatrix}, \tag{3.2}$$

where $\overline{\kappa}_{\mathrm{cyc}} : G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$ denotes the cyclotomic character, and $\lambda : G_{\mathbb{Q}_p} \to k_\mathfrak{p}^\times$ denotes the unramified character sending the arithmetic Frobenius Fr_p at p to the image of a_p in $k_\mathfrak{p}^\times$ (cf. [33, Theorem 4]). Under (a) or (b), $\overline{\kappa}_{\mathrm{cyc}}^{k/2} \lambda^{-1}$ and $\overline{\kappa}_{\mathrm{cyc}}^{(2-k)/2} \lambda$ are non-trivial, which implies that $\mathrm{H}^0(\mathbb{Q}_p, T/\mathfrak{p}) = 0$.

Under (c), by [6, Theorem 4.2.1], the semi-simplification of $T/\mathfrak{p}|_{G_{\mathbb{Q}_p}}$ is isomorphic to the representation $\overline{V}_{k.0}$ of $G_{\mathbb{Q}_p}$ explained in [6, §1.1]. By the same argument as in the proof of [18, Lemma 4.4], we have that $\mathrm{H}^0(\mathbb{Q}_p, \overline{V}_{k,0}) = \{0\}$. □

Proposition 3.8. — *Assume that* $p \geqslant 5$ *and that* $F_\mathfrak{p}/\mathbb{Q}_p$ *is unramified. Let* l *be a prime such that* $l^2 \mid N$, *then* $\mathrm{H}^0(\mathbb{Q}_l^{\mathrm{ur}}, A) = \{0\}$.

Proof. — Since $A[\mathfrak{p}] \cong T_f/\mathfrak{p}$ as a $G_{\mathbb{Q}_l^{\mathrm{ur}}}$-module, we are reduced to showing that $\mathrm{H}^0(\mathbb{Q}_l^{\mathrm{ur}}, T_f/\mathfrak{p}) = \{0\}$. Let $\overline{x}$ be a non-zero element of $\mathrm{H}^0(\mathbb{Q}_l^{\mathrm{ur}}, T_f/\mathfrak{p})$. Let $\mathscr{I}^w$ be the wild inertia group of $G_{\mathbb{Q}_l}$, which is a pro-l group. We note that since $\mathscr{O}_\mathfrak{p}$ is unramified, the kernel of the natural map $\mathrm{GL}_2(\mathscr{O}_\mathfrak{p}) \to \mathrm{GL}_2(\mathscr{O}/\mathfrak{p})$ is pro-p. Hence, by $l \neq p$, there exists a lift $x \in T_f$ of $\overline{x}$ fixed by $\mathscr{I}^w$. In particular, $\dim_{F_\mathfrak{p}}(V_f^{\mathscr{I}^w}) = 1, 2$. Moreover, since $l^2 \mid N$, we have that $V_f|_{G_{\mathbb{Q}_l}}$ is absolutely irreducible (cf. [33, §3.1]), and hence $\dim_{F_\mathfrak{p}}(V_f^{\mathscr{I}^w}) = 2$, that is, $V_f = V_f^{\mathscr{I}^w}$. If we denote by $\mathscr{I}$ the inertia subgroup of $G_{\mathbb{Q}_l}$, then $\mathscr{I}/\mathscr{I}^w$ is abelian. Hence, there exist a finite extension E of $\mathbb{Q}_p$ and continuous characters $\chi_1, \chi_2 : \mathscr{I} \to \mathscr{O}_E^\times$ such that $V_f \otimes E \cong E(\chi_1) \oplus E(\chi_2)$ as $\mathscr{I}$-modules. Since $\det(V_f) \cong F_\mathfrak{p}(1-k)$ as a representation of $G_\mathbb{Q}$, $\chi_2 = \chi_1^{-1}$. By the existence of $\overline{x} \in \mathrm{H}^0(\mathbb{Q}_l^{\mathrm{ur}}, T_f/\mathfrak{p}) \setminus \{0\}$, the image of χ_1 is contained in $1 + m_E$, where m_E denotes the maximal ideal of the ring of integers in E. Then, by Grothendieck's monodromy theorem (cf. [32, p. 515]), the order of χ_1 is a power of p. Since I acts on $V_f \otimes E$ factoring through a conjugation of $\mathrm{GL}_2(\mathscr{O}_\mathfrak{p})$, which has no non-trivial p-torsion element (since $\mathscr{O}_\mathfrak{p}$ is unramified over $\mathbb{Z}_p$ and $p \geqslant 5$), we have that χ_1 is trivial. Hence $V_f \otimes E$ is unramified, which contradicts that $V_f|_{G_{\mathbb{Q}_l}}$ is absolutely irreducible. □

The following is a proposition concerning the condition (1.1).

Proposition 3.9. — *Under Assumption A (2), the density of the primes l such that $\mathrm{H}^0(\mathbb{Q}_l, A[\mathfrak{p}])$ is isomorphic to $\mathscr{O}_{\mathfrak{p}}/\mathfrak{p}$ or $\{0\}$ is greater than or equal to $1-(p^3-p)^{-1}|(\mathbb{F}_p^\times)^{k-1}|^{-1}$.*

Proof. — We first note that since $A[\mathfrak{p}] \cong k_{\mathfrak{p}}^{\oplus 2}$ (recall that $k_{\mathfrak{p}} := \mathscr{O}_{\mathfrak{p}}/\mathfrak{p}$), for a prime $l \nmid pN$, the vector space $\mathrm{H}^0(\mathbb{Q}_l, A[\mathfrak{p}])$ is isomorphic to $k_{\mathfrak{p}}$ or $\{0\}$ if and only if the action of the arithmetic Frobenius Fr_l on $A[\mathfrak{p}]$ is nontrivial. Hence, we estimate the density of primes l such that Fr_l acts on $A[\mathfrak{p}]$ trivially. We recall that for a prime $l \nmid pN$, the characteristic polynomial of Fr_l is given by

$$\det(1-\mathrm{Fr}_l\, X|V) = 1 - a_l l^{(2-k)/2}X + lX^2.$$

Then, if Fr_l acts on $A[\mathfrak{p}]$ trivially, then $l=1$ in $k_{\mathfrak{p}}$, which implies that $\kappa^{\mathrm{cyc}}(\mathrm{Fr}_l) \in 1+p\mathbb{Z}_p$ and that Fr_l acts on $A[\mathfrak{p}](-k/2) \cong T_f/\mathfrak{p}$ trivially as well. If we denote by $\mathbb{Q}\,(T_f/\mathfrak{p})$ the smallest Galois extension L of $\mathbb{Q}$ such that G_L acts on $T_f/\mathfrak{p}$ trivially, then by Assumption A (2), $\bar\rho_f\,(\mathrm{Gal}\,(\mathbb{Q}\,(T_f/\mathfrak{p})\,/\mathbb{Q}))$ contains a subgroup isomorphic to

$$H := \left\{ g \in \mathrm{GL}_2(\mathbb{F}_p) |\det(g) \in (\mathbb{F}_p^\times)^{k-1} \right\},$$

where $\bar\rho_f : G_{\mathbb{Q}} \to \mathrm{Aut}_{k_{\mathfrak{p}}}(T_f/\mathfrak{p}) \cong \mathrm{GL}_2(k_{\mathfrak{p}})$ denotes the representation attached to $T_f/\mathfrak{p}$. Since $\mathrm{GL}_2(\mathbb{F}_p) = \coprod_{a\in\mathbb{F}_p^\times} g_a\,\mathrm{SL}_2(\mathbb{F}_p)$, where g_a is any element of $\mathrm{GL}_2(\mathbb{F}_p)$ such that $\det(g_a)=a$, we have $|H| = |\mathrm{SL}_2(\mathbb{F}_p)|\cdot|(\mathbb{F}_p^\times)^{k-1}| = (p^3-p)|(\mathbb{F}_p^\times)^{k-1}|$. Hence, the density of primes $l \nmid pN$ such that Fr_l acts on $A[\mathfrak{p}](-k/2)$ trivially is less than or equal to $(p^3-p)^{-1}|(\mathbb{F}_p^\times)^{k-1}|^{-1}$. Then, the density of primes $l \nmid pN$ such that Fr_l acts on $A[\mathfrak{p}]$ trivially is less than or equal to $(p^3-p)^{-1}|(\mathbb{F}_p^\times)^{k-1}|^{-1}$. □

4. Preliminaries of derivatives classes

We apply the derivatives introduced in [8] to Euler systems for T (in the sense of Definition 4.4), and we review the local conditions of resulting derivative classes. We keep the same notation as in the previous section.

For an integer $S>0$, we denote by $\mathbb{Q}(S)$ the maximal p-extension of $\mathbb{Q}$ inside $\mathbb{Q}(\zeta_S)$, and then $\Gamma_S = \mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q})$. For integers S and S' with $(S,S')=1$, by the canonical decomposition $\Gamma_{SS'} = \Gamma_S \times \Gamma_{S'}$, we regard Γ_S and $\Gamma_{S'}$ as subgroups of $\Gamma_{SS'}$.

4.1. Darmon–Kolyvagin derivatives

We recall the derivatives introduced in [8].

As usual, for integers $j \geqslant 0$ and $k \geqslant 1$, we put

$$\binom{j}{k} = \frac{j(j-1)\cdots(j-k+1)}{k!}$$

and $\binom{j}{0} = 1$. For $k < 0$, we define $\binom{j}{k} = 0$. For an element $\sigma \in \Gamma_S$ of order n and for an integer $k \geqslant 0$, we define

$$D_\sigma^{(k)} = \sum_{j=0}^{n-1} \binom{j}{k} \sigma^j \in \mathbb{Z}[\Gamma_S].$$

We note that $D_\sigma^{(k)} = 0$ if either $k \geqslant n$ or $k < 0$. By a simple computation we have the following.

Lemma 4.1. — *Let q be a power of p. If $\sigma \in \Gamma_S$ is of order q and $0 \leqslant k \leqslant p-1$, then*

$$(\sigma - 1) D_\sigma^{(k)} \equiv -\sigma D_\sigma^{(k-1)} \mod q.$$

Definition 4.2. — *In the rest of this paper, for each prime $l \neq p$, we fix a generator σ_l of Γ_l. We write $D_l^{(k)} = D_{\sigma_l}^{(k)}$. Let $S > 0$ be a square-free integer relatively prime to p. We call a non-zero element D of $\mathbb{Z}[\Gamma_S]$ a* Darmon–Kolyvagin derivative*, or simply, a* derivative *if D is of the following form:*

$$D_{l_1}^{(k_1)} \cdots D_{l_s}^{(k_s)} \in \mathbb{Z}[\Gamma_{l_1 \cdots l_s}] \subseteq \mathbb{Z}[\Gamma_S],$$

where $l_1, \ldots, l_s$ are distinct primes dividing S, and each k_i is an integer such that $0 \leqslant k_i < |\Gamma_{l_i}|$. We note that if we are given such a D, then $l_1, \ldots, l_s, k_1, \ldots, k_s$ are uniquely determined, and we define

$$\mathrm{Supp}(D) = l_1 \cdots l_s, \qquad \mathrm{Cond}(D) = \prod_{k_i > 0} l_i,$$

which we call the support *and the* conductor *of D, respectively. We put*

$$\mathrm{ord}(D) = k_1 + \cdots + k_s, \quad n(D) = \min_{k_i > 0}\{|\Gamma_{l_i}|\}, \quad e_{l_i}(D) = k_i.$$

We call $\mathrm{ord}(D)$ *the* order *of D. When $k_i = 0$ for all i, we define $n(D) = 1$. By convention, we also regard $1 \in \mathbb{Z}[\Gamma_{Sp^n}]$ as a derivative, and put* $\mathrm{Supp}(1) = 1, \mathrm{Cond}(1) = 1$ *and* $\mathrm{ord}(1) = 0$. *When $S = l_1 \cdots l_s$, we put*

$$N_S = D_{l_1}^{(0)} \cdots D_{l_s}^{(0)}.$$

We denote by $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and fix a generator γ of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$*. For a non-negative integer a, we put $D_{p^n}^{(a)} = D_\gamma^{(a)} \in \mathbb{Z}[\Gamma_{p^n}]$,* *where we denote by the same symbol* γ *its image in* Γ_{p^n}*. We also put* $\mathrm{ord}(D^{(a)}_{p^n}D) = a + \mathrm{ord}(D)$ *and*

$$n(D^{(a)}_{p^n}D) = \begin{cases} \min\{p^{n-1}, n(D)\} & (a > 0), \\ n(D) & (a = 0). \end{cases}$$

Lemma 4.3. — *Let* S *be a square-free positive integer relatively prime to* p*, let* $n \geqslant 0$ *and let* M *be a* $\mathscr{O}_{\mathfrak{p}}[\Gamma_{p^nS}]$*-module without* p*-torsion elements. Let* z *be an element of* M *and put* $\theta = \sum_{\sigma\in\Gamma_{p^nS}} \sigma z \otimes \sigma \in M \otimes_{\mathscr{O}_{\mathfrak{p}}} \mathscr{O}_{\mathfrak{p}}[\Gamma_{p^nS}]$*. Let* $t \geqslant 1$*. Assume that* $D^{(a)}_{p^n}Dz \equiv 0 \mod n(D^{(a)}_{p^n}D)$ *for every integer* $a \geqslant 0$ *and every Darmon–Kolyvagin derivative* D *such that* $\mathrm{Supp}(D) = S$ *and* $\mathrm{ord}(D^{(a)}_{p^n}D) < \min\{t, p\}$*. Then,* $\theta - N_S z \otimes 1 \in M \otimes_{\mathscr{O}_{\mathfrak{p}}} I^{\min\{t,p\}}_{\Gamma_{Sp^n}}$*, where* $I_{\Gamma_{Sp^n}}$ *denotes the augmentation ideal of* $\mathscr{O}_{\mathfrak{p}}[\Gamma_{Sp^n}]$*.*

Proof. — This is [26, Lemma 3.6]. □

4.2. Euler system

We recall the definition of Euler system (for T). As is remarked in [26, Remark 3.12], our definition is slightly different from the usual definition as in [31].

For a prime l, we define $P_l(t) \in F[t]$ by

$$P_l(t) = 1 - l^{1-\frac{k}{2}} a_l t + \epsilon(l)t^2. \tag{4.1}$$

Let Σ be a finite set of primes which contains all the primes dividing pN. We put

$$\mathscr{R} = \{\text{primes } l \mid l \notin \Sigma, l \equiv 1 \bmod p\},$$
$$\mathscr{N} = \{\text{square-free products of primes in } \mathscr{R}\} \cup \{1\}.$$

Definition 4.4. — *We call* $\{z_{Sp^n}\}_{S\in\mathscr{N}, n\geqslant 0} \in \prod_{S,n} \mathrm{H}^1(\mathbb{Q}(Sp^n), T)$ *an* Euler system *(for* T *and* $\mathscr{N}$*) if it satisfies the following conditions.*

1. *Let* $S \in \mathscr{N}$*, and let* $l \in \mathscr{R}$ *be a prime not dividing* S*. For* $n \geqslant 0$*,*
$$\mathrm{Cor}_{Slp^n/Sp^n}(z_{Slp^n}) = P_l(\mathrm{Fr}_l^{-1})(z_{Sp^n}),$$
where $\mathrm{Cor}_{Slp^n/Sp^n} : \mathrm{H}^1(\mathbb{Q}(Slp^n), T) \to \mathrm{H}^1(\mathbb{Q}(Sp^n), T)$ *denotes the corestriction map.*
2. *For every* $S \in \mathscr{N}$*, the system* $\{z_{Sp^n}\}_{n\geqslant 0}$ *is a norm compatible system, that is,* $\{z_{Sp^n}\}_{n\geqslant 0}$ *lies in* $\varprojlim_n \mathrm{H}^1(\mathbb{Q}(Sp^n), T)$*, where the limit is taken with respect to the corestriction maps* $\mathrm{Cor}_{Sp^{n+1}/Sp^n}$*.*

4.3. Local images at primes not dividing p

In this subsection, following [26], we recall local properties of derivatives of Euler systems at primes *not* dividing p.

Let $\mathfrak{q} \neq \mathscr{O}_{\mathfrak{p}}$ be an ideal of $\mathscr{O}_{\mathfrak{p}}$ and $\{z_{Sp^n}\}_{S\in\mathscr{N},n\geqslant 0}$ an Euler system. For a finite extension field K of $\mathbb{Q}$ or $\mathbb{Q}_l$ for some prime l, by taking Galois cohomology with respect to the exact sequence

$$0 \to T \xrightarrow{\times\varpi^n} T \to T/\mathfrak{q} \to 0,$$

where ϖ is a uniformizer of $F_{\mathfrak{p}}$, the natural homomorphism $\mathrm{H}^1(K,T)/\mathfrak{q} \to \mathrm{H}^1(K,T/\mathfrak{q})$ is injective. Then, by this injection, we often regard $\mathrm{H}^1(K,T)/\mathfrak{q}$ as s submodule of $\mathrm{H}^1(K,T/\mathfrak{q}) \cong \mathrm{H}^1(K,A[\mathfrak{q}])$.

For a prime $l \neq p$, we put

$$t_{f,l} = \min\left\{n \geqslant 0 \,\middle|\, \varpi^n \mathrm{H}^1\left(\mathbb{F}_l, \mathrm{H}^0(\mathbb{Q}_l^{\mathrm{ur}}, A)/(\mathrm{div.})\right) = \{0\}\right\}, \tag{4.2}$$

which is less than or equal to $\mathrm{length}_{\mathscr{O}_{\mathfrak{p}}}(\mathrm{H}^1(\mathbb{F}_l, \mathrm{H}^0(\mathbb{Q}_l^{\mathrm{ur}}, A)/(\mathrm{div.})))$, the Tamagawa exponent. We note that if $l \nmid N$, then $t_{f,l} = 0$.

Proposition 4.5. — *Let D be a Darmon–Kolyvagin derivative such that $S := \mathrm{Supp}(D) \in \mathscr{N}_{\mathfrak{q}}$, and put $S' = \mathrm{Cond}(D)$. Let a be a non-negative integer. Suppose that the image of $D_{p^n}^{(a)} D z_{Sp^n}$ in $\mathrm{H}^1(\mathbb{Q}(Sp^n),T)/\mathfrak{q}$ is fixed by Γ_{Sp^n}, and denote by $\kappa \in \mathrm{H}^1(\mathbb{Q},T/\mathfrak{q})$ the element whose restriction is equal to the image of $D_{p^n}^{(a)} D z_{Sp^n}$ in $\mathrm{H}^1(\mathbb{Q}(Sp^n),T/\mathfrak{q})$ (cf. Proposition 3.2). Then, for a prime $l \nmid pS'$ we have $\varpi^{t_{f,l}} \mathrm{loc}_l(\kappa) \in \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l,T/\mathfrak{q})$.*

Proof. — By the same argument as in the proof of [26, Proposition 3.14], we have $\mathrm{loc}_l(\kappa) \in \mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}_l,T/\mathfrak{q})$. It is known that $\varpi^{t_{f,l}}\mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}_l,T/\mathfrak{q}) \subseteq \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l,T/\mathfrak{q})$ (cf. [31, Lemmas 1.3.5 and 1.3.8]), and then we complete the proof. □

We put

$$\begin{aligned} &\mathscr{R}_{\mathfrak{q}} = \{l \in \mathscr{R} \,|\, l-1 \in \mathfrak{q}\}, \quad \mathscr{R}_{f,\mathfrak{q}} = \{l \in \mathscr{R}_{\mathfrak{q}} \,|\, P_l(1) \in \mathfrak{q}\}, \\ &\mathscr{N}_{\mathfrak{q}} = \{\text{square-free products of primes in } \mathscr{R}_{\mathfrak{q}}\} \cup \{1\}. \end{aligned} \tag{4.3}$$

For an $\mathscr{O}_{\mathfrak{p}}$-module M of finite cardinality and an element $x \in M$, we define

$$\mathrm{ord}(x,M) = \inf\{m \geqslant 0 \,|\, \varpi^m x = 0\} \in \mathbb{Z}.$$

By the same argument as in those of proofs of [31, Theorem 4.5.4] and [26, Theorem 3.18], one can show the following proposition.

Proposition 4.6. — *Assume Assumption A (2). Let S be an element of $\mathscr{N}_{\mathfrak{p}}$. Let $n \geqslant 1$, and let $l \in \mathscr{R}_{f,\mathfrak{q}}$ be a prime which splits completely in $\mathbb{Q}(Sp^n)$. Let λ be a prime of $\mathbb{Q}(Sp^n)$ above l. For a Darmon–Kolyvagin derivative D whose support is S, the following hold.*

(1) *For* $a \geqslant 0$, *the image of* $\mathrm{loc}_\lambda(D_{p^n}^{(a)} D z_{Sp^n})$ *in* $\mathrm{H}^1(\mathbb{Q}(Sp^n)_\lambda, T/\mathfrak{q}) = \mathrm{H}^1(\mathbb{Q}_l, T/\mathfrak{q})$ *lies in* $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l, T/\mathfrak{q})$.
(2) *The image of* $D_{p^n}^{(a)} D D_l^{(1)} z_{Slp^n}$ *in* $\mathrm{H}^1(\mathbb{Q}(Slp^n), T)/\mathfrak{q}$ *is fixed by* Γ_l.
(3) *Let* $\kappa^{(l)} \in \mathrm{H}^1(\mathbb{Q}(Sp^n), T/\mathfrak{q})$ *be the element corresponding to the class* $D_{p^n}^{(a)} D D_l^{(1)} z_{Slp^n} \bmod \mathfrak{q}$ *under the isomorphism*

$$\mathrm{H}^1(\mathbb{Q}(Sp^n), T/\mathfrak{q}) \cong \mathrm{H}^0\left(\Gamma_l, \mathrm{H}^1(\mathbb{Q}(Slp^n), T/\mathfrak{q})\right)$$

induced by the restriction map. If $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l, A[\mathfrak{q}]) \cong \mathscr{O}_\mathfrak{p}/\mathfrak{q}$, *then we have*

$$\mathrm{ord}\left(\mathrm{loc}_{/\mathrm{f},\lambda}(\kappa^{(l)}), \mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}_l, T/\mathfrak{q})\right) = \mathrm{ord}\left(\mathrm{loc}_\lambda(D_{p^n}^{(a)} D z_S \bmod q), \mathrm{H}^1(\mathbb{Q}_l, T/\mathfrak{q})\right).$$

5. Divisibility of derivative classes

In this section, we study p-divisibility of derivatives of Euler systems (cf. Theorem 5.5), and we give its applications. Since some lemmas and propositions of this section are proved in the same way as in [26], we often omit their proof and refer the reader to [26, §4].

We keep the notation as in Section 4. In particular, $\{z_{Sp^n}\}_{S \in \mathscr{N}, n \geqslant 0}$ denotes an Euler system for $T = T_f(k/2)$ and some $\mathscr{N}$ in the sense of Definition 4.4.

5.1. The key theorem

The aim of this subsection is to prove Theorem 5.5. Throughout this subsection, we assume the hypotheses (2) and (3) in Assumption A.

5.1.1. Consequence of the classical Euler system argument

Proposition 5.1. — *The following assertions hold.*
(1) *If* $\mathfrak{r}_f := \mathrm{corank}_{\mathscr{O}_\mathfrak{p}}\left(\mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q}, A)\right) > 0$, *then* $z_1 = 0 \in \mathrm{H}^1(\mathbb{Q}, T)$.
(2) *If* $r_f > 0$, *then* $\mathrm{loc}_{/\mathrm{f},p}(z_1) = 0 \in \mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}_p, T)$.

Proof. — The assertion (1) (resp. (2)) follows from [31, Theorem 2.2.3] (resp. [31, Theorem 2.2.10]) and Lemma 3.1. □

5.1.2. Notation

Let $\mathfrak{q}$ be an ideal of $\mathscr{O}_\mathfrak{p}$ which is not equal to $\{0\}$ or $\mathscr{O}_\mathfrak{p}$. For a finitely generated $\mathscr{O}_\mathfrak{p}$-module M, we define an integer $r_\mathfrak{q}(M)$ by

$$M \otimes_{\mathscr{O}_\mathfrak{p}} \mathscr{O}_\mathfrak{p}/\mathfrak{q}\mathscr{O}_\mathfrak{p} \cong (\mathscr{O}_\mathfrak{p}/\mathfrak{q}\mathscr{O}_\mathfrak{p})^{\oplus r_\mathfrak{q}(M)} \oplus M',$$

where M' is killed by the ideal $\mathfrak{q}\mathfrak{p}^{-1} \subseteq \mathscr{O}_\mathfrak{p}$.

Lemma 5.2. — *For an exact sequence of finite $\mathscr{O}_\mathfrak{p}/\mathfrak{q}\mathscr{O}_\mathfrak{p}$-modules $0 \to M' \to M \to M''$, we have $r_\mathfrak{q}(M) \leqslant r_\mathfrak{q}(M') + r_\mathfrak{p}(M'')$.*

Proof. — This is [20, Lemma 3.4]. □

Definition 5.3. — *Let D be a Darmon–Kolyvagin derivative with support $S \in \mathscr{N}$. We define the* weight *of D as*

$$w_\mathfrak{q}(D) = \mathrm{ord}(D) - \#\left\{l \in \mathscr{R}_{f,\mathfrak{q}} \mid l \text{ divides } S\right\}.$$

Proposition 5.4. — *Let D be a Darmon–Kolyvagin derivative such that its support S lies in $\mathscr{N}_\mathfrak{q}$. Suppose that $n > 0$ is an integer such that $p^{n-1} \in \mathfrak{q}$. If $w_{p^n}(D) := w_{p^n\mathscr{O}_\mathfrak{p}}(D) < 0$ and $\max_{l|S}\{e_l(D)\} < p$ (see Definition 4.2 for $e_l(D)$), then for $a \geqslant 0$ we have*

$$D_{p^n}^{(a)} D z_{p^n S} \equiv 0 \mod \mathfrak{q}\mathrm{H}^1(\mathbb{Q}(p^n S), T).$$

Proof. — We first note that the assumption $w_{p^n}(D) < 0$ implies that there exist a prime $l \in \mathscr{R}_{f,p^n}$ dividing S and a derivative D' such that

$$D = D' N_l, \quad \mathrm{Supp}(D') = S/l, \quad \mathrm{ord}(D') = \mathrm{ord}(D). \tag{5.1}$$

As in [26, Proposition 4.7], we prove the proposition by induction on the number of primes dividing S. If $S = l$ is a prime, then $l \in \mathscr{R}_{f,p^n} := \mathscr{R}_{f,p^n\mathscr{O}_\mathfrak{p}}$ and $D = N_l$. Since $P_l(1) \equiv 0 \bmod \mathfrak{q}$ and since l splits completely in $\mathbb{Q}(p^n)$, we have

$$D_{p^n}^{(a)} D z_{p^n l} = D_{p^n}^{(a)} N_l z_{p^n l} = D_{p^n}^{(a)} P_l(\mathrm{Fr}_l^{-1}) z_{p^n} = P_l(1) D_{p^n}^{(a)} z_{p^n} \equiv 0 \mod \mathfrak{q}.$$

For general S, since $w_{p^n}(D) < 0$, there exist a prime $l \in \mathscr{R}_{f,p^n}$ dividing S and a derivative D' as in (5.1). Then, we have $w_{p^n}(D') = w_{p^n}(D) + 1 \leqslant 0$. We write $S/l = l_1 \cdots l_b$. We shall first show that for $1 \leqslant i \leqslant b$,

$$(\sigma_{l_i} - 1) D_{p^n}^{(a)} D' z_{p^n S/l} \equiv 0 \mod \mathfrak{q}, \tag{5.2}$$

where σ_{l_i} is the generator of Γ_{l_i} fixed in Definition 4.2. It suffices to consider the case $i = 1$. We write $D' = D_{l_1}^{(k_1)} \cdots D_{l_b}^{(k_b)}$. In the case where $k_1 = 0$, we have $D' = N_{l_1} D_{l_2}^{(k_2)} \cdots D_{l_b}^{(k_b)}$, and hence (5.2) is clear. We may then assume that $k_1 \geqslant 1$. Since the order of σ_{l_1} is congruent to 0 modulo $\mathfrak{q}$ and since $0 < k_1 < p$, Lemma 4.1 implies that

$$(\sigma_{l_1} - 1)D' \equiv -\sigma_{l_1} D_{l_1}^{(k_1-1)} D_{l_2}^{(k_2)} \cdots D_{l_b}^{(k_b)} \mod \mathfrak{q}. \tag{5.3}$$

We note that

$$\begin{aligned} \mathrm{Supp}(D_{l_1}^{(k_1-1)} D_{l_2}^{(k_2)} \cdots D_{l_b}^{(k_b)}) &= S/l, \\ w(D_{l_1}^{(k_1-1)} D_{l_2}^{(k_2)} \cdots D_{l_b}^{(k_b)}) &= w(D') - 1 < 0. \end{aligned}$$

Then, the induction hypothesis implies that

$$D_{p^n}^{(a)} D_{l_1}^{(k_1-1)} D_{l_2}^{(k_2)} \cdots D_{l_b}^{(k_b)} z_{p^n S/l} \equiv 0 \mod \mathfrak{q},$$

and hence by (5.3), we deduce (5.2).

Since each Γ_{l_i} is generated by σ_{l_i}, the assertion (5.2) implies that

$$D_{p^n}^{(a)} D' z_{p^n S/l} \bmod \mathfrak{q} \in \mathrm{H}^0\left(\Gamma_{S/l}, \mathrm{H}^1(\mathbb{Q}(p^n S/l), T)/\mathfrak{q}\right),$$

that is, the action of $\Gamma_{p^n S/l}$ on $D_{p^n}^{(a)} D' z_{p^n S/l} \bmod \mathfrak{q}$ factors through Γ_{p^n}. Therefore, by $l \in \mathscr{R}_{f,p^n}$ and (5.1), we have

$$\begin{aligned} D_{p^n}^{(a)} D z_{p^n S} = D_{p^n}^{(a)} D' N_l z_{p^n S} &= D_{p^n}^{(a)} P_l(\mathrm{Fr}_l^{-1}) D' z_{p^n S/l} \\ &\equiv D_{p^n}^{(a)} P_l(1) D' z_{p^n S/l} \equiv 0 \mod \mathfrak{q}. \quad \square \end{aligned}$$

5.1.3. The theorem and its proof

Let $\mathfrak{q}$ be an ideal of $\mathscr{O}_\mathfrak{p}$ which is not equal to $\{0\}$ or $\mathscr{O}_\mathfrak{p}$.

Theorem 5.5. — *Let D be a Darmon–Kolyvagin derivative. Suppose that* $\max_{l|S}\{e_l(D)\} < p$, *where* $S := \mathrm{Supp}(D)$. *Suppose also that* $S \in \mathscr{N}_\mathfrak{q}$ *and that every prime* $l \mid S$ *satisfies* (1.1). *Then, the following assertions hold.*

(1) *If* $\mathrm{ord}(D) < r_\mathfrak{q}\left(\mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q}, A[\mathfrak{q}])\right)$, *then for* $m \geqslant 0$, *we have* $Dz_S = D_{p^m}^{(0)} D z_{p^m S} \equiv 0 \mod \mathfrak{q}\mathrm{H}^1(\mathbb{Q}(S), T)$.

(2) *Let $n > 0$ be an integer such that $\#\Gamma_{p^n} = p^{n-1} \in \mathfrak{q}$. Let a be an integer such that $0 \leqslant a < p$. If* $a + \mathrm{ord}(D) < r_\mathfrak{q}\left(\mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q}, A[\mathfrak{q}])\right)$, *then*

$$D_{p^n}^{(a)} D z_{p^n S} \equiv 0 \mod \mathfrak{q}\mathrm{H}^1(\mathbb{Q}(p^n S), T). \tag{5.4}$$

The proof of the assertion (1) is the same as [26, Theorem 4.9] and is omitted. Before the proof of (2), we show some lemmas.

Lemma 5.6. — *Let D be a Darmon–Kolyvagin derivative whose support S lies in $\mathscr{N}_{\mathfrak{q}}$. Let a and n be non-negative integers such that $p^{n-1} \in \mathfrak{q}$. Assume that the image of $D_{p^n}^{(a)} D z_{p^n S}$ in $\mathrm{H}^1(\mathbb{Q}(p^n S), T)/\mathfrak{q}$ is fixed by $\Gamma_{p^n S}$. Let $\kappa \in \mathrm{H}^1(\mathbb{Q}, T/\mathfrak{q})$ be as in Proposition 4.5. If $r_{\mathfrak{q}}(\mathrm{H}^1_{\mathrm{f},pS'}(\mathbb{Q}, A[\mathfrak{q}])) > 0$, where $S' := \mathrm{Cond}(D)$, then there exists a prime $l \in \mathscr{R}_{p^n} := \mathscr{R}_{p^n \mathscr{O}_{\mathfrak{p}}}$ such that*

(1) *l splits completely in $\mathbb{Q}(Sp^n)$, and $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l, T/\mathfrak{q}) \cong \mathscr{O}_{\mathfrak{p}}/\mathfrak{q}\mathscr{O}_{\mathfrak{p}}$,*
(2) *we have*

$$\mathrm{ord}\left(D_{p^n}^{(a)} D z_{p^n S} \bmod \mathfrak{q}, \mathrm{H}^1(\mathbb{Q}(p^n S), T)/\mathfrak{q}\right) = \mathrm{ord}(\mathrm{loc}_l(\kappa), \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l, T/\mathfrak{q})),$$

(3) *the localization map $\mathrm{H}^1_{\mathrm{f},pS'}(\mathbb{Q}, A[\mathfrak{q}]) \to \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l, A[\mathfrak{q}])$ is surjective.*

In addition, if the image of $D_{p^n}^{(a)} D D_l^{(1)} z_{Slp^n}$ in $\mathrm{H}^1(\mathbb{Q}(Slp^n), T)/\mathfrak{q}$ is fixed by $\Gamma_{p^n Sl}$, then

$$D_{p^n}^{(a)} D z_{Sp^n} \equiv 0 \mod \mathfrak{q}\mathrm{H}^1(\mathbb{Q}(Sp^n), T).$$

Proof. — By the same argument as in the proof of [26, Lemma 4.10], which is based on an application of Chebotarev's density theorem, one can find a prime l satisfying (1), (2) and (3).

We assume that the image of $D_{p^n}^{(a)} D D_l^{(1)} z_{Slp^n}$ in $\mathrm{H}^1(\mathbb{Q}(Slp^n), T)/\mathfrak{q}$ is fixed by $\Gamma_{p^n Sl}$. We denote by $\kappa_l \in \mathrm{H}^1(\mathbb{Q}, T/\mathfrak{q})$ the element whose image in $\mathrm{H}^1(\mathbb{Q}(Sp^n l), T/\mathfrak{q})$ coincides with that of $D_{p^n}^{(a)} D D_l^{(1)} z_{Sp^n}$. By the conditions (1) and (2) above, Proposition 4.6 (3) reduces us to proving that $\mathrm{loc}_{/\mathrm{f},l}(\kappa_l) = 0$. By taking the dual of the map in the condition (3) above, it suffices to show that $\mathrm{loc}_{/\mathrm{f},l}(\kappa_l)$ lies in the kernel of the injection

$$\mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}_l, T/\mathfrak{q}) \to \mathrm{Hom}_{\mathscr{O}_{\mathfrak{p}}}\left(\mathrm{H}^1_{\mathrm{f},pS'}(\mathbb{Q}, A[\mathfrak{q}]), \mathscr{O}_{\mathfrak{p}}/\mathfrak{q}\right); \ z \mapsto (x \mapsto (z, \mathrm{loc}_l(x))_{l,\mathfrak{q}}),$$

where for a prime v, we denote by $(-,-)_{v,\mathfrak{q}} : \mathrm{H}^1(\mathbb{Q}_v, T/\mathfrak{q}) \times \mathrm{H}^1(\mathbb{Q}_v, A[\mathfrak{q}]) \to \mathscr{O}_{\mathfrak{p}}/\mathfrak{q}$ the perfect pairing induced by the local duality. Let $x \in \mathrm{H}^1_{\mathrm{f},pS'}(\mathbb{Q}, A[\mathfrak{q}])$. Then, by the Hasse principle and the definition of $\mathrm{H}^1_{\mathrm{f},pS'}(\mathbb{Q}, A[\mathfrak{q}])$, we have

$$(\mathrm{loc}_{/\mathrm{f},l}(\kappa_l), \mathrm{loc}_l(x))_{l,\mathfrak{q}} = -\sum_{v \nmid pS'l} (\mathrm{loc}_v(\kappa_l), \mathrm{loc}_v(x))_{v,\mathfrak{q}}, \tag{5.5}$$

where v ranges over all primes not dividing $pS'l$. Hence, it suffices to show that for $v \nmid pS'l$

$$(\mathrm{loc}_v(\kappa_l), \mathrm{loc}_v(x))_{v,\mathfrak{q}} = 0. \tag{5.6}$$

By Assumption A (3), every $v \nmid pS'l$ satisfies at least one of the following two conditions:

(i) $t_{f,v} = 0$ (see (4.2) for $t_{f,v}$),

(ii) $\mathrm{H}^0(\mathbb{Q}_v, A[\mathfrak{p}]) = \{0\}$.

In the case (i), by Proposition 4.5, we have $\mathrm{loc}_v(\kappa_l) \in \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_v, T/\mathfrak{q})$. Since $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_v, T/\mathfrak{q})$ and $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_v, A[\mathfrak{q}])$ are orthogonal complements of each other (cf. [31, Proposition 1.4.3]), by $\mathrm{loc}_v(x) \in \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_v, A[\mathfrak{q}])$, we obtain (5.6). In the case (ii), the assertion (5.6) follows from Lemma 3.4. □

Lemma 5.7. — *Let D be a Darmon–Kolyvagin derivative such that $S := \mathrm{Supp}(D) \in \mathscr{N}_{\mathfrak{q}}$ and $\max_{l|S}\{e_l(D)\} < p$. Let $0 \leqslant a < p$ and $n \geqslant 0$ such that $p^{n-1} \in \mathfrak{q}$, and put $w = w_{p^n}(D)$. Assume that $D^{(b)}_{p^n} D' z_{p^n S} \equiv 0 \bmod \mathfrak{q}$ for every $D^{(b)}_{p^n} D'$ satisfying the assumptions as in Theorem 5.5 (2) such that $w_{p^n}(D') + b < w + a$. If $a + \mathrm{ord}(D) \leqslant r_{\mathfrak{q}}(\mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q}, A[\mathfrak{q}]))$, then the image of $D^{(a)}_{p^n} D z_{p^n S}$ in $\mathrm{H}^1(\mathbb{Q}(p^n S), T)/\mathfrak{q}$ is fixed by $\Gamma_{p^n S}$.*

Proof. — By Lemma 4.1 and the assumption that $D^{(a-1)}_{p^n} D z_{p^n S} \equiv 0 \bmod \mathfrak{q}$, we have

$$D^{(a)}_{p^n} D z_{p^n S} \bmod \mathfrak{q} \in \mathrm{H}^0\left(\Gamma_{p^n}, \mathrm{H}^1(\mathbb{Q}(p^n S), T)/\mathfrak{q}\right).$$

The case where $S = 1$ is completed by the congruence above, and then we may assume that $S \neq 1$. We write $S = l_1 \cdots l_s$. It suffices to show that for each $1 \leqslant i \leqslant s$

$$D^{(a)}_{p^n} D z_{p^n S} \bmod \mathfrak{q} \in \mathrm{H}^0\left(\Gamma_{l_i}, \mathrm{H}^1(\mathbb{Q}(p^n S), T)/\mathfrak{q}\right). \tag{5.7}$$

To prove (5.7), without loss of generality, we only need to consider the case where $i = 1$. If $e_{l_1}(D) = 0$, then we have $D = N_{l_1} D'$ for some derivative D', and hence we have (5.7). We assume that $e_{l_1}(D) \geqslant 1$. Then, by Lemma 4.1 we have

$$(\sigma_{l_1} - 1) D \equiv -\sigma_{l_1} D' \mod \mathfrak{q}\mathscr{O}_{\mathfrak{p}}[\Gamma_S],$$

where D' is a derivative such that $\mathrm{ord}(D') = \mathrm{ord}(D) - 1$ and $\mathrm{Supp}(D') = S$. Hence, we have $w_{p^n}(D') = w_{p^n}(D) - 1$. Therefore, by our assumption we have $D^{(a)}_{p^n} D' z_{p^n S} \equiv 0 \bmod \mathfrak{q}\mathrm{H}^1(\mathbb{Q}(p^n S), T)$. Hence, we obtain

$$(\sigma_{l_1} - 1) D^{(a)}_{p^n} D z_{p^n S} \equiv -\sigma_{l_1} D^{(a)}_{p^n} D' z_{p^n S} \equiv 0 \mod \mathfrak{q},$$

which implies (5.7). □

Proof of Theorem 5.5 (2). — We prove it by induction on $a + w_{p^n}(D)$. We note that the theorem obviously follows from Proposition 5.4 when $w := w_{p^n}(D) < 0$. We assume that the theorem holds for every $D^{(b)}_{p^n} D'$ satisfying the assumptions as in Theorem 5.5 (2) such that $b + w_{p^n}(D') < a + w$. Then, by Lemma 5.7, the image of $D^{(a)}_{p^n} D z_{p^n S}$ in $\mathrm{H}^1(\mathbb{Q}(p^n S), T)/\mathfrak{q}$ is fixed by $\Gamma_{p^n S}$, and we let $\kappa \in \mathrm{H}^1(\mathbb{Q}, T/\mathfrak{q})$ be as in Proposition 4.5.

We shall first prove that

$$r_{\mathfrak{q}}\left(\mathrm{H}^1_{\mathrm{f},pS'}(\mathbb{Q},A[\mathfrak{q}])\right) > 0. \tag{5.8}$$

We assume that $r_{\mathfrak{q}}\left(\mathrm{H}^1_{\mathrm{f},pS'}(\mathbb{Q},A[\mathfrak{q}])\right) = 0$. By Lemma 5.2 and the exact sequence

$$0 \to \mathrm{H}^1_{\mathrm{f},pS'}(\mathbb{Q},A[\mathfrak{q}]) \to \mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q},A[\mathfrak{q}]) \to \bigoplus_{l|S'} \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l,A[\mathfrak{q}]),$$

we have

$$r_{\mathfrak{q}}\left(\mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q},A[\mathfrak{q}])\right) \leqslant r_{\mathfrak{q}}(\mathrm{H}^1_{\mathrm{f},pS'}(\mathbb{Q},A[\mathfrak{q}])) + r_{\mathfrak{p}}\left(\bigoplus_{l|S'} \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l,A[\mathfrak{p}])\right),$$

and hence by our assumption,

$$\mathrm{ord}(D) < \sum_{l|S'} r_{\mathfrak{p}}(\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l,A[\mathfrak{p}])).$$

For each prime $l \mid S$, by the assumption (1.1) and Lemma 3.4 (2), we have $r_{\mathfrak{p}}(\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_l,A[\mathfrak{p}])) \leqslant 1$. Then, $\mathrm{ord}(D) < \sum_{l|S'} 1$, which contradicts the definition of $S' = \mathrm{Cond}(D)$. Hence, $r_{\mathfrak{q}}\left(\mathrm{H}^1_{\mathrm{f},pS'}(\mathbb{Q},A[\mathfrak{q}])\right) > 0$.

By (5.8), there exists a prime $l \in \mathscr{R}_{f,p^n}$ satisfying the conditions (1), (2) and (3) in Lemma 5.6 for $D^{(a)}_{p^n} D z_S$. Since $\mathrm{ord}(DD^{(1)}_l) \leqslant r_{\mathfrak{q}}(\mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q},A[\mathfrak{q}]))$ and $w_{p^n}(DD^{(1)}_l) = w$, by Lemma 5.7 we have

$$D^{(a)}_{p^n} DD^{(1)}_l z_{p^n Sl} \bmod \mathfrak{q} \in \mathrm{H}^0(\Gamma_{p^n Sl}, \mathrm{H}^1(\mathbb{Q}(p^n Sl),T)/\mathfrak{q}).$$

Hence, Lemma 5.6 implies that $D^{(a)}_{p^n} D z_{p^n S} \equiv 0 \mod \mathfrak{q}$. □

By the same argument as in the proof of [26, Theorem 4.15], one can prove a modification of Theorem 5.5 stated as follows:

Theorem 5.8. — *Let D and S be as in Theorem 5.5. Assume further that for each prime l dividing S, the $\mathscr{O}_{\mathfrak{p}}$-module $\mathrm{H}^0(\mathbb{Q}_l,A[\mathfrak{q}])$ is isomorphic to $\mathscr{O}_{\mathfrak{p}}/\mathfrak{q}\mathscr{O}_{\mathfrak{p}}$ or $\{0\}$. If $\mathrm{ord}(D) < r_{\mathfrak{q}}\left(\mathrm{H}^1_{\mathrm{f},pS'}(\mathbb{Q},A[\mathfrak{q}])\right) + r_{\mathfrak{p}}(B_{\mathfrak{q}}(S'))$, then $Dz_S \equiv 0 \bmod \mathfrak{q}\mathrm{H}^1(\mathbb{Q}(S),T)$, where $B_{\mathfrak{q}}(S') := \bigoplus_{v|S'} \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_v,A[\mathfrak{q}])$.*

5.2. Applications

5.2.1. On the refined conjecture for Euler systems

Theorem 5.9. — *Assume Assumption A. Let $S \in \mathscr{N}$ such that every prime $l \mid S$ satisfies (1.1). Then, for $n \geqslant 0$*

$$\sum_{\sigma\in\Gamma_{p^n S}} \sigma^{-1} z_{p^n S} \otimes \sigma \in \mathrm{H}^1(\mathbb{Q}(p^n S),T) \otimes_{\mathscr{O}_{\mathfrak{p}}} I^{\min\{\mathfrak{r}_f,p\}}_{\Gamma_{p^n S}},$$

where we recall that $\mathfrak{r}_f := \mathrm{corank}_{\mathscr{O}_\mathfrak{p}}(\mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q}, A))$.

Proof. — We may assume that $\mathfrak{r}_f \geqslant 1$. To apply Lemma 4.3 to $\mathrm{H}^1(\mathbb{Q}(p^nS), T)$ and z_{p^nS}, we take a derivative D such that $\mathrm{Supp}(D) = S$ and an integer a such that $0 < a + \mathrm{ord}(D) < \min\{\mathfrak{r}_f, p\}$. We denote by S' the conductor of D, and then $D = D'N_{\frac{S}{S'}}$, where the derivative D' satisfies

$$\mathrm{Supp}(D') = \mathrm{Cond}(D') = S', \quad n(D') = n(D), \quad \mathrm{ord}(D') = \mathrm{ord}(D).$$

Therefore,

$$D^{(a)}_{p^n} D z_{Sp^n} = D^{(a)}_{p^n} \left(\prod_{l|(S/S')} P_l(\mathrm{Fr}_l^{-1}) \right) D' z_{S'p^n},$$

where l ranges over all the primes dividing S/S'. If we put $\mathfrak{q} = n(D^{(a)}_{p^n} D)\mathscr{O}_\mathfrak{p}$, then $S' \in \mathscr{N}_\mathfrak{q}$. We note that Lemma 3.6 implies that $\mathfrak{r}_f \leqslant r_\mathfrak{q}(\mathrm{H}^1_{\mathrm{f},p}(\mathbb{Q}, A[\mathfrak{q}]))$. Then, Theorem 5.5 implies that $D^{(a)}_{p^n} D' z_{p^nS'} \equiv 0 \bmod \mathfrak{q}$, and hence we have $D^{(a)}_{p^n} D z_{Sp^n} \equiv 0 \bmod \mathfrak{q}$. Consequently, Lemma 4.3 shows that

$$\sum_{\sigma \in \Gamma_{Sp^n}} \sigma^{-1} z_{Sp^n} \otimes \sigma - N_{Sp^n} z_{Sp^n} \otimes 1 \in \mathrm{H}^1(\mathbb{Q}(Sp^n), T) \otimes I_{\Gamma_{Sp^n}}^{\min\{\mathfrak{r}_f, p\}}. \tag{5.9}$$

Hence, by Proposition 5.1 (1) we complete the proof. □

5.2.2. Localization of derivative classes at p

We state results which are applied to the case (1) of Theorem 1.1.

For a finite extension K of $\mathbb{Q}$, we put $\mathrm{H}^1(K \otimes \mathbb{Q}_p, -) = \bigoplus_{\lambda|p} \mathrm{H}^1(K_\lambda, -)$, where λ ranges over all the primes of K dividing p. We also define

$$\mathrm{H}^1_\mathrm{f}(K \otimes \mathbb{Q}_p, -) = \bigoplus_{\lambda|p} \mathrm{H}^1_\mathrm{f}(K_\lambda, -), \quad \mathrm{H}^1_{/\mathrm{f}}(K \otimes \mathbb{Q}_p, -) = \bigoplus_{\lambda|p} \mathrm{H}^1_{/\mathrm{f}}(K_\lambda, -).$$

For $\eta \in \mathrm{H}^1(K, -)$, we denote by $\mathrm{loc}_p(\eta)$ (resp. $\mathrm{loc}_{/\mathrm{f},p}(\eta)$) the image of η in $\mathrm{H}^1(K \otimes \mathbb{Q}_p, -)$ (resp. $\mathrm{H}^1_{/\mathrm{f}}(K \otimes \mathbb{Q}_p, -)$).

Corollary 5.10. — *Assume that Assumption A holds. Let D be a Darmon–Kolyvagin derivative such that $\max_{l|S}\{e_l(D)\} < p$, where $S :=$ $\mathrm{Supp}(D)$. Suppose that $S \in \mathscr{N}_\mathfrak{p}$ and that each prime $l \mid S$ satisfies* (1.1). *We put $S' = \mathrm{Cond}(D)$. Let $0 \leqslant a < p$ and $0 \leqslant n \leqslant 2$. If $a + \mathrm{ord}(D) <$ $r_\mathfrak{p}\left(\mathrm{H}^1_{\mathrm{f},S'}(\mathbb{Q}, A[\mathfrak{p}])\right) + r_\mathfrak{p}(B_\mathfrak{p}(S'))$, then the following assertions hold.*

1. *The image of $D^{(a)}_{p^n} D z_{Sp^n}$ in $\mathrm{H}^1(\mathbb{Q}(Sp^n), T)/\mathfrak{p}$ is fixed by Γ_{Sp^n}.*
2. *If we let $\kappa \in \mathrm{H}^1(\mathbb{Q}, T/\mathfrak{p})$ be as in Proposition 4.5 ($\mathfrak{q} = \mathfrak{p}$), then*

$$\mathrm{loc}_p(\kappa) \in \mathrm{H}^1_\mathrm{f}(\mathbb{Q}_p, T/\mathfrak{p}).$$

Proof. — The proof of the corollary is the same as in [26, Theorem 4.18], which is a consequence of Theorem 5.8. We omit the details. □

We note that $r_f \leqslant r_{\mathfrak{p}}\left(\mathrm{H}^1_{\mathrm{f},S}(\mathbb{Q}, A[\mathfrak{p}])\right) + r_{\mathfrak{p}}(B_{\mathfrak{p}}(S))$. Then, by a similar argument to the proof of Corollary 5.9 and by Proposition 5.1 (2) and Corollary 5.10, we obtain the following.

Corollary 5.11. — *Assume that Assumption A holds and that $F_{\mathfrak{p}}/\mathbb{Q}_p$ is unramified. Let S be as in Theorem 1.1 (a). If $0 \leqslant n \leqslant 2$, then*

$$\sum_{\tau \in \Gamma_S} \tau^{-1} \operatorname{loc}_{/\mathrm{f},p}(z_{Sp^n}) \otimes \tau \in \mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, T) \otimes I_S^{\min\{r_f, p\}}.$$

Proof. — By Assumption A (1) and the assumption that $F_{\mathfrak{p}}/\mathbb{Q}_p$ is unramified, we have a commutative diagram (with exact rows)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_p, T) & \xrightarrow{\times p} & \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_p, T) & \longrightarrow & \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}_p, T/\mathfrak{p}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{H}^1(\mathbb{Q}_p, T) & \xrightarrow{\times p} & \mathrm{H}^1(\mathbb{Q}_p, T) & \longrightarrow & \mathrm{H}^1(\mathbb{Q}_p, T/\mathfrak{p}) & \longrightarrow & 0, \end{array}$$

where the vertical arrows are the inclusions. By the snake lemma, we have an exact sequence

$$0 \longrightarrow \mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}_p, T) \xrightarrow{\times p} \mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}_p, T) \longrightarrow \mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}_p, T/\mathfrak{p}) \longrightarrow 0\ .$$

Hence, for $D^{(a)}_{p^n} D z_{sp^n}$ as in Corollary 5.10, we have

$$\operatorname{loc}_{/f,p}(D^{(a)}_{p^n} D z_{sp^n}) \in p\mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, T).$$

Noting that the exponent of the abelian group Γ_{Sp^n} is killed by p, by Proposition 5.1 (2), the proof is the same as that of Corollary 5.9. □

6. Kato's Euler system and Mazur–Tate elements

By using a method of Perrin-Riou [28], we construct local cohomology classes to connect Kato's Euler system with Mazur–Tate elements. The main result (Theorem 6.22) of this section may be regarded as a generalization of work of Otsuki [27] to higher weight modular forms with more care about integrality.

6.1. Construction of families of local points

In this subsection, we construct a family of local points to connect Kato's Euler system and p-adic L-functions which interpolate the special values of L-function twisted by tame characters as well.

6.1.1. Review of Perrin-Riou's method

Regarding V_f as a representation of $G_{\mathbb{Q}_p}$, we consider the filtered φ-module $D_{\mathrm{cris}}(V_f)$ associated to V_f, whose filtration is given by

$$\mathrm{Fil}^i D_{\mathrm{cris}}(V_f) = \begin{cases} D_{\mathrm{cris}}(V_f) & (i \leqslant 0), \\ S(f) \otimes_F F_{\mathfrak{p}} & (1 \leqslant i \leqslant k-1), \\ 0 & (i \geqslant k). \end{cases}$$

We note that $D_{\mathrm{cris}}(V_f)$ is a two-dimensional $F_{\mathfrak{p}}$-vector space and its φ is $F_{\mathfrak{p}}$-linear. We recall that T_f is the fixed lattice of V_f, and we denote by $M \subseteq D_{\mathrm{cris}}(V_f)$ the φ-stable lattice which is attached to T_f as in [3, §3.2]. We note that by [5, Proposition V.1.2], the determinant of the comparison isomorphism

$$B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V_f \cong B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} D_{\mathrm{cris}}(V_f)$$

with respect to basis of T_f and M lies in $t^{k-1}(\widehat{\mathbb{Z}}_p^{\mathrm{ur}})^\times$, where $\widehat{\mathbb{Z}}_p^{\mathrm{ur}}$ denotes the p-adic completion of the ring of integers in the maximal unramified extension of $\mathbb{Q}_p$, and $t \in B_{\mathrm{dR}}$ is the element associated to the fixed basis $\{\zeta_{p^n}\}_n$ of $\mathbb{Z}_p(1)$ (see [2, §1.1.2] for t).

Let H be a finite unramified extension of $\mathbb{Q}_p$ and W the ring of integers in H. Let $\sigma : H \to H$ denote the absolute Frobenius map. We let σ act on $W[\![X]\!]$ by $\sigma(\sum_{n\geqslant 0} a_n X^n) = \sum_{n \geqslant 0} a_n^\sigma X^n$. We define $\varphi : W[\![X]\!] \to W[\![X]\!]$ by

$$\varphi\left(\sum_{n\geqslant 0} a_n X^n\right) = \sum_{n\geqslant 0} a_n^\sigma((1+X)^p - 1)^n.$$

By abuse of notation, we denote by φ the operator $\varphi \otimes \varphi$ on $W[\![X]\!] \otimes_{\mathbb{Z}_p} M$. We put $H_n = H(\zeta_{p^n})$, $H_\infty = \cup_n H_n$ and $G_\infty = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \mathrm{Gal}(H_\infty/H)$. Then, G_∞ acts on $W[\![X]\!]$ by

$$\gamma\left(\sum_{n\geqslant 0} a_n X^n\right) = \sum_{n\geqslant 0} a_n((1+X)^{\kappa_{\mathrm{cyc}}(\gamma)} - 1)^n,$$

where we recall $\kappa_{\mathrm{cyc}} : G_\infty \to \mathbb{Z}_p^\times$ denotes the p-adic cyclotomic character. As in Subsection 3.2, for $h \in \mathbb{Z}$ we put

$$\mathrm{H}^1_{\mathrm{f}}(H_n, T_f(h)) = \mathrm{Ker}\big(\mathrm{H}^1(H_n, T_f(h)) \to \mathrm{H}^1(H_n, V_f(h) \otimes B_{\mathrm{cris}})\big),$$
$$\mathrm{H}^1_{\mathrm{f}}(H_n, V_f(h)) = \mathrm{Ker}\big(\mathrm{H}^1(H_n, V_f(h)) \to \mathrm{H}^1(H_n, V_f(h) \otimes B_{\mathrm{cris}})\big).$$

We define $\mathscr{H}_W(T_f(h)) \subseteq W[\![X]\!] \otimes_{\mathbb{Z}_p} D_{\mathrm{cris}}(V_f(h))$ as

$$\left\{ G \in W[\![X]\!] \otimes M \otimes_{\mathbb{Z}_p} e_{-h}\mathbb{Z}_p \;\middle|\; \sum_{\zeta \in \mu_p} G(\zeta(1+X)-1) = p\varphi(G(X)) \right\},$$

where $e_{-h} := t^{-h} \otimes \{\zeta_{p^n}\}^{\otimes h}$, the basis of $D_{\mathrm{cris}}(\mathbb{Q}_p(h))$. For a $\mathbb{Z}_p$-module L and $g(X) = \sum_{i=1}^n g_i(X) \otimes m_i \in W[\![X]\!] \otimes_{\mathbb{Z}_p} L$, if ζ is an element of the maximal ideal of $\overline{\mathbb{Q}}_p$, then we simply write $g(\zeta) = \sum_{i=1}^n g_i(\zeta) \otimes m_i \in W[\zeta] \otimes_{\mathbb{Z}_p} L$.

For $n \geqslant 0$ and $h \geqslant 1$, Perrin-Riou [28] constructs a family of homomorphisms

$$\Sigma_{H,h,n} : \mathscr{H}_W(T_f) \to \mathrm{H}^1_{\mathrm{f}}(H_n, T_f(h))$$

satisfying the following conditions (see [2, Theorem 4.3] or [3, §3.2] for details):

- for $G \in \mathscr{H}_W(T_f)$, if $n \geqslant 1$, then

$$\mathrm{Cor}_{H_{n+1}/H_n}(\Sigma_{H,h,n+1}(G)) = \Sigma_{H,h,n}((\sigma \otimes \varphi)G), \tag{6.1}$$

- for $G(X) \in \mathscr{H}_W(T_f(h))$,

$$\Sigma_{H,h,n}(D^h G(X) \otimes e_h) = (-1)^h (h-1)! p^{(h-1)n} \exp_{V_f(h),H_n}(G(\zeta_{p^n}-1)), \tag{6.2}$$

  where D denotes the differential operator $(1+X)\frac{\mathrm{d}}{\mathrm{d}X}$, and

$$\exp_{V_f(h),H_n} : H_n \otimes D_{\mathrm{cris}}(V_f(h)) / \mathrm{Fil}^0 D_{\mathrm{cris}}(V_f(h)) \to \mathrm{H}^1_{\mathrm{f}}(H_n, V_f(h))$$

  denotes the Bloch–Kato exponential map (cf. [7]).

In the rest of this section, we fix a root $\alpha \in \mathbb{C}_p$ of $X^2 - a_p X + p^{k-1}$ such that

$$\mathrm{ord}_p(\alpha) < k-1. \tag{6.3}$$

Let β be the other root. We note that if f is ordinary (i.e. $a_p \in \mathscr{O}_{\mathfrak{p}}^\times$), then α is the unit root, that is, $\alpha \in \mathscr{O}_{\mathfrak{p}}^\times$.

Proposition 6.1. — *If $\alpha^{[H:\mathbb{Q}_p]} \not\equiv 1 \bmod \mathfrak{p}$, then $1-\varphi : W \otimes M \to W \otimes M$ is surjective.*

Remark 6.2. — If f is non-ordinary, then the assumption that $\alpha^{[H:\mathbb{Q}_p]} \not\equiv 1 \bmod \mathfrak{p}$ is automatic. In the case where f is ordinary (α is the unit root in this case), if $a_p \in \mathbb{Z}_p$ and $a_p \not\equiv 1 \bmod p$, then $\alpha \in \mathbb{Z}_p^\times \setminus 1 + p\mathbb{Z}_p$, and hence $\alpha^d \not\equiv 1 \bmod p$ for any power d of p.

Proof. — Let $x \in W \otimes M$. If neither α nor β is a unit, then $A = \sum_{n\geqslant 0} \varphi^n(x)$ converges, and $(1-\varphi)A = x$. Hence, we obtain the proposition. We assume that f is ordinary. Then, $\alpha \in \mathscr{O}_{\mathfrak{p}}^\times$, and β is not a unit. In this case, we write $x = ax_\alpha + bx_\beta$, where $a, b \in W$, and $x_\alpha, x_\beta \in M$ are elements such that $\varphi x_\alpha = \alpha x_\alpha$ and $\varphi x_\beta = \beta x_\beta$ (we note that M is an $\mathscr{O}_{\mathfrak{p}}$-module). We put $d = [H : \mathbb{Q}_p]$ and

$$A_\alpha = \frac{1}{1-\alpha^d} \sum_{0\leqslant i\leqslant d-1} \varphi^i(ax_\alpha), \quad A_\beta = \sum_{n\geqslant 0} \varphi^n(bx_\beta).$$

We note that by the assumption that $\alpha^d \not\equiv 1 \mod \mathfrak{p}$, we have $A_\alpha \in W \otimes M$. Since $\sigma^d = 1$ on W, we have $(1-\varphi)(A_\alpha + A_\beta) = x$. □

6.1.2. Construction

We assume the following assumption.

Assumption B. — *For every $n \geqslant 0$, we have $\alpha^{p^n} \not\equiv 1 \bmod \mathfrak{p}$.*

Remark 6.3. — The assumption is automatic if f is non-ordinary. Even in the case where f is ordinary and α is the unit root, if $a_p \in \mathbb{Z}_p$ and $a_p \not\equiv 1 \bmod p$ then by Remark 6.2, Assumption B holds.

For a positive integer S relatively prime to p, we denote by O_S the ring of integers of $\mathbb{Q}(S)$, and for $h \in \mathbb{Z}$ we define $\mathscr{H}_S(T_f(h)) \subseteq (O_S \otimes_{\mathbb{Z}} \mathbb{Z}_p)[\![X]\!] \otimes_{\mathbb{Z}_p} D_{\mathrm{cris}}(V_f(h))$ as the submodule consisting of $G(X) \in (O_S \otimes_{\mathbb{Z}} \mathbb{Z}_p)[\![X]\!] \otimes M \otimes \mathbb{Z}_p e_{-h}$ such that $\sum_{\zeta\in\mu_p} G(\zeta(1+X)-1) = p\varphi(G(X))$. For $h \geqslant 1$, we define

$$\Sigma_{S,h,n} : \mathscr{H}_S(T_f) \to \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}(S) \otimes_{\mathbb{Q}} \mathbb{Q}_p(\zeta_{p^n}), T_f(h))$$

by $\Sigma_{S,h,n} = \prod_{v|p} \Sigma_{\mathbb{Q}(S)_v,h,n}$, where v ranges over all primes of $\mathbb{Q}(S)$ above p, and the cohomology group $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}(S) \otimes_{\mathbb{Q}} \mathbb{Q}_p(\zeta_{p^n}), T_f(h))$ may be defined as $\prod_{v|p} \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}(S)_v(\zeta_{p^n}), T_f(h))$.

Since $\mathbb{Q}(S)$ is a p-extension of $\mathbb{Q}$, Proposition 6.1 implies that the map in [2, p. 247]

$$\Delta_0 : (O_S \otimes \mathbb{Z}_p)[\![X]\!] \otimes \ M \to O_S \otimes M \ / \ (1-\varphi)O_S \otimes M; \quad g(X) \mapsto g(0)$$

is the zero-map. Hence, by the short exact sequence in the proof of [2, Lemma 4.1.3], for each $\eta \in M \otimes_{\mathscr{O}_\mathfrak{p}} \mathscr{O}_\mathfrak{p}[\alpha]$, there exists a unique $G_{S,\eta} \in \mathscr{H}_S(T_f) \otimes_{\mathscr{O}_\mathfrak{p}} \mathscr{O}_\mathfrak{p}[\alpha]$ such that

$$(1-\varphi)G_{S,\eta} = \frac{1}{S}\gamma_S^{-1}(\xi_S(1+X)\otimes\eta) = \frac{1}{S}\xi_S(1+X)^{1/S}\otimes\eta, \tag{6.4}$$

where $\xi_S := \mathrm{tr}_{\mathbb{Q}(\mu_S)/\mathbb{Q}(S)}(\zeta_S)$, and $\gamma_S \in G_\infty$ is the element such that $\kappa_{\mathrm{cyc}}(\gamma_S) = S \in \mathbb{Z}_p^\times$. By the abuse of notation, we let $\Sigma_{S,h,n}$ denote the homomorphism

$$\mathscr{H}_S(T_f)\otimes F_\mathfrak{p}[\alpha] \to \mathrm{H}^1_\mathrm{f}(\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^n}), V_f(h))\otimes F_\mathfrak{p}[\alpha]$$

obtained by extension of scalars.

For an $\mathscr{O}_\mathfrak{p}$-module B, we put

$$B^* = \mathrm{Hom}_{\mathscr{O}_\mathfrak{p}}(B, \mathscr{O}_\mathfrak{p}).$$

Proposition 6.4. — *There exists an element η_α of $D_{\mathrm{cris}}(V_f)\otimes_{\mathscr{O}_\mathfrak{p}} \mathscr{O}_\mathfrak{p}[\alpha]$ satisfying the following conditions:*

(1) *For a nonzero element $\omega \in S(f) \cong F$, we have*

$$\varphi\eta_\alpha = \alpha\eta_\alpha, \quad [\omega, \eta_\alpha] = ce_{k-1},$$

for some $c \in F^\times$, where $[-,-]$ denotes the scalar extension of the natural pairing

$$[-,-] : D_{\mathrm{cris}}(V_f)\times D_{\mathrm{cris}}(V_f) \to D_{\mathrm{cris}}(F_\mathfrak{p}(1-k))$$

induced by the isomorphism $\mathrm{Hom}_{F_\mathfrak{p}}(V_f, F_\mathfrak{p}) \cong V_f(k-1)$.

(2) *For $1 \leqslant i \leqslant k-1$, $n \geqslant 0$ and S with $(S,p)=1$, the element $\Sigma_{S,i,n}(G_{S,\eta_\alpha}^{\sigma^{-n}})$ of $\mathrm{H}^1_\mathrm{f}(\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^n}), V_f(i))\otimes\mathscr{O}_\mathfrak{p}[\alpha]$ lies in*

$$\mathrm{H}^1_{/\mathrm{f}}\left(\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^n}), T_f(k-i)\right)^*\otimes\mathscr{O}_\mathfrak{p}[\alpha],$$

which is regarded as a subgroup of $\mathrm{H}^1_\mathrm{f}(\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^n}), V_f(i))\otimes\mathscr{O}_\mathfrak{p}[\alpha]$ by the cup product (cf. [7, Proposition 3.8]*) and the isomorphism $\mathrm{Hom}_{F_\mathfrak{p}}(V_f(i), F_\mathfrak{p}(1)) \cong V_f(k-i)$.*

Proof. — By (6.3) and [13, Theorem 16.6 (1)], there exists η_α such that $\varphi\eta_\alpha = \alpha\eta_\alpha$ and $[\omega,\eta_\alpha] = e_{k-1}$. We note that the image of $\mathrm{H}^1_\mathrm{f}(\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^n}), T_f(i))$ in the vector space $\mathrm{H}^1(\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^n}), V_f(i))$ is contained in

$$\mathrm{Hom}_{\mathscr{O}_\mathfrak{p}}\left(\mathrm{H}^1_{/\mathrm{f}}\left(\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^n}), T_f(k-i)\right), \mathscr{O}_\mathfrak{p}\right).$$

It then suffices to show that there exists $c \in F^\times$ such that the element $\Sigma_{S,i,n}(c\eta_\alpha)$ of $\mathrm{H}^1_\mathrm{f}(\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^n}), V_f(i))\otimes F_\mathfrak{p}[\alpha]$ lies in the submodule $\mathrm{H}^1_\mathrm{f}(\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^n}), T_f(i))\otimes\mathscr{O}_\mathfrak{p}[\alpha]$. Since M is a lattice of $D_{\mathrm{cris}}(V_f)$, there exists $c \in F^\times$ such that $c\eta_\alpha$ lies in $M\otimes\mathscr{O}_\mathfrak{p}[\alpha]$. Since $\Sigma_{S,i,n}$ is induced by the extension of scalars of $\mathscr{H}_S(T_f) \to \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}(S) \otimes \mathbb{Q}_p(\zeta_{p^n}), T_f(i))$, we deduce that $c\eta_\alpha$ satisfies (2) as well as (1). □

By replacing ω by $c^{-1}\omega$, where $c \in F^\times$ as in Proposition 6.4(1), we obtain the following.

Corollary 6.5. — *There exists a pair*

$$(\omega, \eta_\alpha) \in S(f) \times (D_{\mathrm{cris}}(V_f) \otimes F_{\mathfrak{p}}[\alpha])$$

such that η_α satisfies the conditions (1) and (2) in Proposition 6.4, and $[\omega, \eta_\alpha] = e_{k-1} \in D_{\mathrm{cris}}(F_{\mathfrak{p}}(1-k))$.

Definition 6.6. — *In the rest of this paper, we fix a pair $(\omega, \eta_\alpha) \in S(f) \times (D_{\mathrm{cris}}(V_f) \otimes F_{\mathfrak{p}}[\alpha])$ as in Corollary 6.5. We write $G_{S,\alpha} = G_{S,\eta_\alpha} \in \mathscr{H}_S(T_f) \otimes F_{\mathfrak{p}}[\alpha]$, which is defined by* (6.4)*. For $1 \leqslant i \leqslant k-1$ and $n \geqslant 0$, we put*

$$d^\alpha_{S,i,n} = -\Sigma_{S,i,n}(G^{\sigma^{-n}}_{S,\alpha}) \in \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}(S) \otimes \mathbb{Q}_p(\zeta_{p^n}), V_f(i)) \otimes \mathscr{O}_{\mathfrak{p}}[\alpha].$$

To simplify the notation, we denote by $\Omega^\pm$ the associated periods $\Omega^\pm_\omega$ (see Definition 2.1 for the notation). We also write $\theta_{S,i} = \theta_{S,i,\omega}$ and $\vartheta_{S,i} = \vartheta_{S,i,\omega}$.

Remark 6.7.

(1) We explain how many the pairs as in the Corollary 6.5 exist. Requiring the condition in Corollary 6.5, the choice of ω is equivalent to η_α. If (ω, η_α) is as in the corollary, then for a nonzero element $c \in \mathscr{O}_{F,(p)} := F \cap \mathscr{O}_{\mathfrak{p}}$, the pair $(c^{-1}\omega, c\eta_\alpha)$ also satisfies the condition in the corollary. Hence, the set of pairs (ω, η_α) as in the corollary may be identified with $\mathscr{O}_{F,(p)} \setminus \{0\}$. We note that Theorem 1.1 holds for every pair.

(2) By the proof of Proposition 6.4, we may take a pair (ω, η_α) such that η_α is a member of a basis of the lattice $M \otimes \mathscr{O}_{\mathfrak{p}}[\alpha]$ of $D_{\mathrm{cris}}(V_f) \otimes \mathscr{O}_{\mathfrak{p}}[\alpha]$.

Proposition 6.8. — *We have the following norm relations.*

(1) *If l is a prime not dividing pS, then we have $\mathrm{Cor}_{\mathbb{Q}(Sl)/\mathbb{Q}(S)}(d^\alpha_{Sl,i,n}) = -l^{i-1}\,\mathrm{Fr}_l^{-1}\, d^\alpha_{S,i,n}$, where $\mathrm{Cor}_{\mathbb{Q}(Sl)/\mathbb{Q}(S)} : \mathrm{H}^1(\mathbb{Q}(Sl) \otimes \mathbb{Q}_p(\zeta_{p^n}), -) \to \mathrm{H}^1(\mathbb{Q}(S) \otimes \mathbb{Q}_p(\zeta_{p^n}), -)$ is induced by the corestriction maps.*

(2) *We have*

$$\mathrm{Cor}_{\mathbb{Q}_p(\zeta_{p^{n+1}})/\mathbb{Q}_p(\zeta_{p^n})}(d^\alpha_{S,i,n+1}) = \begin{cases} \alpha d^\alpha_{S,i,n} & (n \geqslant 1), \\ (\alpha - p^{i-1}\,\mathrm{Fr}_p^{-1}) d^\alpha_{S,i,0} & (n = 0), \end{cases}$$

where

$$\mathrm{Cor}_{\mathbb{Q}_p(\zeta_{p^{n+1}})/\mathbb{Q}_p(\zeta_{p^n})} : \mathrm{H}^1(\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^{n+1}}),-) \to \mathrm{H}^1(\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^n}),-)$$

denotes the corestriction map.

Proof. — By [28, 2.2.7] and [2, Lemma 4.1.3 (i)], there exists a unique $G_{S,i} \in \mathscr{H}_S(T_f(i)) \otimes F_{\mathfrak{p}}(\alpha)$ such that

$$(6.5)\qquad \begin{aligned}(1-\varphi)(G_{S,i}(X)) &= \gamma_S^{-1}(\xi_S(1+X)) \otimes \eta_\alpha \otimes e_{-i}\\ &= \xi_S(1+X)^{1/S} \otimes \eta_\alpha \otimes e_{-i}.\end{aligned}$$

Since $(D^i \otimes e_i)(\xi_S(1+X)^{1/S} \otimes \eta_\alpha \otimes e_{-i}) = \frac{1}{S^i}\xi_S(1+X)^{1/S} \otimes \eta_\alpha$, by [2, Lemma 4.1.3 (ii)] we have $(D^i \otimes e_i)G_{S,i} = S^{-(i-1)}G_{S,\alpha}$. Hence, by (6.2)

$$(6.6)\qquad d^\alpha_{S,i,n} = (-1)^{i-1}(i-1)!S^{i-1}p^{(i-1)n}\exp_{S,n,V_f(i)}(G^{\sigma^{-n}}_{S,i}(\zeta_{p^n}-1)),$$

where

$$\exp_{S,n,V_f(i)} : (\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^n})) \otimes_{\mathbb{Q}_p} \frac{D_{\mathrm{cris}}(V_f(i))}{\mathrm{Fil}^0(D_{\mathrm{cris}}(V_f(i)))} \to \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}(S)\otimes\mathbb{Q}_p(\zeta_{p^n}), V_f(i))$$

denotes the direct sum of the exponential maps. The assertion (1) follows from (6.5) and (6.6). If $n \geqslant 1$, then the assertion (2) follows from $\varphi\eta_\alpha = \alpha\eta_\alpha$ and (6.1). See [28, §2.4.2] for the case $n = 0$ (we note that $d^\alpha_{S,i,n} = (-1)^{i-1}(i-1)!S^{i-1}\Sigma_{n-1,i}(G^{\sigma^{-n}}_{S,i}(X))$ where $\Sigma_{n-1,i}$ is as in [28] and associated to $V_f(i)$). ☐

6.2. Kato's Euler system

We recall Kato's Euler system constructed in [13]. We assume the hypothesis (2) in Assumption A.

For a finite extension L of $\mathbb{Q}$ or $\mathbb{Q}_p$ and for $i, j \in \mathbb{Z}$ we denote by $\mathrm{Tw}_{j,T_f(i)}$ the composite

$$\begin{aligned}\mathrm{Tw}_{j,T_f(i)} : \varprojlim_n \mathrm{H}^1(L(\zeta_{p^n}), T_f(i)) &\to \varprojlim_n \mathrm{H}^1(L(\zeta_{p^n}), T_f(i))(j)\\ &\xrightarrow{\sim} \varprojlim_n \mathrm{H}^1(L(\zeta_{p^n}), T_f(i+j)),\end{aligned}$$

where the first map is induced by the product with $\{\zeta_{p^m}\}^{\otimes i}_{m\geqslant 1} \in \mathbb{Z}_p(i)$, and we refer the reader to [31, Proposition 6.2.1] for the second map.

For $n \geqslant 0$, we put $K_n = \mathbb{Q}(\zeta_{p^n})$, $K_\infty = \cup_{n\geqslant 0}K_n$ and $G_{p^n} = \mathrm{Gal}(K_n/\mathbb{Q})$. For a positive integer S relatively prime to p, we denote by $K_n(S)$ the compositum $K_n\mathbb{Q}(S)$. By applying [31, Lemma 9.6.1] to Kato's Euler system (cf. [13, Theorems 9.7 and 12.5]), we have the following.

Theorem 6.9. — *There exists an element*

$$\{\mathfrak{z}_{Sp^n}\}_{n\geqslant 0,(S,p)=1} \in \prod_{n,S} \mathrm{H}^1(K_n(S), T_f(k))$$

satisfying the following conditions.

(1) *For a prime $l \neq p$, we have*

$$\mathrm{Cor}_{K_n(Sl)/K_n(S)}(\mathfrak{z}_{Slp^n}) = \begin{cases} (1 - a_l l \,\mathrm{Fr}_l^{-1} + \epsilon(l) l^k \,\mathrm{Fr}_l^{-2})\mathfrak{z}_{Sp^n} & (l \nmid S), \\ \mathfrak{z}_{Sp^n} & (l \mid S). \end{cases}$$

(2) *We have $\{\mathfrak{z}_{Sp^n}\}_n \in \varprojlim_n \mathrm{H}^1(K_n(S), T_f(k))$.*

(3) *For $1 \leqslant i \leqslant k-1$, $S > 0$ and $n \geqslant 0$, we denote by $\mathfrak{z}_{Sp^n}^{(k-i)}$ the image of $\{\mathfrak{z}_{Sp^m}\}_{m\geqslant 0}$ under the composite*

$$\varprojlim_m \mathrm{H}^1(K_m(S), T_f(k)) \xrightarrow{\mathrm{Tw}_{-i,T_f(k)}} \varprojlim_m \mathrm{H}^1(K_m(S), T_f(k-i)) \to \mathrm{H}^1(K_n(S), T_f(k-i)),$$

where the second map is the natural projection. Then, for a Dirichlet character χ of $\mathrm{Gal}(K_n(S)/\mathbb{Q})$ of conductor Sp^n, we have

$$\sum_{\gamma\in\mathrm{Gal}(K_n(S)/\mathbb{Q})} \chi(\gamma) \exp^*_{S,n,V_f(i)^*(1)}(\gamma \,\mathrm{loc}_p(\mathfrak{z}_{Sp^n}^{(k-i)})) = (2\pi\sqrt{-1})^{k-i-1} \frac{L_{\{p\}}(f,\chi,i)}{\Omega_\omega^\pm} \omega \otimes e_{i-k},$$

where the sign $\pm$ is equal to that of $(-1)^{i-1}\chi(-1)$,

$$\exp^*_{S,n,V_f(i)^*(1)} : \mathrm{H}^1(K_n(S) \otimes \mathbb{Q}_p, V_f(k-i)) \to K_n(S) \otimes_{\mathbb{Q}} D_{\mathrm{cris}}(V_f(k-i))$$

denotes the sum of the dual exponential maps, and $L_{\{p\}}(f,\chi,s)$ is the L-function without Euler factor at p.

Remark 6.10.

(1) Although in [13] the integrality of such a system is verified only in the case where $S = 1$, one can generalize the arguments to general S under Assumption A (2). Let us briefly explain about it. Following [13, §13.9] (cf. [9, Definition A.1]), for $\delta \in V_f = V_{F_\mathfrak{p}}(f)$, we define $\mathbf{z}_\delta^{(p)} \in \varprojlim_m \mathrm{H}^1(K_m(S), T_f) \otimes_{\Lambda^{(S)}} Q(\Lambda^{(S)})$, where we put $\Lambda^{(S)} = \mathscr{O}[\![\mathrm{Gal}(K_\infty/\mathbb{Q})]\!][\Gamma_S]$ and $Q(\Lambda^{(S)})$ denotes its total quotient ring. By the same argument as in [13, §13.12], one can show that $\mathbf{z}_\delta^{(p)}$ lies in $\left(\varprojlim_m \mathrm{H}^1(K_m(S), T_f)\right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and that if $\delta \in T_f$ and $\mathfrak{P}$ is a height-one prime ideal of $\Lambda^{(1)}$, then $\mathbf{z}_\delta^{(p)} \in \left(\varprojlim_m \mathrm{H}^1(K_m(S), T_f)\right) \otimes_{\Lambda^{(1)}}$

$\Lambda^{(1)}_{\mathfrak{P}}$. Here, $\Lambda^{(1)}_{\mathfrak{P}}$ denotes the localization at $\mathfrak{P}$. We also note that by Shapiro's lemma, we have $\varprojlim_m \mathrm{H}^1(K_m(S), T_f) = \varprojlim_m \mathrm{H}^1(K_m, T_f \otimes \mathscr{O}[\Gamma_S])$. Under Assumption A (2), by Lemma 3.1 and applying the same argument as in [13, §13.8] to the representation $T_f \otimes \mathscr{O}[\Gamma_S]$, we have that $\varprojlim_m \mathrm{H}^1(K_m(S), T_f)$ is $\Lambda^{(1)}$-free (see also [19, Lemma 6.8.12]). Then, as in [13, §13.14], if $\delta \in T_f$, then $\mathbf{z}^{(p)}_\delta \in \varprojlim_m \mathrm{H}^1(K_m(S), T_f)$ (a similar phenomenon is observed in [19, Corollary 6.8.13]). If we put $\{\mathfrak{z}'_{Sp^n}\}_{n\geqslant 0} = \mathrm{Tw}_{k,T_f}(\mathbf{z}^{(p)}_{\delta_f^+ + \delta_f^-})$, where $\delta_f^\pm$ are as in Definition 2.1, then the system $\{\mathfrak{z}'_{Sp^n}\}_{S,n}$ satisfies the assertion (3), which follows in the same way as in the case where $S = 1$ (cf. [13, Theorem 12.5]). By [13, Proposition 8.12], it suffices to apply [31, Lemma 9.6.1] to $\{\mathfrak{z}'_{Sp^n}\}$ in order to obtain $\{\mathfrak{z}_{Sp^n}\}$ which satisfies the norm relations (1) and (2) as well as (3).

(2) By the argument as in the proof of [31, Theorem 6.3.5], for a prime $l \nmid pS$, we have

$$\mathrm{Cor}_{K_n(Sl)/K_n(S)}(\mathfrak{z}^{(k-i)}_{Slp^n}) = (1 - a_l l^{1-i}\,\mathrm{Fr}_l^{-1} + \epsilon(l) l^{k-2i}\,\mathrm{Fr}_l^{-2})\mathfrak{z}^{(k-i)}_{Sp^n}.$$

In particular, $\{\mathfrak{z}^{(k/2)}_{Sp^n}\}_{n,(S,pN)=1}$ gives rise to an Euler system in the sense of Definition 4.4.

For $n \geqslant 0$ and a square-free integer $S > 0$ relatively prime to p, we put

$$\mathfrak{Z}_{Sp^n,i} = \sum_{\gamma\in\Gamma_{Sp^n}} \gamma^{-1}\mathfrak{z}^{(k-i)}_{Sp^n} \otimes \gamma \in \mathrm{H}^1(K_n(S), T_f(k-i)) \otimes_{\mathscr{O}_\mathfrak{p}} \mathscr{O}_\mathfrak{p}[\Gamma_{Sp^n}].$$

Proposition 6.11. — *For $n \geqslant 0$ and a square-free integer $S > 0$ relatively prime to p, we have*

$$\mathfrak{Z}_{Sp^n,i} \in \mathrm{H}^1(K_n(S), T(k-i)) \otimes_{\mathscr{O}_\mathfrak{p}} I^{a_i(S)}_{K_n(S)},$$

where $a_i(S)$ denotes the number of primes l of dividing S such that $l^{i-1} - a_l + \epsilon(l)l^{k-i-1} = 0$, and we write $I_{K_n(S)}$ for the augmentation ideal of $\mathscr{O}_\mathfrak{p}[\mathrm{Gal}(K_n(S)/\mathbb{Q})]$.

Proof. — The proof is the same as that of [26, Proposition 5.10]. □

6.3. Kato's Euler system and p-adic L-functions with tame characters

We recall the p-adic L-function associated to f, which is originally constructed by [1, 34], and we describe its relation with Kato's Euler system by using local points $d^\alpha_{S,i,n}$ (cf. Definition 6.6). We assume Assumption A (2).

For $h \geqslant 1$ and a subfield L of $\mathbb{C}_p$, we put

$$\mathscr{H}_{h,L}[\![\Gamma]\!] = \left\{ \sum_{n\geqslant 0} a_n(\gamma-1)^n \in L[\![\gamma-1]\!] \,\middle|\, \lim_{n\to\infty} \frac{|a_n|_p}{n^h} = 0 \right\},$$

where $\Gamma \cong \mathbb{Z}_p$ denotes the Galois group of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$, $\gamma \in \Gamma$ is a topological generator, and $|\cdot|_p$ denotes the multiplicative valuation of $\mathbb{C}_p$. Noting $G_\infty = \Gamma \times G_p$, we put $\mathscr{H}_{h,L}[\![G_\infty]\!] = \mathscr{H}_{h,L}[\![\Gamma]\!][G_p]$. For $j \in \mathbb{Z}$, we denote by $\mathrm{Tw}_j : \mathscr{H}_{h,L}[\![G_\infty]\!] \to \mathscr{H}_{h,L}[\![G_\infty]\!]$ the twist defined as

$$\sum_{n\geqslant 0, \tau\in G_p} a_n(\gamma-1)^n\tau \mapsto \sum a_n(\kappa_{\mathrm{cyc}}(\gamma)^j\gamma-1)^n\kappa_{\mathrm{cyc}}(\tau)^j\tau.$$

Let

$$\mathrm{pr}_n : \mathscr{H}_{h,L}[\![G_\infty]\!][G_S] \to L[G_{p^n}][G_S]$$

denote the projection which is induced by $\mathscr{H}_{\infty,L}[\![G_\infty]\!]/(\gamma^{p^n}-1) \cong L[G_{p^n}]$. Here, $G_S := \mathrm{Gal}(\mathbb{Q}(\zeta_S)/\mathbb{Q})$, and $\mathscr{H}_{\infty,L}[\![G_\infty]\!] = \cup_{h\geqslant 1}\mathscr{H}_{h,L}[\![G_\infty]\!]$. For a square-free integer $S > 0$ relatively prime to p, by [23] there exists a unique $L_{p,S,\alpha}(f) \in \mathscr{H}_{k-1,F_\mathfrak{p}[\alpha]}[\![G_\infty]\!][G_S]$ such that for $0 \leqslant i \leqslant k-2$ and $n \geqslant 0$

$$\begin{aligned}(6.7)\quad &\mathrm{pr}_n \circ \mathrm{Tw}_i(L_{p,S,\alpha}(f)) \\ &= \begin{cases} \alpha^{-n}\left(\vartheta_{Sp^n,i+1} - p^{k-2}\alpha^{-1}\nu_{Sp^{n-1},Sp^n}(\vartheta_{Sp^{n-1},i+1})\right) & (n\geqslant 1), \\ (1-p^i\alpha^{-1}\,\mathrm{Fr}_p)(1-p^{k-i-2}\alpha^{-1}\,\mathrm{Fr}_p^{-1})\vartheta_{S,i+1} & (n=0), \end{cases} \\ &\qquad\qquad \in F_\mathfrak{p}(\alpha)[G_{p^n}][G_S].\end{aligned}$$

Definition 6.12. — *Let $\mathscr{L}_{p,S,\alpha}(f)$ be the image of $\mathrm{Tw}_{-1}(L_{p,S,\alpha}(f))$ under the natural projection $\mathscr{H}_{k-1,F_\mathfrak{p}[\alpha]}[\![G_\infty]\!][G_S] \to \mathscr{H}_{k-1,F_\mathfrak{p}[\alpha]}[\![G_\infty]\!][\Gamma_S]$.*

Proposition 6.13. — *The p-adic L-functions $\mathscr{L}_{p,S,\alpha}(f)$ are elements of $\mathscr{H}_{k-1,F_\mathfrak{p}[\alpha]}[\![G_\infty]\!][\Gamma_S]$ which have the following properties and are characterized by them:*

(1) *For all $1 \leqslant i \leqslant k-1$ and all characters $\chi : G_\infty \times \Gamma_S \to \overline{\mathbb{Q}}^\times$ of finite order whose conductor is divisible by S, we have*

$$\begin{aligned}(6.8)\quad &\kappa_{\mathrm{cyc}}^i\chi(\mathscr{L}_{p,S,\alpha}(f)) \\ &= e_p(\alpha,i-1,\chi)S^{i-1}p^{n(i-1)}\tau(\chi)(i-1)!(-2\pi\sqrt{-1})^{k-i-1}\frac{L(f,\chi^{-1},i)}{\Omega^\pm},\end{aligned}$$

where $n \geqslant 0$ is the integer such that p^n exactly divides the conductor of χ, the sign $\pm$ is that of $(-1)^{i-1}\chi(-1)$, and

$$e_p(\alpha,i-1,\chi) := \frac{1}{\alpha^n}\left(1-\frac{\chi^{-1}(p)p^{k-1-i}}{\alpha}\right)\left(1-\frac{\chi(p)p^{i-1}}{\alpha}\right).$$

(2) *For a prime l relatively prime to pS,*

$$\pi_{Sl/S}\left(\mathscr{L}_{p,Sl,\alpha}(f)\right) = -l^{-1}\operatorname{Fr}_l\left(1 - a_l l \operatorname{Fr}_l^{-1} + \epsilon(l)l^k \operatorname{Fr}_l^{-2}\right)\mathscr{L}_{p,S,\alpha}(f),$$

where $\pi_{Sl/S} : \mathscr{H}_{k-1}[\![G_\infty]\!][\Gamma_{Sl}] \to \mathscr{H}_{k-1}[\![G_\infty]\!][\Gamma_S]$ is induced by $\Gamma_{Sl} \to \Gamma_S$, and by abuse of notation, $\operatorname{Fr}_l \in G_\infty \times \Gamma_S$ denotes the element whose image in G_∞ is γ_S and whose image in Γ_S is Fr_l.

Remark 6.14.

(1) By our choice of periods, if f is ordinary, then we have $\mathscr{L}_{p,S,\alpha}(f) \in \mathscr{O}_\mathfrak{p}[\![G_\infty]\!][\Gamma_S]$ (cf. Corollary 6.16).
(2) The p-adic L-function $\mathscr{L}_{p,S,\alpha}(f)$ is in fact characterized by the property (2) above and the more relaxed condition as follows: for $1 \leqslant i \leqslant k-1$ and for *almost* all characters χ of $G_\infty \times \Gamma_S$ of finite order whose conductor is divisible by S, we have (6.8).

Proof. — The assertion (1) follows from (6.7) and Proposition 2.2 (2). The assertion (2) is deduced from Proposition 2.2 (1).

We next prove that our p-adic L-functions are characterized by (1) and (2). If there is another family $\{\mathscr{M}_S\}_S$ of elements of $\mathscr{H}_{k-1,F_\mathfrak{p}[\alpha]}[\![G_\infty]\!][\Gamma_S]$ satisfying the properties (1) and (2), then for each S, $\kappa^i_{\mathrm{cyc}}\chi(\mathscr{L}_{p,S,\alpha}(f)) = \kappa^i_{\mathrm{cyc}}\chi(\mathscr{M}_S)$ for all $1 \leqslant i \leqslant k-1$ and for almost all characters $\chi : G_\infty \times \Gamma_S \to \overline{\mathbb{Q}}^\times$ of finite order. Hence, by using [28, §1.3.1], we have $\mathscr{L}_{p,S,\alpha}(f) = \mathscr{M}_S$. □

For $S > 0$ with $(S,p) = 1$, the pairings induced by the cup product

$$(-,-)_{T_f(k-i),S,n} : \mathrm{H}^1(K_n(S)\otimes\mathbb{Q}_p, T_f(k-i)) \times \mathrm{H}^1(K_n(S)\otimes\mathbb{Q}_p, T_f(i)) \to \mathscr{O}_\mathfrak{p}$$

induce a paring

$$\langle -,-\rangle_{T_f(k-i),S} : Z_{\infty,S}(T_f(k-i)) \times Z_{\infty,S}(T_f(i)) \to \Lambda[\Gamma_S]$$

as follows, where $\Lambda := \mathscr{O}_\mathfrak{p}[\![G_\infty]\!]$ and $Z_{\infty,S}(-) := \varprojlim_n \mathrm{H}^1(K_n(S)\otimes\mathbb{Q}_p, -)$. For $x_\infty = (x_n) \in Z_{\infty,S}(T_f(k-i)), y_\infty = (y_n) \in Z_{\infty,S}(T_f(i))$, the pairing $\langle x_\infty, y_\infty\rangle_{T_f(k-i),S}$ is defined as the limit of

$$\sum_{\tau \in G_{p^n}\times\Gamma_S} (\tau^{-1}x_n, y_n)_{T_f(k-i),S,n}\tau \in \mathscr{O}_\mathfrak{p}[G_{p^n}][\Gamma_S]. \tag{6.9}$$

By abuse of notation, we denote by $\langle -,-\rangle_{T_f(k-i),S}$ the base change

$$\mathscr{H}_{k-1}[\![G_\infty]\!] \otimes_\Lambda Z_{\infty,S}(T_f(k-i)) \times \mathscr{H}_{k-1}[\![G_\infty]\!] \otimes_\Lambda Z_{\infty,S}(T_f(i)) \to \mathscr{H}_{k-1}[\![G_\infty]\!][\Gamma_S].$$

We put

$$\mathscr{R}_{S,\psi} = \left\{ f(X) \in (O_S \otimes \mathbb{Z}_p)[\![X]\!] \;\middle|\; \sum_{\zeta \in \mu_p} f(\zeta(1+X)-1) = 0 \right\},$$

which is the $(O_S \otimes \mathbb{Z}_p)[\![G_\infty]\!]$-submodule of $(O_S \otimes \mathbb{Z}_p)[\![X]\!]$ freely generated by $1+X$, and we put $\mathscr{D}_S(V_f) = \mathscr{R}_{S,\psi} \otimes_{\mathbb{Z}_p} D_{\mathrm{cris}}(V_f)$. Let

$$\Omega^{(0)}_{V_f,S} : \mathscr{D}_S(V_f) \otimes \mathscr{O}_{\mathfrak{p}}[\alpha] \to \mathscr{H}_{k,F_{\mathfrak{p}}(\alpha)}[\![G_\infty]\!] \otimes_{\mathscr{O}_{\mathfrak{p}}[\![G_\infty]\!]} Z_{\infty,S}(T_f)$$

be Perrin-Riou's big exponential map such that for $i, n \geqslant 1$,

$$\mathrm{pr}_n \circ \mathrm{Tw}_i \circ \Omega^{(0)}_{V_f,S}(g) = \Sigma_{S,i,n}((\sigma \otimes \varphi)^{-n} G), \tag{6.10}$$

where $(1-\varphi)G = g$, and

$$\mathrm{pr}_n : \mathscr{H}_{k,F_{\mathfrak{p}}(\alpha)}[\![G_\infty]\!] \otimes Z_{\infty,S}(T_f(i)) \to \mathrm{H}^1(K_n(S) \otimes \mathbb{Q}_p, V_f(i)) \otimes F_{\mathfrak{p}}(\alpha)$$

denotes the projection. See [28], [29, §3.3] or [2, §5] for the details (although in those paper, the quotient $Z_{\infty,S}(T_f)/\mathrm{H}^0(K_\infty(S) \otimes \mathbb{Q}_p, T_f)$ is considered, by [4, Remark II. 14] we do not need to take the quotient).

Proposition 6.15. — *We put* $g_S = -\frac{1}{S}\xi_S(1+X)^{1/S} \otimes \eta_\alpha \in \mathscr{D}_S(V_f) \otimes \mathscr{O}_{\mathfrak{p}}[\alpha]$ *and* $\mathfrak{z}_{\infty,S} = \{\mathfrak{z}_{Sp^n}\}_n \in Z_{\infty,S}(T_f(k))$. *Then,* $\langle \mathfrak{z}_{\infty,S}, \Omega^{(0)}_{V_f,S}(g_S)\rangle_{T_f(k),S} = \mathscr{L}_{p,S,\alpha}(f)$.

Proof. — Let $\mathscr{M}_S = \langle \mathfrak{z}_{\infty,S}, \Omega^{(0)}_{V_f,S}(g_S)\rangle_{T_f(k),S}$. Since $\eta_\alpha \in D_{\mathrm{cris}}(V_f)$ is an eigenvector such that the slope of its eigenvalue is less than $k-1$, $\mathscr{M}_S$ lies in $\mathscr{H}_{k-1,F_{\mathfrak{p}}(\alpha)}[\![G_\infty]\!][\Gamma_S]$ (cf. [13, Theorem 16.4]). Hence, it suffices to show that $\mathscr{M}_S$ verifies the properties (1) and (2) in Proposition 6.13.

(1). — We verify the slightly more relaxed condition in Remark 6.14 (2). Let χ be a character of $G_\infty \times \Gamma_S$ of finite order whose conductor is Sp^n with $n \geqslant 1$. Let $G_{S,i} \in \mathscr{H}_S(T_f(i)) \otimes F_{\mathfrak{p}}[\alpha]$ be as in (6.5). Then, by [28,

§3.6.1], for $1 \leqslant i \leqslant k-1$ we have

$$
\begin{aligned}
(6.11)\quad & \kappa_{\mathrm{cyc}}^{i}\chi(\mathscr{M}_S) \\
&= \chi \mathrm{Tw}_i\left(\langle \mathfrak{z}_{\infty,S}, \Omega^{(0)}_{V_f,S}(g_S)\rangle_{T_f(k),S}\right) \\
&= \chi\langle \mathrm{Tw}_{-i,T_f(k)}\left(\mathfrak{z}_{\infty,S}\right), \mathrm{Tw}_i(\Omega^{(0)}_{V_f,S}(g_S))\rangle_{T_f(k-i),S} \\
&= -\chi\left(\sum_{\tau\in G_{p^n}\times\Gamma_S}\left(\tau^{-1}\mathfrak{z}^{(k-i)}_{Sp^n}, \Sigma_{S,i,n}((\sigma\otimes\varphi)^{-n}G_{S,\alpha})\right)_{T_f(k-i),S,n}\tau\right) \\
&= -\chi\left(\sum_{\tau}\left(\tau^{-1}\mathfrak{z}^{(k-i)}_{Sp^n}, \frac{1}{\alpha^n}\Sigma_{S,i,n}(G^{\sigma^{-n}}_{S,\alpha})\right)_{T_f(k-i),S,n}\tau\right) \\
&= -\frac{(-1)^i S^{i-1}p^{(i-1)n}}{\alpha^n} \\
&\qquad \times\sum_{\tau}\left(\tau^{-1}\mathfrak{z}^{(k-i)}_{Sp^n}, \exp_{S,n,V_f(i)}(G^{\sigma^{-n}}_{S,i}(\zeta_{p^n}-1))\right)_{T_f(k-i),S,n}\chi(\tau) \\
&= \frac{(-1)^{i-1} S^{i-1}p^{(i-1)n}}{\alpha^n} \\
&\qquad \times\sum_{\tau}\left[\exp^{*}_{S,n,V_f(i)^*}(\tau^{-1}\mathfrak{z}^{(k-i)}_{Sp^n}), G^{\sigma^{-n}}_{S,i}(\zeta_{p^n}-1)\right]_{S,n}\chi(\tau),
\end{aligned}
$$

where

- $[-,-]_{S,n}$ denotes the composite

$$
\begin{aligned}
(K_n(S)\otimes D_{\mathrm{cris}}(V_f(k-i)))\times(K_n(S)\otimes D_{\mathrm{cris}}(V_f(i))) \\
\to K_n(S)\otimes D_{\mathrm{cris}}(F_{\mathfrak{p}}(1))\to F_{\mathfrak{p}}.
\end{aligned}
$$

  Here, the first map is the natural pairing, and the last map is the tensor product of the trace map $K_n(S)\to\mathbb{Q}$ and the natural identification $D_{\mathrm{cris}}(F_p(1)) = F_p$.
- the fourth equality follows from $\varphi\eta_\alpha = \alpha\eta_\alpha$.
- the fifth equality follows from (6.6).

Since χ is primitive as a character of $\Gamma_S\times G_{p^n}$ and $(\varphi G^{\sigma^{-n}}_{S,i})(\zeta_{p^n}-1) = G^{\sigma^{-(n-1)}}_{S,i}(\zeta_{p^{n-1}}-1)$, by Theorem 6.9 (3), (6.5) and Corollary 6.5, we have that the last term of the computation (6.11) is equal to $\kappa^i_{\mathrm{cyc}}\chi(\mathscr{L}_{p,S,\alpha}(f))$.

(2). — It follows from Proposition 6.8 and the norm relation of $\{\mathfrak{z}_{Sp^n}\}$. □

Corollary 6.16. — *For $1 \leqslant i \leqslant k-1$ and $n \geqslant 0$,*

$$\begin{aligned}&\mathrm{pr}_n \circ \mathrm{Tw}_i(\mathscr{L}_{p,S,\alpha}(f))\\ &= \begin{cases} \alpha^{-n} \sum_{\tau \in G_{p^n} \times \Gamma_S} \left(\tau^{-1} \mathrm{loc}_p(\mathfrak{z}_{Sp^n}^{(k-i)}), d_{S,i,n}^{\alpha}\right)_{T_f(k-i),S,n} \tau & (n \geqslant 1), \\ \sum_{\tau \in \Gamma_S} \left(\tau^{-1} \mathrm{loc}_p(\mathfrak{z}_S^{(k-i)}), (1 - p^{i-1}\alpha^{-1} \mathrm{Fr}_p^{-1}) d_{S,i,0}^{\alpha}\right) \tau & (n = 0), \end{cases}\\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \in F(\alpha)[G_{p^n}][\Gamma_S].\end{aligned}$$

Moreover, if f is ordinary, then the p-adic L-function $\mathscr{L}_{p,S,\alpha}(f)$ lies in $\mathscr{O}_{\mathfrak{p}}[\![G_\infty]\!][\Gamma_S] := \varprojlim_n \mathscr{O}_{\mathfrak{p}}[G_{p^n}][\Gamma_S]$.

Proof. — The first assertion follows from Propositions 6.8 and 6.15.

If f is ordinary, then by Proposition 6.4 (2), for $n \geqslant 1$ the projection $\mathrm{pr}_n \circ \mathrm{Tw}_i \circ \Omega_{V_f,S}^{(0)}(g_S) = \frac{1}{\alpha^n} d_{S,i,n}^{\alpha}$ lies in $\mathrm{H}^1_{/\mathrm{f}}(K_n(S) \otimes \mathbb{Q}_p, T_f(k-i))^*$. Therefore,

$$\alpha^{-n} \sum_{\tau \in G_{p^n} \times \Gamma_S} \left(\tau^{-1} \mathrm{loc}_p(\mathfrak{z}_{Sp^n}^{(k-i)}), d_{S,i,n}^{\alpha}\right)_{T_f(k-i),S,n} \tau \in \mathscr{O}_{\mathfrak{p}}[G_{p^n}][\Gamma_S].$$

Hence, by the first assertion and [28, §3.6.1], $\mathscr{L}_{p,S,\alpha}(f) \in \mathscr{O}_{\mathfrak{p}}[\![G_\infty]\!][\Gamma_S]$. □

Definition 6.17. — *For $1 \leqslant i \leqslant k-1$, $n \geqslant 1$ and a positive integer S relatively prime to p, we put*

$$\begin{aligned} \theta_{Sp^n,i,\alpha} &= \begin{cases} \theta_{Sp^n,i} - p^{k-2}\alpha^{-1} \nu_{Sp^{n-1},Sp^n}(\theta_{Sp^{n-1},i}) & (n \geqslant 2), \\ \theta_{Sp,i} - (p-1)p^{k-2}\alpha^{-1}\theta_{S,i} & (n = 1), \end{cases}\\ &\quad \in F_{\mathfrak{p}}[\Gamma_{Sp^n}] \otimes \mathscr{O}_{\mathfrak{p}}[\alpha],\\ z_{Sp^n}^{(i)} &= \mathrm{Cor}_{K_n(S)/\mathbb{Q}(Sp^n)}\left(\mathfrak{z}_{Sp^n}^{(i)}\right) \in \mathrm{H}^1(\mathbb{Q}(Sp^n), T_f(i)),\\ c_{Sp^n,\alpha}^{(i)} &= \mathrm{Cor}_{K_n(S)/\mathbb{Q}(Sp^n)}\left(d_{S,i,n}^{\alpha}\right) \in \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, V_f(i)) \otimes \mathscr{O}_{\mathfrak{p}}[\alpha] \end{aligned}$$

where by abuse of notation, we denote by $\mathrm{Cor}_{K_n(S)/\mathbb{Q}(Sp^n)}$ the corestriction map $\mathrm{H}^1(K_n(S) \otimes \mathbb{Q}_p, -) \to \mathrm{H}^1(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, -)$. For $n = 0$, we define $z_S^{(i)} = \mathfrak{z}_S^{(i)} \in \mathrm{H}^1(\mathbb{Q}(S), T_f(i))$, which coincides with $z_{Sp}^{(i)}$ (we note that $\mathbb{Q}(Sp) = \mathbb{Q}(S)$).

We note that by (6.7), for $n \geqslant 1$, $\alpha^{-n}\theta_{Sp^n,i,\alpha}$ is equal to the image of $\mathrm{pr}_n \circ \mathrm{Tw}_i(\mathscr{L}_{p,S,\alpha}(f))$ in $F_{\mathfrak{p}}[\alpha][\Gamma_{Sp^n}]$. Hence, Proposition 6.15, (6.10) and Proposition 6.4 (2) imply the following corollary.

Corollary 6.18. — *If $(S, p) = 1$ and $n \geqslant 1$, then*

$$\theta_{Sp^n,i,\alpha} = \sum_{\tau \in \Gamma_{Sp^n}} \left(\tau^{-1} \mathrm{loc}_p(z_{Sp^n}^{(k-i)}), c_{Sp^n,\alpha}^{(i)}\right)_{T_f(k-i),S,n} \tau \quad \in \mathscr{O}_{\mathfrak{p}}[\alpha][\Gamma_{Sp^n}].$$

PROPOSITION 6.19.

(1) *For* $n \geqslant 1$, $\pi_{\mathbb{Q}(Sp^{n+1})/\mathbb{Q}(Sp^n)}(\theta_{Sp^{n+1},i,\alpha}) = \alpha\theta_{Sp^n,i,\alpha}$ *where* $\pi_{\mathbb{Q}(Sp^{n+1})/\mathbb{Q}(Sp^n)} : \mathbb{C}_p[\Gamma_{Sp^{n+1}}] \to \mathbb{C}_p[\Gamma_{Sp^n}]$ *denotes the natural projection.*

(2) *We have* $\theta_{Sp,i,\alpha} = \alpha(1 - p^{i-1}\alpha^{-1}\,\mathrm{Fr}_p)(1 - p^{k-i-1}\alpha^{-1}\,\mathrm{Fr}_p^{-1})\theta_{S,i}$ *in* $\mathscr{O}_{\mathfrak{p}}[\alpha][\Gamma_{Sp}] = \mathscr{O}_{\mathfrak{p}}[\alpha][\Gamma_S]$.

Proof. — The proposition follows from simple computation combined with Proposition 2.2 (1). □

6.4. Mazur–Tate elements and Kato's Euler system

Finally we construct local points to connect Mazur–Tate elements with Kato's Euler system. We keep the same assumption and notation as in the previous section. In particular, we assume Assumptions A (2) and B.

LEMMA 6.20. — *Under Assumption B, there exists a root* $\alpha \in \mathbb{C}_p$ *of* $X^2 - a_pX + p^{k-1}$ *such that* $\mathrm{ord}_p(\alpha) < k-1$, *and for* $1 \leqslant i \leqslant k-1$ *and* $m \in \mathbb{Z}$, *we have* $\mathrm{ord}_p(1 - (p^{k-i-1}\alpha^{-1})^m) \leqslant 0$.

Proof. — In the case where f is ordinary, it suffices to take α to be the unit root (we need Assumption B only for the case where $i = k-1$).

We next consider the case where f is non-ordinary. Then, all the roots α and β satisfy $\mathrm{ord}_p(\alpha) < k-1$ and $\mathrm{ord}_p(\beta) < k-1$. If $\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta) = k-i-1$ for some $1 \leqslant i \leqslant k-1$, then $k-1 = \mathrm{ord}_p(\alpha\beta) = 2(k-i-1)$, which contradicts the assumption that k is even. Hence, there is a root α such that for all $1 \leqslant i \leqslant k-1$, we have $\mathrm{ord}_p(\alpha) \neq k-i-1$, which implies that for $m \in \mathbb{Z}$ we have $\mathrm{ord}_p(1 - (p^{k-i-1}\alpha^{-1})^m) \leqslant 0$. □

We consider the following assumption.

ASSUMPTION C. — *If a root* α *of* $X^2 - a_pX + p^{k-1}$ *lies in* $F_{\mathfrak{p}}$, *then* $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$, *where* β *is the other root.*

PROPOSITION 6.21. — *If either* $F_{\mathfrak{p}}/\mathbb{Q}_p$ *is unramified or* f *is ordinary, then Assumption C holds.*

Proof. — The case where f is ordinary is immediate. We assume that $F_{\mathfrak{p}}/\mathbb{Q}_p$ is unramified and that $\alpha \in F_{\mathfrak{p}}$, which implies that $\beta \in F_{\mathfrak{p}}$. Since F_p is unramified, $\mathrm{ord}_p(\alpha)$ and $\mathrm{ord}_p(\beta)$ are integers. If $\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta)$, then $\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_p(p^{k-1}) = k-1$ is even, which contradicts the assumption that k is even. □

Theorem 6.22. — *Let S be a positive integer relatively prime to p. Let $c_{Sp^n}^{(i)}$ be the elements defined in* (6.13), (6.15), (6.16) *or* (6.17) *below.*

(1) *For $n \geqslant 0$ and $1 \leqslant i \leqslant k-1$,*

$$\theta_{Sp^n,i} = \sum_{\tau \in \Gamma_{Sp^n}} \left(\tau^{-1} \operatorname{loc}_p \left(z_{Sp^n}^{(k-i)}\right), c_{Sp^n}^{(i)}\right)_{T_f(k-i),S,n} \tau \in F_{\mathfrak{p}}[\Gamma_{Sp^n}]. \tag{6.12}$$

(2) *The element $c_S^{(i)}$ lies in $\mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}(S) \otimes \mathbb{Q}_p, T_f(k-i))^* \otimes \mathscr{O}_{\mathfrak{p}}[\alpha]$, and hence $\theta_{S,i}$ also lies in the integral ring $\mathscr{O}_{\mathfrak{p}}[\Gamma_S]$.*

(3) *Under Assumption C, for $n \geqslant 1$, $c_{sp^n}^{(i)} \in \mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, T_f(k-i))^*$, and hence $\theta_{Sp^n,i} \in \mathscr{O}_{\mathfrak{p}}[\Gamma_{Sp^n}]$.*

Remark 6.23. — Even without assuming Assumption A (2) or Assumption B, we may obtain at least the assertion (1). The reason that we are assuming those assumption in this section is to guarantee the integrality of $c_{Sp^n}^{(i)}$ and $z_{Sp^n}^{(i)}$.

In the rest of this section, we prove Theorem 6.22. Let α be a root of $X^2 - a_p X + p^{k-1}$ such that $\operatorname{ord}_p(\alpha) < k-1$, and β the other root.

6.4.1. The case where $n = 0$

Let α be as in Lemma 6.20. We define $c_S^{(i)}$ by

$$c_S^{(i)} = (1-p^{k-i-1}\alpha^{-1} \operatorname{Fr}_p^{-1})^{-1} d_{S,i,0}^{\alpha} \in \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}(S) \otimes \mathbb{Q}_p, V_f(i)) \otimes \mathscr{O}_{\mathfrak{p}}[\alpha]. \tag{6.13}$$

By Corollary 6.18 and Propositions 6.8 and 6.19, we obtain (6.12) for $n = 0$, that is,

$$\theta_{S,i} = \sum_{\tau \in \Gamma_S} (\tau^{-1} \operatorname{loc}_p(z_S^{(k-i)}), c_S^{(i)})_{T_f(k-i),S,0} \tau. \tag{6.14}$$

We note that since $\operatorname{ord}_p\left(1 - (p^{k-i-1}\alpha^{-1})^{[\mathbb{Q}(S)_v : \mathbb{Q}_p]}\right) \leqslant 0$, where v is any prime of $\mathbb{Q}(S)$ above p, we have $(1 - p^{k-i-1}\alpha^{-1} \operatorname{Fr}_p^{-1})^{-1} \in \mathscr{O}_{\mathfrak{p}}[\alpha][\Gamma_S]$, and hence Proposition 6.4 (2) implies the assertion (2).

6.4.2. The case where $n \geqslant 1$

In the following, we construct $c_{Sp^n}^{(i)}$ for $n \geqslant 1$ and complete the proof of the theorem. We assume Assumption C holds. In order to obtain (6.12) without assuming Assumption C, it suffices to consider $c_{Sp^n}^{(i)}$ as in (6.15) below (even if f is non-ordinary, the construction and the proof of (6.12) works).

The case where f is ordinary

In this case, α is the unit root of $X^2 - a_pX + p^{k-1}$, and $\alpha \in F_{\mathfrak{p}}$. We define $c_{Sp^n}^{(i)}$ $(n \geqslant 1)$ inductively by

$$c_{Sp^n}^{(i)} = \begin{cases} c_{Sp,\alpha}^{(i)} + (p-1)p^{k-2}\alpha^{-1}c_S^{(i)} & (n=1), \\ c_{Sp^n,\alpha}^{(i)} + \alpha^{-1}p^{k-2}\operatorname{res}_{n-1,n}(c_{Sp^{n-1}}^{(i)}) & (n \geqslant 2), \end{cases} \tag{6.15}$$

where $\operatorname{res}_{n-1,n} : \mathrm{H}^1(\mathbb{Q}(Sp^{n-1}) \otimes \mathbb{Q}_p, V_f(i)) \to \mathrm{H}^1(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, V_f(i))$ denotes the map induced by the restriction maps. Since $c_S^{(i)} \in \mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}(S) \otimes \mathbb{Q}_p, T_f(k-i))^*$ and since $c_{Sp^n,\alpha}^{(i)} \in \mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, T_f(k-i))^*$ for $n \geqslant 1$, we have $c_{Sp^n}^{(i)} \in \mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, T_f(k-i))^*$.

The assertion (6.12) follows from (6.14), Corollary 6.18 and the definition of $\theta_{Sp^n,i,\alpha}$.

The case where $\alpha \notin F_{\mathfrak{p}}$

In this case, for $n \geqslant 1$ we define $c_{Sp^n}^{(i)} \in \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, V_f(i))$ by

$$\alpha c_{Sp^n,\alpha}^{(i)} = \alpha c_{Sp^n}^{(i)} + y, \tag{6.16}$$

where y is an element of $\mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, V_f(i))$. We note that since for $1 \leqslant i \leqslant k-1$, $c_{Sp^n,\alpha}^{(i)} \in \mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, T_f(k-i))^* \otimes \mathscr{O}_{\mathfrak{p}}[\alpha]$, the element $c_{Sp^n}^{(i)}$ lies in $\mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, T_f(k-i))^*$.

The assertion (6.12) follows from Corollary 6.18 and from that $\theta_{Sp^n,i} \in F_{\mathfrak{p}}[\Gamma_{Sp^n}] \subsetneq F_{\mathfrak{p}}[\Gamma_{Sp^n}][\alpha]$.

The case where $\operatorname{ord}_p(\alpha) \neq \operatorname{ord}_p(\beta)$ and f is non-ordinary

In this case, β also satisfies $\operatorname{ord}_p(\beta) < k-1$ and then, the results in the previous section may be applied with replacing α by β. For $n \geqslant 1$, we define

$$c_{Sp^n}^{(i)} = \frac{\alpha c_{Sp^n,\alpha}^{(i)} - \beta c_{Sp^n,\beta}^{(i)}}{\alpha - \beta}. \tag{6.17}$$

Since $\operatorname{ord}_p(\alpha) \neq \operatorname{ord}_p(\beta)$, for any $i \geqslant 0$ the element $c_{Sp^n}^{(i)}$ lies in $\mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}_p \otimes \mathbb{Q}(Sp^n), T_f(k-i))^*$. The assertion (6.12) follows from Corollary 6.18 and

$$\theta_{Sp^n,i} = \frac{\alpha\theta_{Sp^n,i,\alpha} - \beta\theta_{Sp^n,i,\beta}}{\alpha - \beta}.$$

7. Proof of the results

We prove the theorems stated in Section 1 (Theorems 7.2, 7.4 and Corollary 7.5). We also prove a result on exceptional zeros of Mazur–Tate elements (Theorem 7.3).

We keep the same notation as in the previous section. We write $\theta_{Sp^n} = \theta_{Sp^n,k/2}$ and $\theta_{Sp^n,\alpha} = \theta_{Sp^n,k/2,\alpha}$, where α is a root of $X^2 - a_pX + p^{k-1}$ satisfying such that $\mathrm{ord}_p(\alpha) < k-1$. We put $\{z_{Sp^n}\}_{S\in\mathscr{N},n\geqslant 0} = \{z^{(k/2)}_{Sp^n}\}_{S\in\mathscr{N},n\geqslant 0}$ (cf. Definition 6.17), which is an Euler system for $T = T_f(k/2)$ in the sense of Definition 4.4. Here, $\mathscr{N}$ is the set of square-free, positive integers relatively prime to pN, with the convention that $1 \in \mathscr{N}$.

7.1. Applications of local points $c^{(k/2)}_{Sp^n,\alpha}$ and $c^{(k/2)}_{Sp^n}$

7.1.1. Proof of a part of Theorem 1.1

Corollary 7.1. — *Assume Assumptions A and B. Let S be a positive integer relatively prime to pN such that every prime $l \mid S$ satisfies* (1.1).

(1) *We have*

$$\theta_S \in I_S^{\min\{p,\mathfrak{r}_f\}}, \quad \theta_{Sp^n,\alpha} \in I_{Sp^n}^{\min\{p,\mathfrak{r}_f\}} \otimes \mathscr{O}_\mathfrak{p}[\alpha] \ \ \textit{for } n \geqslant 1.$$

(2) *If Assumption C holds, then for $n \geqslant 1$, we have $\theta_{Sp^n} \in I_{Sp^n}^{\min\{p,\mathfrak{r}_f\}}$.*

Proof. — If we denote by S' the square-free integer divisible by the prime factors of S, then $\Gamma_S = \Gamma_{S'}$. Hence, we may assume that S is square-free.

We first prove the assertion on $\theta_{Sp^n,\alpha}$. Since $c^{(k/2)}_{Sp^n,\alpha} \in \mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, T)^* \otimes \mathscr{O}_\mathfrak{p}[\alpha]$ (cf. Definition 6.17), it induces a homomorphism of $\mathscr{O}_\mathfrak{p}$-modules

$$\mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}(Sp^n) \otimes \mathbb{Q}_p, T) \otimes \mathscr{O}_\mathfrak{p}[\Gamma_{Sp^n}] \to \mathscr{O}_\mathfrak{p}[\alpha][\Gamma_{Sp^n}] \tag{7.1}$$

which sends $\sum_{\tau\in\Gamma_{Sp^n}} a_\tau \otimes \tau$ to $\sum_\tau (a_\tau, c^{(k/2)}_{Sp^n})_{T,S,n}\tau$. If we regard the $\mathscr{O}_\mathfrak{p}$-module $\mathrm{H}^1_{/\mathrm{f}}(\mathbb{Q}(Sp^n)\otimes\mathbb{Q}_p, T)\otimes\mathscr{O}_\mathfrak{p}[\Gamma_{Sp^n}]$ as an $\mathscr{O}_\mathfrak{p}[\Gamma_{Sp^n}]$-module by its action on the second factor, then the map (7.1) is a homomorphism of $\mathscr{O}_\mathfrak{p}[\Gamma_{Sp^n}]$-modules. Since (7.1) sends $\sum_\tau \tau^{-1} z_{Sp^n} \otimes \tau$ to $\theta_{Sp^n,\alpha}$ (by Corollary 6.18), by Theorem 5.9 we obtain the assertion (1).

The other assertions similarly follow from Theorem 6.22. □

The following is a part of the main result.

Theorem 7.2. — *Under the assumption and notation as in Corollary 7.1, assume further that $F_{\mathfrak{p}}/\mathbb{Q}_p$ is unramified and that every prime $l \mid S$ satisfies $p^2 \nmid l-1$. Then, for $n = 1, 2$, we have*

$$\theta_{Sp^n,\alpha} \in I_{Sp^n}^{\min\{p,r_f\}} \otimes \mathscr{O}_{\mathfrak{p}}[\alpha], \quad \theta_{Sp^n} \in I_{Sp^n}^{\min\{p,r_f\}}, \quad \text{and} \quad \theta_S \in I_S^{\min\{p,r_f\}}.$$

Proof. — By using Corollary 5.11 instead of Theorem 5.9 and by Proposition 6.21, the same argument as in the proof of Corollary 7.1, we deduce the theorem. □

7.1.2. Exceptional zeros

By Proposition 6.11 and Theorem 6.22, following the same argument of the proof of Corollary 7.1, we obtain the following theorem on the exceptional zeros of Mazur–Tate elements.

Theorem 7.3. — *Assume Assumptions A (2) and B. Let S be a positive integer relatively prime to p and n a non-negative integer. If either Assumption C holds or $n = 0$, then for $1 \leqslant i \leqslant k-1$, we have $\theta_{Sp^n,i} \in I_{Sp^n}^{a_i(S)}$,where we recall that $a_i(S)$ denotes the number of primes dividing S such that $l^{i-1} - a_l + \epsilon(l)l^{k-i-1} = 0$.*

7.2. Proof of the main result

It remains to prove Theorems 1.1 under (b) and 1.3.

Theorem 7.4. — *Assume Assumptions A and B. Assume also that the p-parity conjecture holds. Let S be a positive integer relatively prime to pN such that every prime $l \mid S$ satisfies* (1.1)*. Then, the following assertions hold.*

1. *We have $\theta_S \in I_S^{\min\{r_f,p\}}$, and for $n \geqslant 1$, $\theta_{Sp^n,\alpha} \in I_{Sp^n}^{\min\{r_f,p\}} \otimes \mathscr{O}_{\mathfrak{p}}[\alpha]$.*
2. *Assume further Assumption C (which holds if $F_{\mathfrak{p}}/\mathbb{Q}_p$ is unramified). Then, for $n \geqslant 1$ we have $\theta_{Sp^n} \in I_{Sp^n}^{\min\{r_f,p\}}$.*

Proof. — We first note that Proposition 2.5 implies that

$$\theta_{Sp^n,\alpha} = (-1)^{\frac{k}{2}} \varepsilon_f \operatorname{Fr}_{-N}^{-1} \iota(\theta_{Sp^n,\alpha}). \tag{7.2}$$

Let $R = \mathscr{O}_{\mathfrak{p}}[\alpha]$ (resp. $R = \mathscr{O}_{\mathfrak{p}}$) and $\Theta_{Sp^n} = \theta_{Sp^n,\alpha}$ (resp. $\Theta_{Sp^n} = \theta_{Sp^n}$). Lemma 3.5 (1) implies that $\mathfrak{r}_f \leqslant r_f \leqslant \mathfrak{r}_f + 1$. By Corollary 7.1, we may assume that $1 \leqslant r_f = \mathfrak{r}_f + 1 \leqslant p$. Then, we have $\Theta_{Sp^n} \in I_{Sp^n}^{r_f-1} \otimes_{\mathscr{O}_{\mathfrak{p}}} R$. Since

ι acts on $I_{Sp^n}^{r_f-1}/I_{Sp^n}^{r_f}$ by the multiplication by $(-1)^{r_f-1}$ and since Γ_{Sp^n} acts on $I_{Sp^n}^{r_f-1}/I_{Sp^n}^{r_f}$ trivially, Proposition 2.5 or (7.2) implies that

$$\Theta_{Sp^n} \equiv \varepsilon_f(-1)^{r_f-1+\frac{k}{2}}\Theta_{Sp^n} \mod I_{Sp^n}^{r_f} \otimes_{\mathscr{O}_\mathfrak{p}} R.$$

Then, by (2.3) and the assumption that $\mathrm{ord}_{s=k/2}(L(f,s)) \equiv r_f \bmod 2$, we conclude the theorem. □

Corollary 7.5. — *Assume Assumptions A and B. Let S be a positive integer relatively prime to pN such that every prime $l \mid S$ satisfies* (1.1)*. If f is ordinary, then $\mathscr{L}_{p,S,\alpha}(f) \in \mathscr{O}_\mathfrak{p}[\![G_\infty]\!][\Gamma_S]$, and $\mathscr{L}_{p,S,\alpha}(f) \in I_{\infty,S,k/2}^{\min\{r_f,p\}}$,where $I_{\infty,S,k/2}$ is as in Theorem 1.3.*

Proof. — The assertion that $\mathscr{L}_{p,S,\alpha}(f) \in \mathscr{O}_\mathfrak{p}[\![G_\infty]\!][\Gamma_S]$ is proved in Corollary 6.16. If we put $\Xi_{Sp^n} = \mathrm{pr}_n \circ \mathrm{Tw}_{k/2}(\mathscr{L}_{p,S,\alpha}(f)) \in \mathscr{O}_\mathfrak{p}[G_{p^n}][\Gamma_S]$, then it suffices to show that for every $n \geqslant 1$

$$\Xi_{Sp^n} \in \mathscr{I}_n^{\min\{r_f,p\}}, \tag{7.3}$$

where $\mathscr{I}_n^{\min\{r_f,p\}}$ denotes the augmentation ideal of $\mathscr{O}_\mathfrak{p}[G_{p^n}][\Gamma_S]$. By Corollaries 6.16 and 6.18, the image of Ξ_{Sp^n} under $\mathscr{O}_\mathfrak{p}[G_{p^n}][\Gamma_S] \to \mathscr{O}_\mathfrak{p}[\Gamma_{p^n}][\Gamma_S]$ coincides with $\theta_{Sp^n,\alpha}$. Hence, since Γ_{p^n} is the p-Sylow subgroup of G_{p^n}, [26, Lemma 5.3] and Theorem 7.4 imply (7.3). □

BIBLIOGRAPHY

[1] Y. Amice & J. Vélu, "Distributions p-adiques associées aux séries de Hecke", in *Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974)*, Astérisque, vol. 24-25, Société Mathématique de France, 1975, p. 119-131.

[2] D. Benois, "On Iwasawa theory of crystalline representations", *Duke Math. J.* **104** (2000), no. 2, p. 211-267.

[3] D. Benois & L. Berger, "Théorie d'Iwasawa des représentations cristallines. II", *Comment. Math. Helv.* **83** (2008), no. 3, p. 603-677.

[4] L. Berger, "Bloch and Kato's exponential map: three explicit formulas", *Doc. Math.* **Extra Vol.** (2003), p. 99-129, Kazuya Kato's fiftieth birthday.

[5] ———, "Limites de représentations cristallines", *Compos. Math.* **140** (2004), no. 6, p. 1473-1498.

[6] L. Berger, H. Li & H. J. Zhu, "Construction of some families of 2-dimensional crystalline representations", *Math. Ann.* **329** (2004), no. 2, p. 365-377.

[7] S. Bloch & K. Kato, "L-functions and Tamagawa numbers of motives", in *The Grothendieck Festschrift, Vol. I*, Progress in Mathematics, vol. 86, Birkhäuser, 1990, p. 333-400.

[8] H. Darmon, "A refined conjecture of Mazur-Tate type for Heegner points", *Invent. Math.* **110** (1992), no. 1, p. 123-146.

[9] D. Delbourgo, *Elliptic curves and big Galois representations*, London Mathematical Society Lecture Note Series, vol. 356, Cambridge University Press, 2008, x+281 pages.

[10] F. Diamond & J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer, 2005, xvi+436 pages.

[11] T. Dokchitser & V. Dokchitser, "On the Birch-Swinnerton–Dyer quotients modulo squares", *Ann. Math.* **172** (2010), no. 1, p. 567-596.

[12] C. Gomez, "On Mazur–Tate type conjectures for quadratic imaginary fields and elliptic curves", PhD Thesis, McGill University, 2014.

[13] K. Kato, "p-adic Hodge theory and values of zeta functions of modular forms", in *Cohomologies p-adiques et applications arithmétiques. III*, Astérisque, vol. 295, Société Mathématique de France, 2004, p. 117-290.

[14] C.-H. Kim, "An anticyclotomic Mazur-Tate conjecture for modular forms", 2018, `https://arxiv.org/abs/1612.03743`.

[15] S.-i. Kobayashi, "Iwasawa theory for elliptic curves at supersingular primes", *Invent. Math.* **152** (2003), no. 1, p. 1-36.

[16] M. Kurihara, "On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I", *Invent. Math.* **149** (2002), no. 1, p. 195-224.

[17] ———, "Refined Iwasawa theory for p-adic representations and the structure of Selmer groups", *Münster J. Math.* **7** (2014), no. 1, p. 149-223.

[18] A. Lei, "Iwasawa theory for modular forms at supersingular primes", *Compos. Math.* **147** (2011), no. 3, p. 803-838.

[19] A. Lei, D. Loeffler & S. L. Zerbes, "Euler systems for Rankin-Selberg convolutions of modular forms", *Ann. Math.* **180** (2014), no. 2, p. 653-771.

[20] M. Longo & S. Vigni, "A refined Beilinson-Bloch conjecture for motives of modular forms", *Trans. Am. Math. Soc.* **369** (2017), no. 10, p. 7301-7342.

[21] B. Mazur & K. Rubin, "Kolyvagin systems", *Mem. Am. Math. Soc.* **168** (2004), no. 799, p. viii+96.

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

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

[24] J. Nekovář, "Kolyvagin's method for Chow groups of Kuga-Sato varieties", *Invent. Math.* **107** (1992), no. 1, p. 99-125.

[25] ———, *Selmer complexes*, Astérisque, vol. 310, Société Mathématique de France, 2006, viii+559 pages.

[26] K. Ota, "Kato's Euler system and the Mazur-Tate refined conjecture of BSD type", *Am. J. Math.* **140** (2018), no. 2, p. 495-542.

[27] R. Otsuki, "Construction of a homomorphism concerning Euler systems for an elliptic curve", *Tokyo J. Math.* **32** (2009), no. 1, p. 253-278.

[28] B. Perrin-Riou, "Théorie d'Iwasawa des représentations p-adiques sur un corps local", *Invent. Math.* **115** (1994), no. 1, p. 81-161, with an appendix by Jean-Marc Fontaine.

[29] ———, "Théorie d'Iwasawa et loi explicite de réciprocité", *Doc. Math.* **4** (1999), p. 219-273.

[30] K. A. Ribet, "On l-adic representations attached to modular forms. II", *Glasg. Math. J.* **27** (1985), p. 185-194.

[31] K. Rubin, *Euler systems (Hermann Weyl Lectures)*, Annals of Mathematics Studies, vol. 147, Princeton University Press, 2000, xii+227 pages.

[32] J.-P. Serre & J. Tate, "Good reduction of abelian varieties", *Ann. Math.* **88** (1968), p. 492-517.

[33] J. Tilouine, "Modular forms and Galois representations", *Bull. Greek Math. Soc.* **46** (2002), p. 63-78.

[34] M. M. Višik, "Nonarchimedean measures associated with Dirichlet series", *Mat. Sb., N. Ser.* **99(141)** (1976), no. 2, p. 248-260, 296.

Manuscrit reçu le 1er juin 2018,
révisé le 1er juin 2020,
accepté le 15 novembre 2021.

Kazuto OTA
Department of Mathematics,
Graduate School of Science,
Osaka University Toyonaka,
Osaka 560-0043 (Japan)
kazutoota@math.sci.osaka-u.ac.jp