WACH MODULES AND IWASAWA THEORY FOR MODULAR FORMS

ANTONIO LEI, DAVID LOEFFLER, AND SARAH LIVIA ZERBES

Abstract. We define a family of Coleman maps for positive crystalline p-adic representations of the absolute Galois group of $\mathbb{Q}_p$ using the theory of Wach modules. Let $f = \sum a_n q^n$ be a normalized new eigenform and p an odd prime at which f is either good ordinary or supersingular. By applying our theory to the p-adic representation associated to f, we define Coleman maps $\underline{\mathrm{Col}}_i$ for $i = 1, 2$ with values in $\overline{\mathbb{Q}}_p \otimes_{\mathbb{Z}_p} \Lambda$, where Λ is the Iwasawa algebra of $\mathbb{Z}_p^\times$. Applying these maps to the Kato zeta elements gives a decomposition of the (generally unbounded) p-adic L-functions of f into linear combinations of two power series of bounded coefficients, generalizing works of Pollack (in the case $a_p = 0$) and Sprung (when f corresponds to a supersingular elliptic curve). Using ideas of Kobayashi for elliptic curves which are supersingular at p, we associate to each of these power series a Λ-cotorsion Selmer group. This allows us to formulate a "main conjecture". Under some technical conditions, we prove one inclusion of the "main conjecture" and show that the reverse inclusion is equivalent to Kato's main conjecture.

Contents

Date: 16th October 2010.
2000 *Mathematics Subject Classification.* 11R23,11F80,11S31,12H25.
The first author is supported by Trinity College Cambridge and an ARC DP1092496 grant.
The second author is supported by EPSRC Postdoctoral Fellowship EP/F04304X/1.
The third author is supported by EPSRC Postdoctoral Fellowship EP/F043007/1.

1. Introduction

1.1. **Background.** Let E be an elliptic curve defined over $\mathbb{Q}$ which has good ordinary reduction at the prime p. In [MSD74], Mazur and Swinnerton-Dyer constructed a p-adic L-function, $\tilde{L}_{p,E}$, which interpolates complex L-values of E. Let $\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^\infty})$. If G_∞ denotes the Galois group of $\mathbb{Q}_\infty$ over $\mathbb{Q}$, then $\tilde{L}_{p,E}$ is an element of $\Lambda_{\mathbb{Q}_p}(G_\infty) = \mathbb{Q} \otimes \mathbb{Z}_p[[G_\infty]]$. It is conjectured that $\tilde{L}_{p,E}$ is in fact an element of the Iwasawa algebra $\Lambda(G_\infty) = \mathbb{Z}_p[[G_\infty]]$.

Recall that the p-Selmer group of E over any finite extension F of $\mathbb{Q}$ is defined as

$$\mathrm{Sel}_p(E/F) = \ker\left(H^1(F, E_{p^\infty}) \longrightarrow \prod_v \frac{H^1(F_v, E_{p^\infty})}{E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right),$$

where the product is taken over all places of F. If we let $\mathrm{Sel}_p(E/\mathbb{Q}_\infty) = \varinjlim_n \mathrm{Sel}_p(E/\mathbb{Q}(\mu_{p^n}))$, then $\mathrm{Sel}_p(E/\mathbb{Q}_\infty)$ is equipped with an action of G_∞ which extends to an action of the Iwasawa algebra. It is not difficult to show that the Pontryagin dual $\mathrm{Sel}_p(E/\mathbb{Q}_\infty)^\vee$ is finitely generated over $\Lambda(G_\infty)$, and a theorem of Kato-Rohrlich (conjectured by Mazur) states that it is in fact $\Lambda(G_\infty)$-torsion. We can therefore associate to it a characteristic ideal for each Δ-isotypical component, where Δ is the torsion subgroup of G_∞, and the main conjecture of cyclotomic Iwasawa theory for E predicts that this ideal is generated by the corresponding isotypical component of $\tilde{L}_{p,E}$.

The construction of p-adic L-functions has been generalized to more general primes and modular forms in [AV75, Viš76]. If $f = \sum a_n q^n$ is a normalized new eigenform of weight $k \geq 2$, level N and character ϵ, $p \nmid N$, then there exists a p-adic L-function $\tilde{L}_{p,\alpha}$, for any root α of $X^2 - a_p X + \epsilon(p)p^{k-1}$ such that $v_p(\alpha) < k-1$, interpolating complex L-values of f. Perrin-Riou [PR95] and Kato [Kat93] have established theories of p-adic L-functions for a wide class of p-adic Galois representations and formulated respective Iwasawa main conjectures. When the representation corresponds to a modular form, these main conjectures have been reformulated by Kato [Kat04] using the theory of Euler systems. If f is good ordinary at p (in other words, $p \nmid N$ and a_p is a p-adic unit) and α is the unique unit root, then $\tilde{L}_{p,\alpha}$ is an element of $\Lambda_{\mathbb{Q}_p}(G_\infty)$. At a Δ-isotypical component, the main conjecture is equivalent to asserting that $\tilde{L}_{p,\alpha}$ generates the characteristic ideal of $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)^\vee$. In *op.cit.*, Kato has shown that $\tilde{L}_{p,\alpha}$ is contained in the characteristic ideal of $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)^\vee$ under some technical assumptions; his proof relies on the construction of certain zeta elements (which we will refer to as *Kato zeta elements*).

When f is supersingular at p (by which we mean $p \nmid N$ and a_p is not a p-adic unit), two problems arise: on the one hand, the p-adic L-functions of Amice–Vélu and Vishik are no longer elements of $\Lambda(G_\infty)$, but they lie in the algebra $\mathcal{H}(G_\infty)$ of distributions on G_∞, and on the other hand, $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)^\vee$ is no longer $\Lambda(G_\infty)$-torsion. Perrin-Riou's (and hence Kato's) main conjecture can therefore not be translated into a statement relating $\tilde{L}_{p,\alpha}$ and $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)$ as in the ordinary case. When $a_p = 0$, a remedy was made possible by the works of Pollack [Pol03]. If α_1 and α_2 are the roots of $X^2 + \epsilon(p)p^{k-1}$, Pollack showed that there is a decomposition

$$\tilde{L}_{p,\alpha_i} = \log^+_{p,k} \tilde{L}^+_p + \alpha_i \log^-_{p,k} \tilde{L}^-_p$$

for $i = 1, 2$, where $\tilde{L}^\pm_p \in \Lambda_{\mathbb{Q}_p}(G_\infty)$ and $\log^\pm_{p,k}$ are some explicit elements of $\mathcal{H}(G_\infty)$ which only depend on k. When f corresponds to an elliptic curve $E/\mathbb{Q}$ (and $p > 2$), the $\tilde{L}^\pm_p$ are in fact elements of $\Lambda(G_\infty)$. In [Kob03], Kobayashi formulates a main conjecture giving an arithmetic interpretation of these new p-adic

L-functions. In analogy to the ordinary reduction case, he defines even and odd Selmer groups $\mathrm{Sel}_p^{\pm}(E/\mathbb{Q}_\infty)$ by modifying the local conditions at p in the definition of the usual Selmer group. Let T_pE be the Tate module of E. Kobayashi shows that $\mathrm{Sel}_p^{\pm}(E/\mathbb{Q}_\infty)$ is $\Lambda(G_\infty)$-cotorsion by constructing the so-called plus and minus Coleman maps

$$\mathrm{Col}^{\pm} : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T_pE) \to \Lambda(G_\infty),$$

which depend on the structure of the formal group attached to E. (Here $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T_pE)$ is the Iwasawa cohomology, defined as $\varprojlim_n H^1(\mathbb{Q}_p(\mu_{p^n}), T_pE)$; see §2.3 below.) Kobayashi's modified main conjecture then asserts that in each Δ-isotypical component, the functions $\tilde{L}_p^{\pm}$ generate the respective characteristic ideals of $\mathrm{Sel}_p^{\pm}(E/\mathbb{Q}_\infty)^\vee$. This main conjecture is in fact equivalent to [Kat04, Conjecture 12.10] (to which we refer as *Kato's main conjecture* from now on). Using the fact that the maps $\mathrm{Col}^{\pm}$ send the localization of the Kato zeta elements to $\tilde{L}_p^{\pm}$, Kobayashi shows that the elements $\tilde{L}_p^{\pm}$ are contained in the characteristic ideals of $\mathrm{Sel}_p^{\pm}(E/\mathbb{Q}_\infty)^\vee$ (possibly after inverting p if p is one of the finitely many primes for which the p-adic Galois representation of E is not surjective), establishing half of the main conjecture. (When the elliptic curve has complex multiplication, the full conjecture has been proved by Pollack and Rubin [PoR04].)

Sprung [Spr09] has extended the results of Kobayashi to elliptic curves with supersingular reduction at p and $a_p \neq 0$ (which forces p to be 2 or 3). He constructs Coleman maps

$$\mathrm{Col}^{\vartheta}, \mathrm{Col}^{\upsilon} : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T_pE) \longrightarrow \Lambda(G_\infty)$$

and defines $\tilde{L}_p^{\vartheta}, \tilde{L}_p^{\upsilon} \in \Lambda(G_\infty)$ by applying these Coleman maps to the Kato zeta element. Analogously to the case $a_p = 0$ discussed above, he defines two Selmer groups $\mathrm{Sel}_p^{\vartheta}(E/\mathbb{Q}_\infty)$ and $\mathrm{Sel}_p^{\upsilon}(E/\mathbb{Q}_\infty)$ to formulate the corresponding main conjectures. Moreover, he constructs a matrix $M \in M_2(\mathcal{H}(G_\infty))$ whose entries are functions of logarithmic growth depending only on a_p such that

$$\begin{pmatrix} \tilde{L}_{p,\alpha} \\ \tilde{L}_{p,\beta} \end{pmatrix} = M \begin{pmatrix} \tilde{L}_p^{\vartheta} \\ \tilde{L}_p^{\upsilon} \end{pmatrix}$$

generalizing Pollack's results.

Generalizing Kobayashi's work in a different direction, the first author has shown in [Lei09] that the definition of the maps $\mathrm{Col}^{\pm}$ can be extended to general modular forms with $a_p = 0$, using p-adic Hodge theory in place of formal groups. For a normalized new eigenform f, there exists a p-adic representation V_f of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ attached to f, as constructed by Deligne [Del69]. When $a_p = 0$, one can then construct $\pm$-Coleman maps

$$\mathrm{Col}^{\pm} : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V_f) \to \Lambda_{\mathbb{Q}_p}(G_\infty),$$

using the structure of $\mathbb{D}_{\mathrm{cris}}(V_f)$ and Perrin-Riou's exponential map (see Section 2 in [Lei09]). Generalizing Kobayashi's construction, one can use $\mathrm{Col}^{\pm}$ to define $\pm$-Selmer groups, which again turn out to be $\Lambda(G_\infty)$-cotorsion and whose characteristic ideals at each Δ-isotypical component contain Pollack's p-adic L-functions. Analogous to the work of Pollack and Rubin for elliptic curves, one can show that equality holds for forms of CM type; see [Lei09] for details.

1.2. **Statement of the main results.** Looking at all these results raises some natural questions: Is there a uniform explanation for Sprung's logarithmic matrix M and Pollack's $\pm$-logarithms? Can one generalize the construction of the two Coleman series to more general modular forms which are supersingular at p?

In this paper, we approach these questions using methods from the theory of (φ, G_∞)-modules. As shown by Fontaine (unpublished – for a reference see [CC99]), for any $\mathbb{Z}_p$-linear representation T of $G_{\mathbb{Q}_p}$ there is a canonical isomorphism $h^1_{\mathbb{Q}_p,\mathrm{Iw}} : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T) \cong \mathbb{D}(T)^{\psi=1}$, where $\mathbb{D}(T)$ denotes the (φ, G_∞)-module[1] of T and ψ is a certain left inverse of φ. Recall that $\mathbb{D}(T)$ is a module over the p-adic completion $\mathbb{A}_{\mathbb{Q}_p}$ of the power series ring $\mathbb{Z}_p[[\pi]][\pi^{-1}]$. Also, $\Lambda(G_\infty)$ can be identified with the additive group $\mathbb{Z}_p[[\pi]]^{\psi=0}$ via the Mellin transform (c.f. Section 5.1). It seems therefore natural to expect that by carefully choosing a basis of $\mathbb{D}(T)$, it should be possible to define the two Coleman maps as certain maps on the coefficients of an element

[1] More familiarly known as a (φ, Γ)-module – our G_∞ is denoted by Γ in Fontaine's work, while we use Γ for its torsion-free part.

$x \in \mathbb{D}(T)^{\psi=1}$. Such a construction would generalize the classical case $T = \mathbb{Z}_p(1)$: in this case, the Coleman map $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, \mathbb{Z}_p(1)) \cong \mathbb{A}_{\mathbb{Q}_p}^{\psi=1} \to \mathbb{Z}_p[[\pi]][\pi^{-1}]^{\psi=0}$ is just the map $\varphi - 1$.

Here, we develop this idea using Berger's theory of Wach modules [Ber03], which is a refined version of (φ, G_∞)-modules for crystalline representations over unramified base fields originally studied by Wach in [Wac96]. The Wach module $\mathbb{N}(V)$ of a crystalline $G_{\mathbb{Q}_p}$-representation V is a certain subspace of the (φ, G_∞)-module $\mathbb{D}(V)$ which is a finitely-generated module over the simpler ring $\mathbb{B}^+_{\mathbb{Q}_p} = \mathbb{Z}_p[[\pi]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. If V is a crystalline representation of $G_{\mathbb{Q}_p}$ with non-negative Hodge-Tate weights, and V has no quotient isomorphic to $\mathbb{Q}_p$, then Berger has shown in [Ber03] that $\mathbb{D}(V)^{\psi=1} = \mathbb{N}(V)^{\psi=1}$. Let $\varphi^*\mathbb{N}(V)$ be the $\mathbb{B}^+_{\mathbb{Q}_p}$-submodule of $\mathbb{D}(V)$ generated by the image of φ. For any such representation, $1-\varphi$ gives a map

$$1 - \varphi : \mathbb{N}(V)^{\psi=1} \longrightarrow (\varphi^*\mathbb{N}(V))^{\psi=0}.$$

Our first main result relates this map to Perrin-Riou's theory. Suppose that V_f is the p-adic representation associated to a modular form f with p a good prime for f, i.e. p does not divide the level of f (we assume here for notational simplicity that the coefficient field of the modular form is $\mathbb{Q}$, so V is a 2-dimensional $\mathbb{Q}_p$-vector space). Let $V = V_f(k-1)$, then V is a crystalline representation with Hodge-Tate weights $0, k-1$. We fix $\bar{\nu}_1, \bar{\nu}_2$ a basis of $\mathbb{D}_{\mathrm{cris}}(V_f)$ in Section 3.3. It lifts to a basis n_1, n_2 of $\mathbb{N}(V_f)$. Note that $\pi^{1-k}n_1 \otimes e_{k-1}, \pi^{1-k}n_2 \otimes e_{k-1}$ then gives a basis of $\mathbb{N}(V)$. Let $M = (m_{ij}) \in M_2\big(\varphi(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})\big)$ be such that

$$\begin{pmatrix} \varphi(\pi^{1-k}n_1 \otimes e_{k-1}) \\ \varphi(\pi^{1-k}n_2 \otimes e_{k-1}) \end{pmatrix} = M \begin{pmatrix} \bar{\nu}_1 \otimes t^{1-k}e_{k-1} \\ \bar{\nu}_2 \otimes t^{1-k}e_{k-1} \end{pmatrix}.$$

Proposition 1.1 (see Proposition 3.22)**.** *For $i = 1, 2$ we have a commutative diagram*

$$\begin{tikzcd}
\mathbb{N}(V)^{\psi=1} \arrow[r, "h^1_{\mathbb{Q}_p,\mathrm{Iw}}"] \arrow[d, "1-\varphi"] & H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \arrow[ddd, "\mathcal{L}_{1,\bar{\nu}_i\otimes(1+\pi)}"] \\
(\varphi^*\mathbb{N}(V))^{\psi=0} \arrow[d, "M"] & \\
\big((\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}\big)^{\oplus 2} \arrow[d, "\mathrm{pr}_i"] & \\
(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0} \arrow[r, "\mathfrak{M}^{-1}"] & \mathcal{H}(G_\infty)
\end{tikzcd}$$

Here, $\mathcal{L}_{1,\bar{\nu}_i\otimes(1+\pi)}$ is a certain $\Lambda_{\mathbb{Q}_p}$-module homomorphism whose definition is given in equation (18) below, defined using Perrin-Riou's exponential map and the Perrin-Riou pairing $H^1_{\mathrm{Iw}}(V) \times H^1_{\mathrm{Iw}}(V^*(1)) \to \Lambda_{\mathbb{Q}_p}$. Also, $\mathfrak{M}$ is the inverse Mellin transform (see (13)), pr_i is the projection map onto the i-th component, and for an element $x \in (\varphi^*\mathbb{N}(V))^{\psi=0}$, $M.x$ is defined as follows: if $x = x_1\varphi(\pi^{1-k}n_1 \otimes e_{k-1}) + x_2\varphi(\pi^{1-k}n_2 \otimes e_{k-1})$ for some $x_i \in (\mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$, then $M.x = M\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

By applying this diagram to Kato's zeta element $\mathbf{z}^{\mathrm{Kato}} \in H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V)$, we deduce that there exist $\mathcal{M} \in M_2\big(\overline{\mathbb{Q}}_p \otimes_{\mathbb{Q}_p} \varphi(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})\big)$ and $L_{p,1}, L_{p,2} \in (\mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$ (c.f. Section 3.5.1), depending only on the basis n_1, n_2, such that we have a decomposition

$$\begin{pmatrix} \mathfrak{M}(\tilde{L}_{p,\alpha}) \\ \mathfrak{M}(\tilde{L}_{p,\beta}) \end{pmatrix} = \mathcal{M} \begin{pmatrix} L_{p,1} \\ L_{p,2} \end{pmatrix}. \tag{1}$$

In order to interpret this decomposition in terms of measures, we need to study the structure of $(\varphi^*\mathbb{N}(V))^{\psi=0}$ as a $\Lambda(G_\infty)$-module. The following result was proven independently by Berger (Theorem 3.5, for general Wach modules) and ourselves (Theorem 4.24, for the Wach module of the representation arising from a supersingular modular form).

Theorem 1.2. *Let $\mathcal{N}$ be a Wach module of rank d. Then $(\varphi^*\mathcal{N})^{\psi=0}$ is a free $\Lambda_{\mathbb{Q}_p}(G_\infty)$-module of rank d. Moreover, there exists a basis $n_1,\dots,n_d$ of $\mathcal{N}$ such that $(1+\pi)\varphi(n_1),\dots,(1+\pi)\varphi(n_d)$ is a $\Lambda_{\mathbb{Q}_p}(G_\infty)$-basis of $(\varphi^*\mathbb{N}(V))^{\psi=0}$.*

When V is the p-adic representation associated to a modular form with $v_p(a_p) > \lfloor\frac{k-2}{p-1}\rfloor$, then there is an explicit choice of the $\mathbb{B}^+_{\mathbb{Q}_p}$-basis of $\mathbb{N}(V)$ which was constructed in [BLZ04] (c.f. Section 4). We show (Theorem 4.24) that this basis (n_1,n_2) has the additional property that $(1+\pi)\varphi(n_1),(1+\pi)\varphi(n_2)$ is a $\Lambda_{\mathbb{Q}_p}(G_\infty)$-basis of $(\varphi^*\mathbb{N}(V))^{\psi=0}$. Hence we may define the *Iwasawa transform*

$$\mathfrak{J} : (\varphi^*\mathbb{N}(V))^{\psi=0} \longrightarrow \Lambda_{\mathbb{Q}_p}(G_\infty)^{\oplus 2}$$

to be the induced isomorphism of $\Lambda_{\mathbb{Q}_p}(G_\infty)$-modules associated to this basis. This map has the following property: if $a_p = 0$, then $\mathfrak{J}$ fits into the commutative diagram

$$\begin{tikzcd}
\mathbb{N}(V)^{\psi=1} \arrow[r, "h^1_{\mathbb{Q}_p,\mathrm{Iw}}"] \arrow[d, "1-\varphi"'] & H^1_{\mathrm{Iw}}(\mathbb{Q}_p,V) \arrow[d, "(\mathrm{Col}^{\pm})"] \\
(\varphi^*\mathbb{N}(V))^{\psi=0} \arrow[r, "\mathfrak{J}"] & \Lambda_{\mathbb{Q}_p}(G_\infty)^{\oplus 2}
\end{tikzcd}$$

where $\mathrm{Col}^{\pm}$ are the Coleman maps constructed in [Kob03] and [Lei09]. In other words, if $i=1,2$ and we define $\underline{\mathrm{Col}}_i : \mathbb{N}(V)^{\psi=1} \to \Lambda_{\mathbb{Q}_p}(G_\infty)$ to be the composition of $\mathfrak{J}\circ(1-\varphi)$ with the projection of $\Lambda_{\mathbb{Q}_p}(G_\infty)^{\oplus 2}$ onto the i-th component, then we recover the constructions in *op.cit.* In Sections 5.2 and 5.3, we use this new description of the Coleman maps to give alternative proofs of their main properties.

When $v_p(a_p) > \lfloor\frac{k-2}{p-1}\rfloor$, we define the maps $\underline{\mathrm{Col}}_i$ in the same manner, and it it follows from Proposition 3.24 that the following diagram is commutative:

$$\begin{tikzcd}
\mathbb{N}(V)^{\psi=1} \arrow[r, "h^1_{\mathbb{Q}_p,\mathrm{Iw}}"] \arrow[d, "1-\varphi"'] & H^1_{\mathrm{Iw}}(\mathbb{Q}_p,V) \arrow[d, "(\underline{\mathrm{Col}}_1,\underline{\mathrm{Col}}_2)"'] \arrow[ddd, bend left=60, "\mathcal{L}_{1,\bar{\nu}_i\otimes(1+\pi)}"] \\
(\varphi^*\mathbb{N}(V))^{\psi=0} \arrow[r, "\mathfrak{J}"] \arrow[d, "M"'] & \Lambda_{\mathbb{Q}_p}(G_\infty)^{\oplus 2} \arrow[d, "\underline{M}"'] \\
\left((\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}\right)^{\oplus 2} \arrow[r, "\mathfrak{M}^{-1}"] \arrow[d, "\mathrm{pr}_i"'] & \mathcal{H}(G_\infty)^{\oplus 2} \arrow[d, "\underline{\mathrm{pr}}_i"'] \\
(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0} \arrow[r, "\mathfrak{M}^{-1}"] & \mathcal{H}(G_\infty).
\end{tikzcd}$$

Here, the map $\underline{\mathrm{pr}}_i$ is the projection onto the i-th component in $\mathcal{H}(G_\infty)^{\oplus 2}$. In particular, this diagram allows us to translate (1) in terms of $\Lambda_{\mathbb{Q}_p}(G_\infty)$:

Theorem 1.3 (see Theorem 3.25)**.** *For $i=1,2$, define $\tilde{L}_{p,i} = \underline{\mathrm{Col}}_i(\mathbf{z}^{\mathrm{Kato}})$. There exists a 2×2-matrix $\underline{\mathcal{M}} \in M_2(\overline{\mathbb{Q}}_p \otimes_{\mathbb{Q}_p} \mathcal{H}(G_\infty))$ depending only on k and a_p such that*

$$\begin{pmatrix}\tilde{L}_{p,\alpha}\\ \tilde{L}_{p,\beta}\end{pmatrix} = \underline{\mathcal{M}}\begin{pmatrix}\tilde{L}_{p,1}\\ \tilde{L}_{p,2}\end{pmatrix} \tag{2}$$

We show in Proposition 5.10 that this decomposition reduces to the decompositions of $\tilde{L}_{p,\alpha}, \tilde{L}_{p,\beta}$ given by Pollack when $a_p = 0$.

Assume now that V_f is the p-adic representation associated to a modular form f which is good ordinary at p, and let $V = V_f(k-1)$. By choosing a suitable basis for $\mathbb{D}_{\mathrm{cris}}(V_f)$ (c.f Section 3.6) and applying Theorem 3.5 to $(\varphi^*\mathbb{N}(V))^{\psi=0}$, we can prodeed analogously to the supersingular case discussed above to construct Coleman maps $\underline{\mathrm{Col}}_i : \mathbb{N}(V)^{\psi=1} \to \Lambda_{\mathbb{Q}_p}(G_\infty)$. Let α and β be the unit and non-unit eigenvalues of the Frobenius respectively. The Kato zeta element gives rise to two p-adic L-functions $\tilde{L}_{p,\alpha}$ and $\tilde{L}_{p,\beta}$, where $\tilde{L}_{p,\beta}$ conjecturally agrees with the critical-slope p-adic L-function constructed by Pollack and Stevens in [PoS09] when V_f is not locally split at p. The analogue of (2) becomes

$$\begin{pmatrix} \tilde{L}_{p,\alpha} \\ \tilde{L}_{p,\beta} \end{pmatrix} = \begin{pmatrix} 0 & \bar{u} \\ -\alpha \log_{p,k} & * \end{pmatrix} \begin{pmatrix} \tilde{L}_{p,1} \\ \tilde{L}_{p,2} \end{pmatrix}. \tag{3}$$

for some $\bar{u} \in \Lambda_E(G_\infty)^\times$ (c.f. (37)). Note that a similar decomposition can be obtained from works of Perrin-Riou for elliptic curves with good ordinary reduction at p (see [PR93, Section 1.4]). The decomposition (3) allows us to show that $\tilde{L}_{p,1}, \tilde{L}_{p,2} \neq 0$ under some technical assumptions.

As in the cases studied in [Kob03] and [Lei09], we can use the maps $\underline{\mathrm{Col}}_i$ to construct Selmer groups $\mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)$ (see Definition 6.4), and we prove the following results. Define assumptions

(A) (when f is supersingular at p) $k \geq 3$ or $a_p = 0$;

(A') (when f is good ordinary at p) $k \geq 3$ and V_f is not locally split at p.

Theorem 1.4 (see Theorem 6.5)**.** *Under assumption (A) (if f is supersingular at p) or assumption (A') (if f is good ordinary at p), the group $\mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)$ is $\Lambda_{\mathcal{O}_E}(G_\infty)$-cotorsion for $i = 1, 2$. Moreover, there exist some $n_i \geq 0$ such that*

$$\varpi^{n_i} \tilde{L}_{p,i}^\eta \in \mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)^{\vee,\eta})$$

where η is any character on Δ when $i = 1$ and it is the trivial character when $i = 2$.

Corollary 1.5 (see Corollary 6.6)**.** *Let η be a character on Δ as in Theorem 1.4. If either assumption (A) or assumption (A') is satisfied, and the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_\infty)$ in $\mathrm{GL}(V_f)$ contains a conjugate of $\mathrm{SL}_2(\mathbb{Z}_p)$, then Kato's main conjecture is equivalent to*

$$\mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)^{\vee,\eta}) = \mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathrm{Im}(\underline{\mathrm{Col}}_i)^\eta/(\tilde{L}_{p,i}^\eta)).$$

Note that in the ordinary case, $\tilde{L}_{p,2}$ agrees with the usual p-adic L-function of f up to a unit in $\Lambda_E(G_\infty)$. It will be shown in a forthcoming paper of the first and third authors [LZ10] that the corresponding Selmer group is the usual $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)$; whereas the first Coleman map gives a new p-adic L-function $\tilde{L}_{p,1}$ and a new Selmer group.

1.3. **Notation.** Throughout this paper, let p be an odd prime. Fix embeddings of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$, and into $\mathbb{C}$. For $n \geq 0$, write $\mathbb{Q}_{p,n} = \mathbb{Q}_p(\mu_{p^n})$ (resp. $\mathbb{Q}_n = \mathbb{Q}(\mu_{p^n})$) for the extension of $\mathbb{Q}_p$ (resp. $\mathbb{Q}$) obtained by adjoining the p^n-th roots of unity. Let G_n denote its Galois group. Let $\mathbb{Q}_{p,\infty} = \bigcup \mathbb{Q}_{p,n}$, and write G_∞ for the Galois group of $\mathbb{Q}_{p,\infty}$ over $\mathbb{Q}_p$. We identify G_∞ with the Galois group of $\mathbb{Q}_\infty = \bigcup_{n\geq 1} \mathbb{Q}_n$ over $\mathbb{Q}$. Then $G_\infty \cong \Delta \times \Gamma$ where Δ is a finite group of order $p-1$ and $\Gamma \cong \mathbb{Z}_p$, the Galois group of $\mathbb{Q}_{p,\infty}$ over $\mathbb{Q}_p(\mu_p)$. We fix a topological generator γ of Γ and write χ for the cyclotomic character of G_∞. Let $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and $H_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p,\infty})$, where $\overline{\mathbb{Q}}_p$ denotes an algebraic closure of $\mathbb{Q}_p$.

Given a finite extension K of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$, $\Lambda_{\mathcal{O}_K}(G_\infty)$ (respectively $\Lambda_{\mathcal{O}_K}(\Gamma)$) denotes the Iwasawa algebra of G_∞ (respectively Γ) over $\mathcal{O}_K$. We further write $\Lambda_K(G_\infty) = \Lambda_{\mathcal{O}_K}(G_\infty) \otimes \mathbb{Q}$ and $\Lambda_K(\Gamma) = \Lambda_{\mathcal{O}_K}(\Gamma) \otimes \mathbb{Q}$.

Given a module M over $\Lambda_{\mathcal{O}_K}(G_\infty)$ (respectively $\Lambda_K(G_\infty)$) and a character $\eta : \Delta \to \mathbb{Z}_p^\times$, M^η denotes the η-isotypical component of M. For any $m \in M$, we write m^η for the projection of m into M^η.

2. Representations of $G_{\mathbb{Q}_p}$

In this section we review some aspects of the theory of p-adic representations of $G_{\mathbb{Q}_p}$. Most of our account is reproduced from [Ber04] and [BLZ04, §2]. Let E be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_E$. An E-linear representation of $G_{\mathbb{Q}_p}$ is a finite dimensional E-vector space V with a continuous E-linear action of $G_{\mathbb{Q}_p}$. We similarly have the notion of an $\mathcal{O}_E$-linear representation of $G_{\mathbb{Q}_p}$, which is a finitely-generated (not necessarily free) $\mathcal{O}_E$-module with a continuous $\mathcal{O}_E$-linear action of $G_{\mathbb{Q}_p}$. Define $\mathrm{Rep}_E(G_{\mathbb{Q}_p})$ (respectively $\mathrm{Rep}_{\mathcal{O}_E}(G_{\mathbb{Q}_p})$) to be the categoy of E-linear (respectively $\mathcal{O}_E$-linear) representations of $G_{\mathbb{Q}_p}$.

2.1. **p-adic Hodge theory.** In this section, we recall the definitions of some of Fountain's rings of periods. Let $\mathbb{C}_p$ be the completion of $\overline{\mathbb{Q}}_p$ for the p-adic topology, endowed with the usual valuation v_p normalized such that $v_p(p) = 1$. Let

$$\tilde{\mathbb{E}} = \varprojlim_{x\mapsto x^p} \mathbb{C}_p = \big\{(x^{(0)}, x^{(1)}, \dots) : (x^{(i+1)})^p = x^{(i)}\big\},$$

and let $\tilde{\mathbb{E}}^+$ be the set of $x \in \tilde{\mathbb{E}}$ such that $x^{(0)} \in \mathcal{O}_{\mathbb{C}_p}$. We can equip $\tilde{\mathbb{E}}$ naturally with the structure of an algebraically closed field of characteristic p: if $x = (x^{(i)})$ and $y = (y^{(i)})$, define $x + y$ and xy by

$$\begin{aligned}(x + y)^{(i)} &:= \lim_{j\to+\infty} \big(x^{(i+j)} + y^{(i+j)}\big)^{p^j}\\ (xy)^{(i)} &:= x^{(i)}y^{(i)}.\end{aligned}$$

Define a complete valuation on $\tilde{\mathbb{E}}$ by $v_{\tilde{\mathbb{E}}}(x) = v_p(x^{(0)})$ if $x = (x^{(i)}) \in \tilde{\mathbb{E}}$. Let $\tilde{\mathbb{A}}^+ = W(\tilde{\mathbb{E}}^+)$ be the ring of Witt vectors of $\tilde{\mathbb{E}}^+$, and let $\tilde{\mathbb{B}}^+ = \tilde{\mathbb{A}}^+[p^{-1}]$. An element $x \in \tilde{\mathbb{B}}^+$ can then be written uniquely in the form

$$x = \sum_{i\gg-\infty} p^i[x_i],$$

where $x_i \in \tilde{\mathbb{E}}^+$ and $[x_i]$ denotes the Teichmüller lift. The ring $\tilde{\mathbb{B}}^+$ is equipped with the Witt vector Frobenius map φ (lifting the map $x \mapsto x^p$ on $\tilde{\mathbb{E}}^+$), and with a map

$$\theta : \tilde{\mathbb{B}}^+ \longrightarrow \mathbb{C}_p$$

via $\theta\left(\sum_{i\gg-\infty} p^i[x_i]\right) = \sum_{i\gg\infty} p^i x_i^{(0)}$. Fix an element $\varepsilon = (\varepsilon^{(n)}) \in \tilde{\mathbb{E}}^+$ with $\varepsilon^{(0)} = 1$ and $\varepsilon^{(1)} \neq 1$. Let $\pi = [\varepsilon] - 1$, $\pi_1 = [\varphi^{-1}(\varepsilon)] - 1$ and $\omega = \frac{\pi}{\pi_1}$.

The ring $\mathbb{B}^+_{\mathrm{dR}}$ is defined as $\mathbb{B}^+_{\mathrm{dR}} = \varprojlim \tilde{\mathbb{B}}^+/\ker(\theta)^n$. It is a discrete valuation ring, and its maximal ideal is generated by $t = \log([\varepsilon])$. Define $\mathbb{B}_{\mathrm{dR}} = \mathbb{B}^+_{\mathrm{dR}}[t^{-1}]$ to be the fraction field of $\mathbb{B}^+_{\mathrm{dR}}$, which is equipped with an action of $G_{\mathbb{Q}_p}$ and a filtration defined by $\mathrm{Fil}^i\,\mathbb{B}_{\mathrm{dR}} = t^i\mathbb{B}^+_{\mathrm{dR}}$.

Define the ring $\mathbb{B}^+_{\mathrm{cris}}$ as

$$\mathbb{B}^+_{\mathrm{cris}} = \Big\{\sum_{n\geq 0} a_n \frac{\omega^n}{n!} \quad \text{where } a_n \in \tilde{\mathbb{B}}^+ \text{ is a sequence converging to } 0\Big\},$$

and $\mathbb{B}_{\mathrm{cris}} = \mathbb{B}^+_{\mathrm{cris}}[t^{-1}]$. The ring $\mathbb{B}_{\mathrm{cris}}$ injects canonically into $\mathbb{B}_{\mathrm{dR}}$, and it is endowed with the induced Galois action and filtration, as well with a continuous Frobenius φ which extends the map $\varphi : \tilde{\mathbb{B}}^+ \to \tilde{\mathbb{B}}^+$. If V is a $\mathbb{Q}_p$-linear representation of $G_{\mathbb{Q}_p}$, then $\mathbb{D}_{\mathrm{cris}}(V) = (V \otimes \mathbb{B}_{\mathrm{cris}})^{G_{\mathbb{Q}_p}}$ is a filtered φ-module of dimension $\leq \dim_{\mathbb{Q}_p}(V)$. We define V to be crystalline if equality holds.

If V is a $\mathbb{Q}_p$-linear representation of $G_{\mathbb{Q}_p}$, say that V is Hodge-Tate, with Hodge-Tate weights $h_1, \dots, h_d$, if we have a decomposition $\mathbb{C}_p \otimes_{\mathbb{Q}_p} V \cong \oplus_{i=1}^d \mathbb{C}_p(h_i)$. Say that V is positive if its Hodge-Tate weights are negative. It is easy to see that a crystalline representation V is Hodge-Tate, and that its Hodge-Tate weights are those integers h such that $\mathrm{Fil}^{-h}\,\mathbb{D}_{\mathrm{cris}}(V) \neq \mathrm{Fil}^{1-h}\,\mathbb{D}_{\mathrm{cris}}(V)$.

If V is an E-linear representation of $G_{\mathbb{Q}_p}$, then we define its Hodge-Tate weights to be the weights of the underlying $\mathbb{Q}_p$-vector space, and we say that V is crystalline if and only if the underlying $\mathbb{Q}_p$-linear representation is crystalline. In this case, $\mathbb{D}_{\mathrm{cris}}(V)$ is an E-vector space, and the filtration and Frobenius are E-linear.

2.2. **Crystalline representations and Wach modules.** Let $\tilde{\mathbb{A}} = W(\tilde{\mathbb{E}})$, and let $\mathbb{A}_{\mathbb{Q}_p}$ be the completion of $\mathbb{Z}_p[[\pi]][\pi^{-1}]$ in $\tilde{\mathbb{A}}$ in the p-adic topology, so $\mathbb{A}_{\mathbb{Q}_p}$ is a complete discrete valuation ring with residue field $\mathbb{F}_p((\varepsilon-1))$. Let $\mathbb{B}$ be the completion of the maximal unramified extension of $\mathbb{B}_{\mathbb{Q}_p} = \mathbb{A}_{\mathbb{Q}_p}[p^{-1}]$ in $\tilde{\mathbb{B}}$, and define $\mathbb{A} = \mathbb{B} \cap \tilde{\mathbb{A}}$ and $\mathbb{B}^+ = \mathbb{B} \cap \tilde{\mathbb{B}}^+$. These rings are endowed with an action of $G_{\mathbb{Q}_p}$ and of the Frobenius operator φ. One can show that $(\mathbb{B}^+)^{H_{\mathbb{Q}_p}} = \mathbb{Z}_p[[\pi]][p^{-1}]$, which we denote by $\mathbb{B}^+_{\mathbb{Q}_p}$.

We define a left inverse $\psi : \mathbb{B} \to \mathbb{B}$ by $x \to \varphi^{-1}\left(p^{-1}\operatorname{Tr}_{\mathbb{B}/\varphi(\mathbb{B})}(x)\right)$. If $x = f(\pi) \in \mathbb{B}_{\mathbb{Q}_p}$, then the value of $\psi(x)$ can also be calculated by

$$\varphi \circ \psi(x) = \frac{1}{p}\sum_{\zeta^p=1} f(\zeta(\pi+1)-1).$$

Since the residual extension $\tilde{\mathbb{E}}/\varphi(\tilde{\mathbb{E}})$ is inseparable of degree p, ψ preserves $\mathbb{A}$ and $\mathbb{A}_{\mathbb{Q}_p}$.

An étale (φ, G_∞)-module over $\mathbb{A}_{\mathbb{Q}_p}$ is a finitely generated $\mathbb{A}_{\mathbb{Q}_p}$-module M, with semi-linear φ and a continuous action of G_∞ commuting with each other, such that $\varphi(M)$ generates M as an $\mathbb{A}_{\mathbb{Q}_p}$-module. In [Fon90], Fontaine constructs a functor $T \to \mathbb{D}(T)$ which associates to every $\mathbb{Z}_p$-linear representation of $G_{\mathbb{Q}_p}$ an étale (φ, G_∞)-module over $\mathbb{A}_{\mathbb{Q}_p}$. Moreover, he shows that this functor is an equivalence of categories. By inverting p, one also gets an equivalence of categories between the category of $\mathbb{Q}_p$-linear p-adic representations and the category of étale (φ, G_∞)-modules over $\mathbb{B}_{\mathbb{Q}_p}$. The left inverse ψ of φ extends to the (φ, G_∞)-module.

If E is a finite extension of $\mathbb{Q}_p$, we extend the Frobenius and the action of G_∞ to $E \otimes \mathbb{B}_{\mathbb{Q}_p}$ by E-linearity. We then get an equivalence of categories from the category of E-linear (or $\mathcal{O}_E$-linear) representations to the category of étale (φ, G_∞)-modules over $E \otimes \mathbb{B}_{\mathbb{Q}_p}$ (resp. over $E \otimes \mathbb{A}_{\mathbb{Q}_p}$).

If V is a crystalline representation, we can say more about the (φ, G_∞)-module. Let $\mathbb{A}^+_{\mathbb{Q}_p} = \mathbb{Z}_p[[\pi]]$ and $\mathbb{B}^+_{\mathbb{Q}_p} = \mathbb{A}^+_{\mathbb{Q}_p}[p^{-1}]$ as above. The following result is shown in [Ber03, §II.1 and §III.4] and [BLZ04, §2]: If V is an E-linear representation, then V is crystalline with Hodge-Tate weights in $[a, b]$ if and only if there exists a (necessarily unique) $E \otimes_{\mathbb{Q}_p} \mathbb{B}^+_{\mathbb{Q}_p}$-module $\mathbb{N}(V)$ contained in $\mathbb{D}(V)$ such that the following conditions are satisfied:

(1) $\mathbb{N}(V)$ is free of rank $d = \dim_E(V)$ over $E \otimes_{\mathbb{Q}_p} \mathbb{B}^+_{\mathbb{Q}_p}$;
(2) the action of G_∞ preserves $\mathbb{N}(V)$ and is trivial on $\mathbb{N}(V)/\pi\mathbb{N}(V)$;
(3) $\varphi(\pi^b\mathbb{N}(V)) \subset \pi^b\mathbb{N}(V)$ and $\pi^b\mathbb{N}(V)/\varphi^*(\pi^b\mathbb{N}(V))$ is killed by q^{b-a} where $q = \frac{\varphi(\pi)}{\pi}$. (If M is a R-module equipped with a Frobenius φ where R is any ring, then $\varphi^*(M)$ denotes the R-module generated by $\varphi(M)$.)

If V is crystalline and positive, then we can take $b = 0$ above, so φ preserves $\mathbb{N}(V)$. In this case, if we endow $\mathbb{N}(V)$ with the filtration $\operatorname{Fil}^i \mathbb{N}(V) = \{x \in \mathbb{N}(V) \mid \varphi(x) \in q^i\mathbb{N}(V)\}$, then $\mathbb{N}(V)/\pi\mathbb{N}(V)$ is a filtered E-linear φ-module, and as shown in [Ber03, §III.4] we have an isomorphism $\mathbb{N}(V)/\pi\mathbb{N}(V) \cong \mathbb{D}_{\mathrm{cris}}(V)$.

If T is a $G_{\mathbb{Q}_p}$-stable lattice in V, then $\mathbb{N}(T) = \mathbb{N}(V) \cap \mathbb{D}(T)$ is an $\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p}$-lattice in $\mathbb{N}(V)$, and by [Ber03, §III.4] the functor $T \to \mathbb{N}(T)$ gives a bijection between the $G_{\mathbb{Q}_p}$-stable lattices T in V and the $\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p}$-lattices in $\mathbb{N}(V)$ satisfying

(1) $\mathbb{N}(T)$ is free of rank $d = \dim_E(V)$ over $\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p}$;
(2) the action of G_∞ preserves $\mathbb{N}(T)$;
(3) $\varphi(\pi^b\mathbb{N}(T)) \subset \pi^b\mathbb{N}(T)$ and $\pi^b\mathbb{N}(T)/\varphi^*(\pi^b\mathbb{N}(T))$ is killed by q^{b-a} where $q = \frac{\varphi(\pi)}{\pi}$.

Let $\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$ be the set of $f(\pi) \in \mathbb{Q}_p[[\pi]]$ such that $f(X)$ converges for all X in the open unit disc in $\mathbb{C}_p$. Note that $t \in \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$. If V is a positive representation of $G_{\mathbb{Q}_p}$, then as shown in [Ber03, §I.5], we can recover $\mathbb{D}_{\mathrm{cris}}(V)$ from $\mathbb{N}(V)$ as $\mathbb{D}_{\mathrm{cris}}(V) = \left(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p} \otimes_{\mathbb{B}^+_{\mathbb{Q}_p}} \mathbb{N}(V)\right)^{G_\infty}$. Moreover, the inclusion $\mathbb{D}_{\mathrm{cris}}(V) \subset \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p} \otimes_{\mathbb{B}^+_{\mathbb{Q}_p}} \mathbb{N}(V)$ gives rise to an isomorphism

$$\iota : \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}[t^{-1}] \otimes_{\mathbb{Q}_p} \mathbb{D}_{\mathrm{cris}}(V) \cong \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}[t^{-1}] \otimes_{\mathbb{B}^+_{\mathbb{Q}_p}} \mathbb{N}(V).$$

In [Ber02, proposition 2.12], Berger shows that for all $n \geq 0$ there is an injective map $\varphi^{-n}(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}) \to \mathbb{B}^+_{\mathrm{dR}}$, which is compatible with the natural map $\varphi^{-n}(\tilde{\mathbb{B}}^+) \to \mathbb{B}^+_{\mathrm{dR}}$. It is characterized by the fact that it sends

π to $\varepsilon^{(n)}\exp(t/p^n)-1$. Define a derivation $\partial:\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}\to\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$ by $\partial=(1+\pi)\frac{d}{d\pi}$. Under the map $\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}\to\mathbb{Q}_p[[t]]$ given by $\pi\mapsto\exp(t)-1$, ∂ corresponds to the derivation $\frac{d}{dt}$.

If $z\in\mathbb{Q}_{p,n}((t))\otimes_{\mathbb{Q}_p}\mathbb{D}_{\mathrm{cris}}(V)$, denote the constant coefficient of z by $\partial_V(z)\in\mathbb{Q}_{p,n}\otimes_{\mathbb{Q}_p}\mathbb{D}_{\mathrm{cris}}(V)$.

2.3. **Iwasawa cohomology and the Fontaine isomorphism.** If $T\in\mathrm{Rep}_{\mathcal{O}_E}(G_{\mathbb{Q}_p})$, define

$$H^1_{\mathrm{Iw}}(\mathbb{Q}_p,T)=\varprojlim_n H^1(\mathbb{Q}_{p,n},T),$$

where the inverse limit is taken with respect to the corestriction maps. As shown by Fontaine (unpublished – for a reference see [CC99, Section II]), for any $T\in\mathrm{Rep}_{\mathcal{O}_E}(G_{\mathbb{Q}_p})$, there is a canonical isomorphism of $\Lambda_{\mathcal{O}_E}(G_\infty)$-modules

$$h^1_{\mathbb{Q}_p,\mathrm{Iw}}:\mathbb{D}(T)^{\psi=1}\xrightarrow{\cong}H^1_{\mathrm{Iw}}(\mathbb{Q}_p,T). \tag{4}$$

Similarly, for $V\in\mathrm{Rep}_E(G_{\mathbb{Q}_p})$, define $H^1_{\mathrm{Iw}}(\mathbb{Q}_p,V)=H^1_{\mathrm{Iw}}(\mathbb{Q}_p,T)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$, where T is any $G_{\mathbb{Q}_p}$-invariant lattice of V; this is independent of the choice of T, and $h^1_{\mathbb{Q}_p,\mathrm{Iw}}$ extends to an isomorphism of $\Lambda_E(G_\infty)$-modules $\mathbb{D}(V)^{\psi=1}\cong H^1_{\mathrm{Iw}}(\mathbb{Q}_p,V)$.

3. The Coleman maps

3.1. **Positive crystalline representations.** In this subsection, we shall define d Coleman maps for a d-dimensional positive crystalline representation V, depending on a choice of basis of the Wach module $\mathbb{N}(T)$ for a lattice T in V.

Let E be a finite extension of $\mathbb{Q}_p$. Let V be a positive crystalline d-dimensional E-linear representation of $G_{\mathbb{Q}_p}$ with Hodge-Tate weights $-r_d\le -r_{d-1}\le\cdots\le -r_1\le 0$. We assume that V has no quotient isomorphic to $E(-r_d)$ and fix an $\mathcal{O}_E$-lattice T in V which is stable under $G_{\mathbb{Q}_p}$. Write $\mathbb{N}(T)$ for its Wach module, which is a free $\mathcal{O}_E\otimes\mathbb{A}^+_{\mathbb{Q}_p}$-module of rank d, whereas $\mathbb{N}(V)=\mathbb{N}(T)\otimes\mathbb{Q}_p$ is a free $E\otimes\mathbb{B}^+_{\mathbb{Q}_p}$-module of rank d. Choose an $\mathcal{O}_E\otimes\mathbb{A}^+_{\mathbb{Q}_p}$-basis $n_1,\ldots,n_d$ of $\mathbb{N}(T)$ and write P for the matrix of φ with respect to this basis. Then

$$\begin{pmatrix}\varphi(n_1)\\ \vdots\\ \varphi(n_d)\end{pmatrix}=P^T\begin{pmatrix}n_1\\ \vdots\\ n_d\end{pmatrix}$$

where A^T denotes the transpose of A if A is a square matrix. Moreover, by [BB10, section 3], the determinant of P is $q^{r_1+\cdots+r_d}$ up to a unit, where $q=\frac{\varphi(\pi)}{\pi}$ as above.

Let $m=\sum_{i=1}^d r_i$. Then, for $x\in\mathbb{D}(T(m))^{\psi=1}$, we have $x\in\mathbb{N}(T(m))^{\psi=1}$ by [Ber03, appendix A]. But $\mathbb{N}(T(m))=\pi^{-m}\mathbb{N}(T)\otimes e_m$, where e_m is a vector space basis of $\mathbb{Z}_p(m)$. Hence, there exist unique $x_1,\ldots,x_d\in\mathcal{O}_E\otimes\mathbb{A}^+_{\mathbb{Q}_p}$ such that

$$x=\pi^{-m}\begin{pmatrix}x_1&\cdots&x_d\end{pmatrix}\begin{pmatrix}n_1\\ \vdots\\ n_d\end{pmatrix}\otimes e_m. \tag{5}$$

Lemma 3.1. *For any $x\in\mathbb{D}(T(m))^{\psi=1}$, the entries of the row vector*

$$\mathbf{Col}(x):=\begin{pmatrix}x_1&\cdots&x_d\end{pmatrix}q^m(P^T)^{-1}-\begin{pmatrix}\varphi(x_1)&\cdots&\varphi(x_d)\end{pmatrix}$$

are elements of $(\mathcal{O}_E\otimes\mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$.

Proof. Recall that the determinant of P is q^m up to a unit in $\mathcal{O}_E\otimes\mathbb{A}^+_{\mathbb{Q}_p}$, so the entries of $\mathbf{Col}(x)$ are indeed elements of $\mathcal{O}_E\otimes\mathbb{A}^+_{\mathbb{Q}_p}$. Since $\varphi(\pi)=\pi q$, (5) implies that

$$x=\begin{pmatrix}x_1&\cdots&x_d\end{pmatrix}q^m(P^T)^{-1}\varphi(\pi^{-m})\begin{pmatrix}\varphi(n_1)\\ \vdots\\ \varphi(n_d)\end{pmatrix}\otimes e_m.$$

Hence,

$$\psi(x) = \psi\left(\begin{pmatrix}x_1 & \cdots & x_d\end{pmatrix} q^m (P^T)^{-1}\right) \pi^{-m} \begin{pmatrix} n_1 \\ \vdots \\ n_d \end{pmatrix} \otimes e_m.$$

Therefore, $\psi(x) = x$ implies that

$$\psi\left(\begin{pmatrix}x_1 & \cdots & x_d\end{pmatrix} q^m (P^T)^{-1}\right) = \begin{pmatrix}x_1 & \cdots & x_d\end{pmatrix}.$$

Hence the result. □

Definition 3.2. *For $1 \le i \le d$, we define the i-th Coleman map $\mathrm{Col}_i : \mathbb{D}(T(m))^{\psi=1} \to (\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$ by sending x to the i-th component of $\mathbf{Col}(x)$.*

Lemma 3.3. *Let $n_1, \ldots, n_d$ and $n'_1, \ldots, n'_d$ be two bases of $\mathbb{N}(T)$ with $\begin{pmatrix} n_1 \\ \vdots \\ n_d \end{pmatrix} = M'' \begin{pmatrix} n'_1 \\ \vdots \\ n'_d \end{pmatrix}$. Then, the Coleman maps defined by these two bases, $\mathbf{Col}$ and $\mathbf{Col}'$ are related by $\mathbf{Col}(x)\varphi(M'') = \mathbf{Col}'(x)$ for all $x \in \mathbb{D}(T(m))^{\psi=1}$.*

Proof. For any $x \in \mathbb{D}(T(m))^{\psi=1}$, write $x = x_1 n_1 + \cdots x_d n_d = x'_1 n'_1 + \cdots x'_d n'_d$. Then,

$$\begin{pmatrix}x'_1 & \cdots & x'_d\end{pmatrix} = \begin{pmatrix}x_1 & \cdots & x_d\end{pmatrix} M''$$

Let P and P' be the matrices of φ with respect to $n_1, \ldots, n_d$ and $n'_1, \ldots, n'_d$ respectively. Then $P^T M'' = \varphi(M'') P'^T$. Therefore,

$$\begin{aligned}
\mathbf{Col}'(x) &= \begin{pmatrix}x'_1 & \cdots & x'_d\end{pmatrix} q^m (P'^T)^{-1} - \begin{pmatrix}\varphi(x'_1) & \cdots & \varphi(x'_d)\end{pmatrix} \\
&= \begin{pmatrix}x_1 & \cdots & x_d\end{pmatrix} q^m M'' (P'^T)^{-1} - \begin{pmatrix}\varphi(x_1) & \cdots & \varphi(x_d)\end{pmatrix} \varphi(M'') \\
&= \begin{pmatrix}x_1 & \cdots & x_d\end{pmatrix} q^m (P^T)^{-1} \varphi(M'') - \begin{pmatrix}\varphi(x_1) & \cdots & \varphi(x_d)\end{pmatrix} \varphi(M'').
\end{aligned}$$

Hence the lemma. □

It is clear that we can extend Col_i to a map from $\mathbb{D}(V(m))^{\psi=1}$ to $(E \otimes \mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$. By an abuse of notation, we will write this map as Col_i as well. We now relate $\mathbf{Col}(x)$ to $(1-\varphi)(x)$. By writing down $\varphi(x)$, we have the following:

$$(1-\varphi)(x) = \mathbf{Col}(x) \cdot \varphi(\pi)^{-m} P^T \begin{pmatrix} n_1 \\ \vdots \\ n_d \end{pmatrix} \otimes e_m \tag{6}$$

Remark 3.4. *We see from (6) that for any x as above, $(1-\varphi)x \in (\varphi^* \mathbb{N}(T(m)))^{\psi=0}$.*

Note that the maps Col_i are *not* $\Lambda(G_\infty)$-homomorphisms under the canonical action of G_∞ on $(\mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$ because G_∞ acts non-trivially on the basis $\{n_i\}_{1 \le i \le d}$ of $\mathbb{N}(V)$. We deal with this problem using Theorem 3.5 below. Its proof is due to Laurent Berger; we quote it with his permission. In the case when V is the p-adic representation associated to a modular form with $v_p(a_p) \ge \lfloor \frac{k-2}{p-1} \rfloor$, we have independently found a proof of this result which uses the basis of $\mathbb{N}(V)$ constructed in [BLZ04]. It is more explicit than Berger's proof, and we give it in Section 4 since it will be needed to analyse the images of the Coleman maps. For notational simplicity, we take $E = \mathbb{Q}_p$ for the time being. Conceptually, there is no difficulty in extending the result to an E-linear representation.

Theorem 3.5. *Let V be a crystalline p-adic representation of $G_{\mathbb{Q}_p}$ of dimension d, and let T be a $G_{\mathbb{Q}_p}$-stable lattice in V. Then $(\varphi^* \mathbb{N}(T))^{\psi=0}$ is a free $\Lambda(G_\infty)$-module of rank d. Moreover, if $n_1^0, \ldots, n_d^0$ is a basis of $\mathbb{N}(T)$, then there exists a basis $n_1, \ldots, n_d$ such that $n_i \equiv n_i^0 \mod \pi$ for all i and $(1+\pi)\varphi(n_1), \ldots, (1+\pi)\varphi(n_d)$ forms a $\Lambda(G_\infty)$-basis of $(\varphi^* \mathbb{N}(T))^{\psi=0}$.*

Note that in this theorem we do not assume that V is positive. The proof of this result requires several preliminary lemmas. We assume without loss of generality that $\chi(\gamma) = 1 + p$. For $k \geq 0$, define

$$p_k = (1-\gamma)(1-\chi(\gamma)^{-1}\gamma)\dots(1-\chi(\gamma)^{1-k}\gamma),$$

which is an element of $\Lambda(\Gamma)$.

Lemma 3.6. *If $a \in \mathbb{Z}_p$ and $x \in \mathbb{N}(T)$ and $f \in \mathbb{A}^+_{\mathbb{Q}_p}$ and $g \in G_\infty$, then*

$$(1-ag)(fx) = ((1-ag)f)x + ag(f)((1-g)x).$$

Proof. Immediate. ☐

Lemma 3.7. *The map $\mathfrak{M} : \Lambda(G_\infty) \to (\mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$ given by $f \to f(1+\pi)$ is an isomorphism of $\Lambda(G_\infty)$-modules, which takes $p_k\Lambda(G_\infty)$ to $\varphi(\pi)^k(\mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$.*

Proof. The first assertion is standard (we recall the relevant theory in section 5.1 below). Note that $\gamma(\pi) = \chi(\gamma)\pi + O(\pi^2)$, which implies that the image of $p_k\Lambda(G_\infty)$ is contained in $\varphi(\pi)^k(\mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$. Hence the surjection $\Lambda(G_\infty) \twoheadrightarrow (\mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$ gives a surjection $\Lambda(G_\infty)/p_k \twoheadrightarrow (\mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}/\varphi(\pi)^k$. Since both are free $\mathbb{Z}_p$-modules of rank $k(p-1)$, this must be an isomorphism. ☐

Remark 3.8. *Following the terminology of* [Ber03, §II.6]*, we refer to the inverse of $\mathfrak{M}$ as the* Mellin transform.

Let $n_1^0, \dots, n_d^0$ be a basis of $\mathbb{N}(T)$. Since the action of G_∞ on $\mathbb{N}(T)$ is trivial modulo π, we have $(1-g)n_i^0 \in \pi\mathbb{N}(T)$ for all $1 \leq i \leq d$ and for all $g \in G_\infty$.

Lemma 3.9. *Let g be a topological generator of G_∞, and write $(1-g)n_i^0 = \pi m_i$ for some $m_i \in \mathbb{N}(T)$. If we put $n_i = n_i^0 - \frac{\pi m_i}{1-\chi(g)}$, then $n_1, \dots, n_d$ is a basis of $\mathbb{N}(T)$, and $(1-\gamma)n_i \in \pi^2\mathbb{N}(T)$.*

Proof. Note that since $p \neq 2$ and g is a topological generator of G_∞, $1-\chi(g) \in \mathbb{Z}_p^\times$, so $n_i \in \mathbb{N}(T)$ for all i, and they are obviously a basis. Since $g(\pi) = \chi(g)\pi + \mathcal{O}(\pi^2)$, this basis is designed such that $(1-g)n_i \in \pi^2\mathbb{N}(T)$, and this implies that $(1-g)n_i \in \pi^2\mathbb{N}(T)$. ☐

Let $\mathcal{N}$ be the $\Lambda(G_\infty)$-submodule of $(\varphi^*(\mathbb{N}(T))^{\psi=0}$ generated by $(1+\pi)\varphi(n_1), \dots, (1+\pi)\varphi(n_d)$.

Lemma 3.10. *Let $y \in (\varphi^*\mathbb{N}(T))^{\psi=0}$. Then there exist $\mathfrak{n} \in \mathcal{N}$ and $z \in (\varphi^*(\mathbb{N}(T))^{\psi=0}$ such that $y = \mathfrak{n} + \varphi(\pi)z$.*

Proof. Write $y = \sum_{i=1}^d y_i\varphi(n_i)$ with $y_i \in (\mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$. By Lemma 3.7 we can write $y_i = b_i(1+\pi)$ for some $b_i \in \Lambda(G_\infty)$, and Lemma 3.9 implies that $b_in_i \equiv n_i \mod \pi^2\mathbb{N}(T)$. Therefore, we have

$$\sum_{i=1}^d b_i\big((1+\pi)\varphi(n_i)\big) - \sum_{i=1}^d y_i\varphi(n_i) \in \varphi(\pi)^2(\varphi^*\mathbb{N}(T))^{\psi=0},$$

which is slightly better than the lemma. ☐

Lemma 3.10 can be generalized to all $k \geq 0$:

Proposition 3.11. *Let $k \geq 0$ and $y \in \varphi(\pi)^k(\varphi^*\mathbb{N}(T))^{\psi=0}$. Then there exists $\mathfrak{n} \in p_k\mathcal{N}$ and $z \in (\varphi^*\mathbb{N}(T))^{\psi=0}$ such that $y = \mathfrak{n} + \varphi(\pi)^{k+1}z$.*

Proof. The case $k = 0$ is just Lemma 3.10. Assume that $k \geq 1$, and that the result is true for $k-1$. If $y = \sum_{i=1}^d y_i\varphi(n_i)$ with $y_i \in \varphi(\pi)^k(\mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$, then we can write $y_i = b_i(1+\pi)$ with $b_i \in p_k\Lambda(G_\infty)$ by Lemma 3.7. By the definition of p_k, we can write $b_i = (1-a\gamma)c_i$ with $a = \chi(\gamma)^{1-k}$ for some $c_i \in \Lambda(G_\infty)$. Moreover, $p_{k-1}|c_i$ for all i. Let $x_i = c_i(1+\pi)$, then

$$\begin{aligned}\sum_{i=1}^d y_i\varphi(n_i) &= \sum_{i=1}^d((1-a\gamma)x_i)\varphi(n_i)\\ &= (1-a\gamma)\left(\sum_{i=1}^d x_i\varphi(n_i)\right) - a\sum_{i=1}^d \gamma(x_i)((1-\gamma)\varphi(n_i))\end{aligned}$$

by Lemma 3.6. Let $z_0 := \sum_{i=1}^d \gamma(x_i)((1-\gamma)\varphi(n_i))$. By Lemma 3.9 and the fact that $p_{k-1}|c_i$ (so $\varphi(\pi)^{k-1}|x_i$), we have $z_0 \in \varphi(\pi)^{k+1}(\varphi^*\mathbb{N}(T))^{\psi=0}$.

Consider the element $\sum_{i=1}^d x_i\varphi(n_i)$ where $x_i = c_i(1+\pi)$ is divisible by $\varphi(\pi)^{k-1}$ by Lemma 3.7 as $p_{k-1}|c_i$. Therefore, by induction, we can write $\sum_{i=1}^d x_i\varphi(n_i)$ as $x + \varphi(\pi)^k w$ with $x \in p_{k-1}\mathcal{N}$ and $w \in (\varphi^*\mathbb{N}(T))^{\psi=0}$. If we set

$$\begin{aligned} \mathfrak{n} &= (1-a\gamma)(x),\\ \varphi(\pi)^{k+1}z &= z_0 + (1-\chi(\gamma)^{-k}\gamma)(\varphi(\pi)^k w) \quad \text{and}\\ py_1 &= \big(\chi(\gamma)^{1-k} - \chi(\gamma)^{-k}\big)\gamma(\varphi(\pi)^k w), \end{aligned}$$

then $y = \mathfrak{n} + \varphi(\pi)^{k+1}z + py_1$ with $\mathfrak{n} \in p_k\mathcal{N}$, $z \in (\varphi^*\mathbb{N}(T))^{\psi=0}$ and $y_1 \in \varphi(\pi)^k(\varphi^*\mathbb{N}(T))^{\psi=0}$.

Iterating this gives us $y_j \in (\varphi^*\mathbb{N}(T))^{\psi=0}$ and converging sequences $\mathfrak{n}_j \in \mathcal{N}$ and $z_n \in (\varphi^*\mathbb{N}(T))^{\psi=0}$ such that

$$y = \mathfrak{n}_j + \varphi(\pi)^{k+1}z_j + p^j y_j.$$

The proposition follows by taking $\mathfrak{n}$ and z to be the limits of $\mathfrak{n}_j$ and z_j, respectively. □

Proof of Theorem 3.5. If $y \in (\varphi^*\mathbb{N}(T))^{\psi=0}$, the iterating Proposition 3.11 shows that for all $k \geq 0$ we can write

$$y = \mathfrak{n}_0 + \mathfrak{n}_1 + \cdots + \mathfrak{n}_k + \varphi(\pi)^{k+1}z$$

with $\mathfrak{n}_j \in p_j\mathcal{N}$. Passing to the limit over k shows that $y = \sum_{i\geq 0}\mathfrak{n}_i \in \mathcal{N}$, which shows that $(1+\pi)\varphi(n_1), \ldots, (1+\pi)\varphi(n_d)$ form a generating set of the $\Lambda(G_\infty)$-module $(\varphi^*\mathbb{N}(T))^{\psi=0}$.

Finally, the map $\Lambda(G_\infty)^{\oplus d}/p_k\Lambda(G_\infty)^{\oplus d} \to (\varphi^*\mathbb{N}(T))^{\psi=0}/\varphi(\pi)^k(\varphi^*\mathbb{N}(T))^{\psi=0}$ is a surjective map between two $\mathbb{Z}_p$-modules of equal rank, so that it is injective, and therefore the kernel of $\Lambda(G_\infty)^{\oplus d} \to (\varphi^*\mathbb{N}(T))^{\psi=0}$ is equal to $\bigcap_{k\geq 0} p_k\Lambda(G_\infty)^d = 0$. This finishes the proof. □

We now resume our assumption that V is a positive crystalline E-linear representation of $G_{\mathbb{Q}_p}$, with Hodge–Tate weights $-r_i$ such that $\sum_i r_i = m$, and $T \subset V$ an $\mathcal{O}_E$-lattice, as above. Applying theorem 3.5 to the representation $V(m)$, we find that for any basis $n_1^0, \ldots, n_d^0$ of $\mathbb{N}(T)$, there is a basis $n_1, \ldots, n_d$ of $\mathbb{N}(T)$ with $n_i = n_i^0 \bmod \pi$ such that the vectors $(1+\pi)\varphi(\pi^{-m}n_i \otimes e_m)$ are a basis of $(\varphi^*\mathbb{N}(T(m))^{\psi=0}$ as a $\Lambda_{\mathcal{O}_E}$-module. With respect to such a basis $n_1, \ldots, n_d$, we make the following definitions:

Definition 3.12. *Define the* Iwasawa transform *to be the $\Lambda_{\mathcal{O}_E}(G_\infty)$-equivariant isomorphism*

$$\mathfrak{J} : (\varphi^*\mathbb{N}(T(m)))^{\psi=0} \longrightarrow \Lambda_{\mathcal{O}_E}(G_\infty)^{\oplus d}$$

determined by sending $(1+\pi)\varphi(n_i \otimes \pi^{-m}e_m)$ to $(0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 is the i-th entry.

Definition 3.13. *Define $\underline{\mathrm{Col}} : \mathbb{N}(T(m))^{\psi=1} \to \Lambda_{\mathcal{O}_E}(G_\infty)^{\oplus d}$ as $\mathfrak{J} \circ (1-\varphi)$, and for $1 \leq i \leq d$, let $\underline{\mathrm{Col}}_i : \mathbb{N}(T(m))^{\psi=1} \to \Lambda_{\mathcal{O}_E}(G_\infty)$ be the composition of $\underline{\mathrm{Col}}$ with the projection onto the i-th component.*

Note 3.14. *For all $1 \leq i \leq d$, the map $\underline{\mathrm{Col}}_i$ is $\Lambda_{\mathcal{O}_E}(G_\infty)$-equivariant.*

3.2. **Comparison with $\mathbb{D}_{\mathrm{cris}}$.** We now give an alternative formula for the Coleman maps of the previous subsection using the comparison isomorphisms between the Wach module $\mathbb{N}(V)$ and $\mathbb{D}_{\mathrm{cris}}(V)$.

Recall from section 2.2 that for any positive crystalline representation V we have a canonical isomorphism $\mathbb{N}(V)/\pi\mathbb{N}(V) \cong \mathbb{D}_{\mathrm{cris}}(V)$ ([Ber03, § III.4]).

Lemma 3.15. *Let V be a positive crystalline E-linear representation of $G_{\mathbb{Q}_p}$. Given any basis $\nu_1, \ldots, \nu_d$ of $\mathbb{D}_{\mathrm{cris}}(V)$ over E, we can lift it to a basis of $n_1, \ldots, n_d$ of $\mathbb{N}(V)$ over $E \otimes \mathbb{B}^+_{\mathbb{Q}_p}$. Moreover, we may assume that $(1+\pi)\varphi(\pi^{-m}n_1 \otimes e_m), \ldots, (1+\pi)\varphi(\pi^{-m}n_d \otimes e_m)$ is a $\Lambda_E(G_\infty)$-basis of $(\varphi^*\mathbb{N}(V(m)))^{\psi=0}$.*

Proof. Let T be a $G_{\mathbb{Q}_p}$-stable $\mathcal{O}_E$-lattice in V. By theorem 3.5 above, we may choose a $\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p}$-basis $\bar{n}_1, \ldots, \bar{n}_d$ of $\mathbb{N}(T)$ such that $(1+\pi)\varphi(\pi^{-m}\bar{n}_i \otimes e_m)$ is a $\Lambda_{\mathcal{O}_E}(G_\infty)$-basis of $(\varphi^*\mathbb{N}(T(m)))^{\psi=0}$. Hence these elements are also a $\Lambda_E(G_\infty)$-basis of $(\varphi^*\mathbb{N}(V(m)))^{\psi=0}$.

By the comparison isomorphism, the elements $\{\bar{\nu}_i := \bar{n}_i \bmod \pi : i = 1, \ldots, d\}$ give a basis of $\mathbb{D}_{\mathrm{cris}}(V)$ over E. Let $A \in GL_d(E)$ be the change of basis matrix from $\nu_1, \ldots, \nu_d$ to $\bar{\nu}_1, \ldots, \bar{\nu}_d$. On applying A^{-1} to

$\bar{n}_1, \ldots, \bar{n}_d$, we obtain a basis $n_1, \ldots, n_d$ of $\mathbb{N}(V)$ lifting $\nu_1, \ldots, \nu_d$. Now it is clear that $(1+\pi)\varphi(\pi^{-m}n_1 \otimes e_m), \ldots, (1+\pi)\varphi(\pi^{-m}n_d \otimes e_m)$ is a $\Lambda_E(G_\infty)$-basis of $(\varphi^*\mathbb{N}(V(m)))^{\psi=0}$, since it differs from the original basis by the scalar matrix A^{-1}, which is clearly invertible in $\Lambda_E(G_\infty)$. □

With respect to such a basis $n_1, \ldots, n_d$ of $\mathbb{N}(V)$, we can clearly define an Iwasawa transform and Coleman map as above but with E-coefficients,

$$\mathfrak{J} : (\varphi^*\mathbb{N}(V(m)))^{\psi=0} \xrightarrow{\cong} \Lambda_E(G_\infty)^{\oplus d}$$
$$\underline{\mathrm{Col}} : \mathbb{N}(V(m))^{\psi=1} \longrightarrow \Lambda_E(G_\infty)^{\oplus d},$$

which are homomorphisms of $\Lambda_E(G_\infty)$-modules.

Remark 3.16. *If T is an $\mathcal{O}_E$-lattice in V stable under $G_{\mathbb{Q}_p}$ and the $\mathcal{O}_E$-lattice in $\mathbb{D}_{\mathrm{cris}}(V)$ spanned by $\nu_1, \ldots, \nu_d$ is the reduction of $\mathbb{N}(T)$, then we can define the Coleman maps integrally, as in the previous section. In section 4 below we will work with a specific basis ν_i for which such a lattice T can be explicitly constructed.*

Now, let $\nu_1, \ldots, \nu_d$ be a basis of $\mathbb{D}_{\mathrm{cris}}(V)$ over E, and $n_1, \ldots, n_d$ a basis of $\mathbb{N}(V)$ lifting $\nu_1, \ldots, \nu_d$ as in lemma 3.15. We write A_φ for the matrix of φ on $\mathbb{D}_{\mathrm{cris}}(V)$ with respect to the basis $\nu_1, \ldots, \nu_d$. Again by [BB10, section 3], $E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$ is a Bézout ring and

$$[(E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}) \otimes_{E \otimes \mathbb{B}^+_{\mathbb{Q}_p}} \mathbb{N}(V) : (E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}) \otimes_E \mathbb{D}_{\mathrm{cris}}(V)] = \left[\left(\frac{t}{\pi}\right)^{r_1}; \cdots ; \left(\frac{t}{\pi}\right)^{r_d}\right]. \tag{7}$$

In other words, there exists $E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$-bases $w_1, \ldots, w_d$ and $v_1, \ldots, v_d$ for $(E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}) \otimes_{E \otimes \mathbb{B}^+_{\mathbb{Q}_p}} \mathbb{N}(V)$ and $(E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}) \otimes_E \mathbb{D}_{\mathrm{cris}}(V)$ respectively such that $v_i = (t/\pi)^{r_i} w_i$ for $i = 1, \ldots, d$. Therefore, the change of basis matrix $M' \in M_d(E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})$ with

$$\begin{pmatrix} \nu_1 \\ \vdots \\ \nu_d \end{pmatrix} = M' \begin{pmatrix} n_1 \\ \vdots \\ n_d \end{pmatrix}, \tag{8}$$

has determinant $(t/\pi)^m$ up to a unit in $E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$. Moreover, since $n_1, \ldots, n_d$ lifts $\nu_1, \ldots, \nu_d$, we have $M'|_{\pi=0} = I$, the identity matrix. The compatibility of the action of φ implies that

$$\varphi(M')P^T = A_\varphi^T M', \tag{9}$$

where P is the matrix of φ on $\mathbb{N}(V)$ with respect to the basis $n_1, \ldots, n_d$ as in the previous subsection. We can now rewrite (5):

$$x = \begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix} \cdot \left(\frac{t}{\pi}\right)^m M'^{-1} \begin{pmatrix} \nu_1 \\ \vdots \\ \nu_d \end{pmatrix} \otimes t^{-m} e_m \tag{10}$$

with $(t/\pi)^m M'^{-1} \in M_d(E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})$ and $\nu_i \otimes t^{-m} e_m$, $i = 1, \ldots, d$ a basis of $\mathbb{D}_{\mathrm{cris}}(V(m))$.

Rewriting (6) using this, we see that

$$(1-\varphi)(x) = \mathbf{Col}(x) \cdot \left(\frac{t}{\pi q}\right)^m P^T M'^{-1} \begin{pmatrix} \nu_1 \\ \vdots \\ \nu_d \end{pmatrix} \otimes t^{-m} e_m. \tag{11}$$

3.3. **Supersingular modular forms.** We now apply the theory of Coleman maps developed above to the Galois representations attached to modular forms.

Let $f = \sum a_n q^n$ be a normalized new eigenform of weight k and character ϵ. Let p be an odd prime which does not divide the level of f. For simplicity, we will always assume that $\epsilon(p) = 1$. In particular $a_p = \bar{a}_p$. We write $E = \mathbb{Q}_p(a_n : n \geq 1)$, which is the completion of the coefficient field F of f at the prime above p determined our choice of embeddings. Then, by Deligne [Del69], we can associate to f a 2-dimensional E-linear representation V_f of $G_{\mathbb{Q}}$. Moreover, when restricted to $G_{\mathbb{Q}_p}$, V_f is crystalline and its de Rham filtration is given by

$$\mathbb{D}^i_{\text{cris}}(V_f) = \begin{cases} E\nu_1 \oplus E\nu_2 & \text{if } i \leq 0 \\ E\nu_1 & \text{if } 1 \leq i \leq k-1 \\ 0 & \text{if } i \geq k \end{cases} \tag{12}$$

for some basis ν_1, ν_2 over E. We further assume that $v_p(a_p) \neq 0$, i.e. f is supersingular at p. Then ν_1 is not an eigenvector of φ by [Kat04, Theorem 16.6] and we may choose $\nu_2 = p^{1-k}\varphi(\nu_1)$ so that the matrix A_φ of φ with respect to the basis ν_1, ν_2 is given by

$$\begin{pmatrix} 0 & -1 \\ p^{k-1} & a_p \end{pmatrix}$$

since $\varphi^2 - a_p\varphi + p^{k-1} = 0$ (c.f. [Sch90]). We call such a basis a 'good basis' for $\mathbb{D}_{\text{cris}}(V_f)$.

Let $\bar{\nu}_1$ and $\bar{\nu}_2$ be a 'good basis' of $\mathbb{D}_{\text{cris}}(V_{\bar{f}})$. Then, the matrix of φ with respect to this basis is equal to A_φ also since $a_p = \bar{a}_p$.

Note that $V_{\bar{f}}$ has Hodge-Tate weights 0 and $-k+1$, so it is positive. Fix a basis n_1, n_2 of $\mathbb{N}(V_{\bar{f}})$ satisfying the conditions in Lemma 3.15, so $\begin{pmatrix} \bar{\nu}_1 \\ \bar{\nu}_2 \end{pmatrix} = M' \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$ with $M'|_{\pi=0} = I$. We obtain two pairs of Coleman maps associated to f:

$$\begin{aligned} \mathrm{Col}_i &: \mathbb{D}(V_{\bar{f}}(k-1))^{\psi=1} \longrightarrow (E \otimes \mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}, \\ \underline{\mathrm{Col}}_i &: \mathbb{D}(V_{\bar{f}}(k-1))^{\psi=1} \longrightarrow \Lambda_E(G_\infty), \end{aligned}$$

for $i = 1, 2$.

Recall the isomorphism (4) above:

$$h^1_{\mathbb{Q}_p,\mathrm{Iw}} : \mathbb{D}(V_{\bar{f}}(k-1))^{\psi=1} \cong H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V_{\bar{f}}(k-1)).$$

We can therefore consider the localization of Kato's zeta element $\mathbf{z}^{\text{Kato}}$ from [Kat04] (see section 6.1 below), which *a priori* is an element of $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V_{\bar{f}}(k-1))$, as an element of $\mathbb{D}(V_{\bar{f}}(k-1))^{\psi=1}$. We can now define two pairs of p-adic L-functions:

Definition 3.17. *For $i = 1, 2$, define $L_{p,i} = \mathrm{Col}_i(\mathbf{z}^{\text{Kato}}) \in (E \otimes \mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$ and $\tilde{L}_{p,i} = \underline{\mathrm{Col}}_i(\mathbf{z}^{\text{Kato}}) \in \Lambda_E(G_\infty)$ where $\mathbf{z}^{\text{Kato}}$ is the localization of the Kato zeta element.*

The reason why we consider $V_{\bar{f}}$ instead of V_f will become apparent in section 3.4 below. In addition, below is a list of assumptions which we will need later when we prove different results.

- **Assumption (A)**: $k \geq 3$ or $a_p = 0$.
- **Assumption (B)**: a_p is not of the form $p^j + p^{k-2-j}$ for some integer $1 \leq j \leq k-3$.
- **Assumption (C)**: $v_p(a_p) > \lfloor (k-2)/(p-1) \rfloor$.
- **Assumption (D)**: $p \geq k-1$.

3.4. **Relation to the Perrin-Riou pairing.** Let α and β be the roots of the quadratic $X^2 - a_pX + p^{k-1}$. By the work of Amice–Vélu and Vishik cited in the introduction, we can associate to α and β p-adic L-functions $L_{p,\alpha}$ and $L_{p,\beta}$ respectively; see [MTT86, §11] for an account of the construction. We will relate them to $L_{p,i}$, $i = 1, 2$, as defined above. We first prove some preliminary results on general crystalline representations.

Let γ be a topological generator of Γ. Define

$$\mathcal{H}(G_\infty) = \left\{ f(\gamma - 1) \mid f(X) \in \mathbb{Q}_p[\Delta][[X]] \text{ such that } f \text{ converges for all } X \in \mathbb{C}_p \text{ with } |X| < 1 \right\}.$$

We can identify $\mathcal{H}(G_\infty)$ with $(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}$ via the map

$$\begin{aligned} \mathfrak{M} : \mathcal{H}(G_\infty) &\longrightarrow (\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0} \\ f(\gamma-1) &\longmapsto f(\gamma-1)(\pi+1), \end{aligned} \tag{13}$$

where any $g \in G_\infty$ acts on π by $(\pi+1)^{\chi(g)}-1$. As shown in [PR01, B.2.8], this map is a bijection, extending the isomorphism $\Lambda(G_\infty) \to (\mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$ of Lemma 3.7. For $r \geq 1$, define

$$\mathcal{H}_r^{\mathrm{temp}} = \left\{ \sum_{\sigma\in\Delta}\sum_{n\geq 0} c_{n,\sigma}\sigma X^n : \lim_{n\to+\infty} \frac{|c_{n,\sigma}|_p}{n^r} = 0 \right\}.$$

Let $\mathcal{H}^{\mathrm{temp}} = \bigcup_{r\geq 1}\mathcal{H}_r^{\mathrm{temp}}$, and define $\mathcal{H}^{\mathrm{temp}}(G_\infty) = \{f(\gamma-1) \mid f(X) \in \mathcal{H}^{\mathrm{temp}}\}$.

Let V be any crystalline E-linear representation of $G_{\mathbb{Q}_p}$, and let h be a positive integer such that $\mathrm{Fil}^{-h}\,\mathbb{D}_{\mathrm{cris}}(V) = \mathbb{D}_{\mathrm{cris}}(V)$. . Denote by

$$\Omega_{V,h} : \left(\mathcal{H}^{\mathrm{temp}}(G_\infty)\otimes\mathbb{D}_{\mathrm{cris}}(V)\right)^{\Sigma=0} \longrightarrow \mathcal{H}^{\mathrm{temp}}(G_\infty)\otimes_{\Lambda_{\mathbb{Q}_p}} H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V)$$

Perrin-Riou's exponential map as constructed in [PR94]. Here,

$$\Sigma : \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}\otimes_{\mathbb{Q}_p}\mathbb{D}_{\mathrm{cris}}(V) \to \bigoplus_{k=0}^{h}\left(\mathbb{D}_{\mathrm{cris}}(V)/(1-p^k\varphi)\right)(k)$$

is the map sending $f \in \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}\otimes_{\mathbb{Q}_p}\mathbb{D}_{\mathrm{cris}}(V)$ to the class of $\oplus\partial^k(f)(0)$, where $\partial = (1+\pi)\frac{d}{d\pi}$ is the derivation on $\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$ defined in §2.2. Since $\Omega_{V,h}$ is a homomorphism of $\mathcal{H}^{\mathrm{temp}}(G_\infty)$-modules, we can extend scalars to get

$$\Omega_{V,h} : \left((\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}\otimes\mathbb{D}_{\mathrm{cris}}(V)\right)^{\Sigma=0} \longrightarrow \mathcal{H}(G_\infty)\otimes_{\Lambda_{\mathbb{Q}_p}} H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V), \tag{14}$$

where we identify $(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}$ with $\mathcal{H}(G_\infty)$ via $\mathfrak{M}$.

Remark 3.18. *We will only apply (14) to elements in which lie in the image of $\mathcal{H}^{\mathrm{temp}}(G_\infty)\otimes\mathbb{D}_{\mathrm{cris}}(V)$ under $\mathfrak{M}$, so we can refer to [PR94] for the properties of $\Omega_{V,h}$. The reason for extending scalars to $\mathcal{H}(G_\infty)$ is that we want to be able to use Berger's description of the exponential map in [Ber03, §II.5].*

Recall that we have chosen a p-power compatible system $\varepsilon^{(n)}$, $n \geq 0$, of p-power roots of unity.

Proposition 3.19. *Assume that V is a crystalline representation of $G_{\mathbb{Q}_p}$. Let $h \geq 1$ such that $\mathbb{D}^{-h}_{\mathrm{cris}}(V) = \mathbb{D}_{\mathrm{cris}}(V)$ and p^{-j} is not an eigenvalue of φ on $\mathbb{D}_{\mathrm{cris}}(V)$ for $j \in \mathbb{Z}$ with $0 \leq j \leq h$. Then, for all $v \in \mathbb{D}_{\mathrm{cris}}(V)$, the projection to the n-th local cohomology $H^1(\mathbb{Q}_{p,n}, V)$ of $\frac{1}{(h-1)!}\Omega_{V,h}((1+\pi)\otimes v)$ is given by*

$$\begin{cases} p^{-n}\exp_{F_n,V}\left(\sum_{m=0}^{n-1}\varepsilon^{(n-m)}\otimes\varphi^{m-n}(v) + (1-\varphi)^{-1}(v)\right) & \text{if } n \geq 1 \\ \exp_{\mathbb{Q}_p,V}\left(\left(1-\frac{\varphi^{-1}}{p}\right)(1-\varphi)^{-1}(v)\right) & \text{if } n = 0. \end{cases} \tag{15}$$

Proof. Let $g \in (\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}\otimes_{\mathbb{Q}_p}\mathbb{D}_{\mathrm{cris}}(V)$. We write $\Delta_j(g) = \partial^j(g)(0)$ and

$$\tilde{g} = g - \sum_{j=0}^{h}\frac{1}{j!}\log_p^j\Delta_j(g).$$

By [PR94, section 2.2], the sum $\sum_{n=0}^{\infty}\varphi^n(\tilde{g})$ converges. A solution to $(1-\varphi)G = g$ with $G \in \left(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}\otimes_{\mathbb{Q}_p}\mathbb{D}_{\mathrm{cris}}\right)^{\psi=1}$ is given by

$$G = \sum_{n=0}^{\infty}\varphi^n(\tilde{g}) + \sum_{j=0}^{h}\frac{1}{j!}\log_p^j v_j$$

where $v_j \in \mathbb{D}_{\mathrm{cris}}(V)$ is such that $\Delta_j(g) = (1 - p^j\varphi)v_j$. Now, take $g = (1+\pi)\otimes v$, so $\Delta_j(g) = v$ for all j. Let n be a positive integer, then

$$\varphi^m(\tilde{g})(\varepsilon^{(n)} - 1) = \begin{cases} (\varepsilon^{(n-m)} - 1)\otimes \varphi^m(v) & \text{if } m < n \\ 0 & \text{otherwise.} \end{cases} \tag{16}$$

Therefore, we have

$$\begin{aligned} G(\varepsilon^{(n)} - 1) &= \sum_{m=0}^{n-1} (\varepsilon^{(n-m)} - 1)\otimes \varphi^m(v) + (1-\varphi)^{-1}(v) \\ &= \sum_{m=0}^{n-1} \varepsilon^{(n-m)} \otimes \varphi^m(v) + (1-\varphi)^{-1}\varphi^n(v) \end{aligned}$$

Hence, by the main result in [PR94], the n-th component of $\frac{1}{(h-1)!}\Omega_{V,h}((1+\pi)\otimes v)$ is given by the image of

$$p^{-n}\varphi^{-n}G(\varepsilon^{(n)} - 1) = \frac{1}{p^n}\left(\sum_{m=0}^{n-1} \varepsilon^{(n-m)}\otimes\varphi^{m-n}(v) + (1-\varphi)^{-1}(v)\right) \tag{17}$$

under the map $\exp_{\mathbb{Q}_{p,n},V}$. For the 0-th level, it is given by the image of

$$\begin{aligned} \mathrm{Tr}_{\mathbb{Q}_{p,1}/\mathbb{Q}_p}\left(\frac{1}{p}\varphi^{-1}G(\varepsilon^{(1)} - 1)\right) &= \frac{1}{p}\,\mathrm{Tr}_{\mathbb{Q}_{p,1}/\mathbb{Q}_p}(\varepsilon^{(1)}\otimes\varphi^{-1}(v) + (1-\varphi)^{-1}(v)) \\ &= \frac{1}{p}\left(-1\otimes\varphi^{-1}(v) + (p-1)(1-\varphi)^{-1}(v)\right) \\ &= \left(1 - \frac{\varphi^{-1}}{p}\right)(1-\varphi)^{-1}(v). \end{aligned}$$

under the map $\exp_{\mathbb{Q}_p,V}$, so we are done. $\square$

Define the Perrin-Riou pairing $\langle\ ,\ \rangle_V$ by

$$\begin{aligned} \langle\ ,\ \rangle_V : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V)\times H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V^*(1)) &\longrightarrow \Lambda_E(G_\infty), \\ \langle (x_n),(y_n)\rangle_V &= \varprojlim \Sigma_{\tau\in G_{\mathbb{Q}_p}/G_{\mathbb{Q}_p}^{p^n}}(\tau(x_n)\cup y_n)\tau. \end{aligned}$$

Remark 3.20. *In [PR94], the pairing is defined by*

$$\langle (x_n),(y_n)\rangle_V = \varprojlim \Sigma_{\tau\in G_{\mathbb{Q}_p}/G_{\mathbb{Q}_p}^{p^n}}(\tau^{-1}(x_n)\cup y_n)\tau.$$

We use the different convention so that the map $\mathcal{L}_{h,z}$ defined in (18) below is a $\Lambda(G_\infty)$-homomorphism.

We can extend the pairing $\langle\ ,\ \rangle_V$ to

$$\langle\ ,\ \rangle_V : \left(\mathcal{H}(G_\infty)\otimes_{\Lambda_{\mathbb{Q}_p}} H^1_{\mathrm{Iw}}(\mathbb{Q}_p,V)\right)\times\left(\mathcal{H}(G_\infty)\otimes_{\Lambda_{\mathbb{Q}_p}} H^1_{\mathrm{Iw}}(\mathbb{Q}_p,V^*(1))\right)\longrightarrow\mathcal{H}(G_\infty).$$

Any $z \in \left((\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}\otimes\mathbb{D}_{\mathrm{cris}}(V)\right)^{\Sigma=0}$ therefore defines a map

$$\begin{aligned} \mathcal{L}_{h,z} : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V^*(1)) &\longrightarrow \mathcal{H}(G_\infty), \\ (y_n)_{n\geq 0} &\longmapsto \left\langle \Omega_{h,V}(z),(y_n)\right\rangle_V. \end{aligned} \tag{18}$$

As recalled in section 2.3 above, for any p-adic representation V of $G_{\mathbb{Q}_p}$ we have a canonical isomorphism

$$h^1_{\mathbb{Q}_p,\mathrm{Iw}} : \mathbb{D}(V)^{\psi=1}\cong H^1_{\mathrm{Iw}}(\mathbb{Q}_p,V).$$

Lemma 3.21. *For all $j\in\mathbb{Z}$ and for all $y\in\mathbb{D}(V)^{\psi=1}$ and $y'\in\mathbb{D}(V^*(1))^{\psi=1}$, we have*

$$\partial^j\langle h^1_{\mathbb{Q}_p,\mathrm{Iw}}(y), h^1_{\mathbb{Q}_p,\mathrm{Iw}}(y')\rangle_V = \langle h^1_{\mathbb{Q}_p,\mathrm{Iw}}(y\otimes e_j), h^1_{\mathbb{Q}_p,\mathrm{Iw}}(y'\otimes e_{-j})\rangle_{V(j)}.$$

Proof. See Lemme ii) Section 3.6 in [PR94]. $\square$

We now return to the setting in Section 3.3. We will apply Perrin-Riou's theory that we recalled above to the crystalline representation $V_f(1)$. In particular, $V_f(1)^*(1) \cong V_{\bar{f}}(k-1)$. By (12), we can take $h=1$. Note that φ acts on $\mathbb{D}_{\mathrm{cris}}(V_f(1))$ by $\begin{pmatrix} 0 & -p^{-1} \\ p^{k-2} & p^{-1}a_p \end{pmatrix}$ with respect to a 'good basis' $\nu_i \otimes t^{-1}e_1$, $i=1,2$ as chosen in Section 3.3. But $a_p \neq p+p^{k-2}$ by the Weil bound, so both $1-\varphi$ and $1-p\varphi$ are isomorphisms on $\mathbb{D}_{\mathrm{cris}}(V_f(1))$ and $\Sigma = 0$. Let $\bar{\nu}_1, \bar{\nu}_2$ be a 'good basis' for $\mathbb{D}_{\mathrm{cris}}(V_{\bar{f}})$. We can identify $\mathbb{D}_{\mathrm{cris}}(V_f)$ with $\mathbb{D}_{\mathrm{cris}}(V_f(1))$ (resp. $\mathbb{D}_{\mathrm{cris}}(V_{\bar{f}})$ with $\mathbb{D}_{\mathrm{cris}}(V_{\bar{f}}(k-1))$) via $\nu_i \mapsto \nu_i \otimes e_1 t^{-1}$ (resp. $\bar{\nu}_i \mapsto \bar{\nu}_i \otimes e_{k-1}t^{1-k}$). Under these identifications, the natural pairing

$$[\ ,\ ] : \mathbb{D}_{\mathrm{cris}}(V_f(1)) \times \mathbb{D}_{\mathrm{cris}}(V_{\bar{f}}(k-1)) \to \mathbb{D}_{\mathrm{cris}}(E(1)) = E \cdot e_1 t^{-1} \tag{19}$$

satisfies $[\nu_1, \bar{\nu}_1] = 0$. By applying φ, we have $[\nu_2, \bar{\nu}_2] = 0$, too. We also have $[\nu_1, \bar{\nu}_2] = -[\nu_2, \bar{\nu}_1] \neq 0$. Without loss of generality, we may assume that $[\nu_1, \bar{\nu}_2] = -[\nu_2, \bar{\nu}_1] = 1$

Let $x \in \mathbb{D}(V_{\bar{f}}(k-1))^{\psi=1}$. It follows from the construction of the Coleman maps in Section 3.3 that if we let

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = \left(\frac{t}{\pi q}\right)^{k-1} P^T M'^{-1}, \tag{20}$$

then, by (11), $(1-\varphi)(x)$ can be written as

$$(1-\varphi)(x) = (y_1 m_{11} + y_2 m_{21})\bar{\nu}_1 \otimes t^{1-k}e_{k-1} + (y_1 m_{12} + y_2 m_{22})\bar{\nu}_2 \otimes t^{1-k}e_{k-1}, \tag{21}$$

where $y_i = \mathrm{Col}_i(x)$ for $i = 1,2$.

Proposition 3.22. *On identifying with their images under $\mathfrak{M}$, we have*

$$\langle \Omega_{V_f(1),1}((1+\pi)\otimes\nu_1), x\rangle_{V_f(1)} = y_1 m_{12} + y_2 m_{22}, \tag{22}$$

$$-\langle \Omega_{V_f(1),1}((1+\pi)\otimes\nu_2), x\rangle_{V_f(1)} = y_1 m_{11} + y_2 m_{21}. \tag{23}$$

The rest of this section is devoted to proving this result. We follow closely Berger's proof of Perrin-Riou's explicit reciprocity law in [Ber03]. We first make the following definition: let $V \in \mathrm{Rep}_{\mathbb{Q}_p}(G_{\mathbb{Q}_p})$. For an element $x \in H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V)$, define $h^1_{\mathbb{Q}_p,V}(x)$ to be the image of x under the projection map $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \to H^1(\mathbb{Q}_p, V)$.

Recall also the map ∂_V defined in subsection 2.2: for $z \in \mathbb{Q}_{p,n}((t)) \otimes_{\mathbb{Q}_p} \mathbb{D}_{\mathrm{cris}}(V_f(1+j))$, we denote the constant coefficient of z by $\partial_{V_f(1+j)}(z) \in \mathbb{Q}_{p,n} \otimes_{\mathbb{Q}_p} \mathbb{D}_{\mathrm{cris}}(V_f(1+j))$.

Lemma 3.23. *Let $i \in \{1,2\}$, and choose $\mathfrak{y}_i \in \left(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p} \otimes_{\mathbb{Q}_p} \mathbb{D}_{\mathrm{cris}}(V_f(1))\right)^{\psi=1}$ such that $(1-\varphi)\mathfrak{y}_i = (1+\pi)\otimes\nu_i$. Then*

$$h^1_{\mathbb{Q}_p,V_f(1+j)}\Omega_{V_f(1+j),1+j}\left(\partial^{-j}(1+\pi)\otimes\nu_i\otimes t^{-j}e_j\right) = j!\exp_{\mathbb{Q}_p,V_f(1+j)}\left(\left(1-\frac{\varphi^{-1}}{p}\right)\partial_{V_f(1+j)}\left(\partial^{-j}\mathfrak{y}_i\otimes t^{-j}e_j\right)\right).$$

Proof. By Proposition 3.19, we need to prove that $\partial_{V_f(1+j)}\left(\partial^{-j}\mathfrak{y}_i \otimes t^{-j}e_j\right) = (1-\varphi)^{-1}(\nu_i \otimes t^{-j}e_j)$. Note that φ commutes with $\partial_{V_f(1+j)}$ and $\varphi\circ\partial^{-j} = p^j\partial^{-j}\circ\varphi$, so

$$(1-\varphi)\partial_{V_f(1+j)}\left(\partial^{-j}\mathfrak{y}_i\otimes t^{-j}e_j\right) = \partial_{V_f(1+j)}\left(\partial^{-j}(1+\pi)\otimes\nu_i\otimes t^{-j}e_j\right).$$

Note that $\partial(1+\pi) = 1+\pi$, so $\partial_{V_f(1+j)}\left(\partial^{-j}(1+\pi)\otimes\nu_i\otimes t^{-j}e_j\right) = \nu_i\otimes t^{-j}e_j$. Also, as observed above, $1-\varphi$ is invertible on $\mathbb{D}_{\mathrm{cris}}(V_f(1))$, which proves the result. ∎

We can now prove Proposition 3.22. We will only prove (23) here; the proof of (22) is analogous.

Proof. For $i=1,2$, let $\mathfrak{y}_i \in \left(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}\otimes_{\mathbb{Q}_p}\mathbb{D}_{\mathrm{cris}}(V_f(1))\right)^{\psi=1}$ such that $(1-\varphi)\mathfrak{y}_i = (1+\pi)\otimes\nu_i$. By p-adic interpolation it is sufficient to show that

$$\partial^j\left(\left\langle\Omega_{V_f(1),1}((1+\pi)\otimes\nu_2), h^1_{\mathbb{Q}_p,\mathrm{Iw}}(x)\right\rangle_{V_f(1)}\right)(0) = \partial^j\left(y_1m_{12}+y_2m_{22}\right)(0)$$

for all $j \gg 0$. We have

$$\begin{aligned} &\partial^j\big(\langle \Omega_{V_f(1),1}((1+\pi)\otimes\nu_2), x\rangle_{V_f(1)}\big) = \big\langle \Omega_{V_f(1),1}\big((1+\pi)\otimes\nu_2\big)\otimes e_j, h^1_{\mathrm{Iw},V_{\bar f}(k-1-j)}(x\otimes e_{-j})\big\rangle_{V_f(1+j)} \\ &= (-1)^j\big\langle \Omega_{V_f(1+j),1+j}\big(\partial^{-j}(1+\pi)\otimes\nu_2\otimes t^{-j}e_j\big), h^1_{\mathrm{Iw},V_{\bar f}(k-1-j)}(x\otimes e_{-j})\big\rangle_{V_f(1+j)} \qquad (24)\end{aligned}$$

by Lemma 3.21 and the properties of Ω (c.f. p. 119, Théorème (B)(ii) in [PR94]). Hence

$$\begin{aligned} &\partial^j\big(\langle \Omega_{V_f(1),1}((1+\pi)\otimes\nu_2), x\rangle_{V_f(1)}\big)(0) \\ &= (-1)^j\big\langle h^1_{\mathbb{Q}_p,V_f(1+j)}\Omega_{V_f(1+j),1+j}\big(\partial^{-j}(1+\pi)\otimes\nu_2\otimes t^{-j}e_j\big), h^1_{\mathbb{Q}_p,V_{\bar f}(k-1-j)}(x\otimes e_{-j})\big\rangle_{V_f(1+j)} \qquad (25)\\ &= j!\Big\langle \exp_{\mathbb{Q}_p,V_f(1+j)}\Big(\Big(1-\frac{\varphi^{-1}}{p}\Big)\partial_{V_f(1+j)}\big(\partial^{-j}\mathfrak{y}_2\otimes t^{-j}e_j\big)\Big), h^1_{\mathbb{Q}_p,V_{\bar f}(k-1-j)}(x\otimes e_{-j})\Big\rangle_{V_f(1+j)} \qquad (26)\\ &= j!\Big[\Big(1-\frac{\varphi^{-1}}{p}\Big)\partial_{V_f(1+j)}\big(\partial^{-j}\mathfrak{y}_2\otimes t^{-j}e_j\big), \exp^*_{\mathbb{Q}_p,V^*(1+j)} h^1_{\mathbb{Q}_p,V_{\bar f}(k-1-j)}(x\otimes e_{-j})\Big]_{V_f(1+j)} \qquad (27)\\ &= j!\Big[\Big(1-\frac{\varphi^{-1}}{p}\Big)\partial_{V_f(1+j)}\big(\partial^{-j}\mathfrak{y}_2\otimes t^{-j}e_j\big), \Big(1-\frac{\varphi^{-1}}{p}\Big)\partial_{V_{\bar f}(k-1-j)}(x\otimes e_{-j})\Big]_{V_f(1+j)} \qquad (28)\\ &= j!\big[\partial_{V_f(1+j)}\big(\partial^{-j}(1+\pi)\otimes\nu_2\otimes t^{-j}e_j\big), \partial_{V_{\bar f}(k-1-j)}((1-\varphi)x\otimes e_{-j})\big]_{V_f(1+j)} \qquad (29)\end{aligned}$$

The equalities can be explained as follows:

- the first equality is immediate from (24) and the construction of $\langle\ ,\ \rangle_V$;
- the implication (25)$\Rightarrow$ (26) follows from Lemma 3.23;
- the implication (26)$\Rightarrow$ (27) is the duality between $\exp_{F,V_f(1+j)}$ and $\exp^*_{F,V_f(1+j)}$;
- the implication (27)$\Rightarrow$ (28) follows from [Ber03, Theorem II.6], and
- (29) follows from (28) since $1-\varphi$ is the adjoint of $1-\frac{\varphi^{-1}}{p}$ under the pairing $[\ ,\ ]$.

Now $\partial(1+\pi) = 1+\pi$, which implies that $\partial^{-j}(1+\pi)\otimes\nu_2\otimes t^{-j}e_j = (1+\pi)\otimes\nu_2\otimes t^{-j}e_j$ and hence

$$\partial_{V_f(1+j)}\big(\partial^{-j}(1+\pi)\otimes\nu_2\otimes t^{-j}e_j\big) = \nu_2\otimes t^{-j}e_j.$$

By (21), we can write

$$(1-\varphi)x = (y_1m_{11}+y_2m_{21})\bar\nu_1 + (y_1m_{12}+y_2m_{22})\bar\nu_2.$$

Recall that by construction, we have $[\nu_2,\bar\nu_1] = -1$ and $[\nu_i,\bar\nu_i] = 0$ for $i=1,2$. It follows that if we write $-(y_1m_{11}+y_2m_{21}) = \Sigma_{i\geq 0}c_it^i$ with $c_i\in\mathbb{Q}_p$, then (29) is equal to $j!c_j$. Since also $-\partial^j\big(y_1m_{11}+y_2m_{21})\big)(0) = j!c_j$, this finishes the proof of (23). $\square$

We can summarize the results of this section by the following corollary:

Corollary 3.24. *We have a commutative diagram*

$$\begin{tikzcd} \mathbb{N}(V)^{\psi=1} \arrow[r, "h^1_{\mathbb{Q}_p,\mathrm{Iw}}"] \arrow[d, "1-\varphi"'] & H^1_{\mathrm{Iw}}(\mathbb{Q}_p,V) \arrow[d, "(\underline{\mathrm{Col}}_1,\underline{\mathrm{Col}}_2)"'] \arrow[dddd, bend left, "\mathcal{L}_{1,\bar\nu_i\otimes(1+\pi)}"] \\ (\varphi^*\mathbb{N}(V))^{\psi=0} \arrow[r, "\mathfrak{I}"] \arrow[d, "M"'] & \Lambda_{\mathbb{Q}_p}(G_\infty)^{\oplus 2} \arrow[d, "\underline{M}"'] \\ \big((\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}\big)^{\oplus 2} \arrow[r, "\mathfrak{M}^{-1}"] \arrow[d, "\mathrm{pr}_i"'] & \mathcal{H}(G_\infty)^{\oplus 2} \arrow[d, "\underline{\mathrm{pr}}_i"'] \\ (\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0} \arrow[r, "\mathfrak{M}^{-1}"] & \mathcal{H}(G_\infty). \end{tikzcd}$$

Here, pr_i *and* $\underline{\mathrm{pr}}_i$ *denote the projection maps onto the respective* i*-th components, and for an element* $x \in (\varphi^*\mathbb{N}(V))^{\psi=0}$, $\underline{M}.x$ *is defined as follows: if* $x = x_1\varphi(\pi^{1-k}n_1 \otimes e_{k-1}) + x_2\varphi(\pi^{1-k}n_2 \otimes e_{k-1})$ *with* $x_1, x_2 \in (\mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$*, then* $M.x = M\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

3.5. **Bounded p-adic L-functions.** We now establish some basic properties of $L_{p,i}$ and $\tilde{L}_{p,i}$.

3.5.1. *Decomposition of p-adic L-functions.* Recall that α and β are the roots of the quadratic $X^2 - a_pX + p^{k-1}$. By [Kat04, Theorem 16.6], there exist eigenvectors η_α and η_β of φ in $E(\alpha)\otimes_E \mathbb{D}_{\mathrm{cris}}(V_f)$ with eigenvalues α and β respectively such that $[\eta_\alpha, \bar{\nu}_1] = [\eta_\beta, \bar{\nu}_1] = 1$ and we have

$$\begin{aligned} \left\langle \Omega_{V_f(1),1}((1+\pi)\otimes\eta_\alpha), \mathbf{z}^{\mathrm{Kato}} \right\rangle_{V_f(1)} &= \tilde{L}_{p,\alpha}, \\ \left\langle \Omega_{V_f(1),1}((1+\pi)\otimes\eta_\beta), \mathbf{z}^{\mathrm{Kato}} \right\rangle_{V_f(1)} &= \tilde{L}_{p,\beta}. \end{aligned}$$

It can be verified that

$$\begin{aligned} \eta_\alpha &= \alpha^{-1}\nu_1 - \nu_2, \\ \eta_\beta &= \beta^{-1}\nu_1 - \nu_2. \end{aligned}$$

Therefore, by Definition 3.17 and Proposition 3.22, we have

$$\begin{aligned} \mathfrak{M}(\tilde{L}_{p,\alpha}) &= (\alpha^{-1}m_{12} + m_{11})L_{p,1} + (\alpha^{-1}m_{22} + m_{21})L_{p,2}, \\ \mathfrak{M}(\tilde{L}_{p,\beta}) &= (\beta^{-1}m_{12} + m_{11})L_{p,1} + (\beta^{-1}m_{22} + m_{21})L_{p,2}; \end{aligned}$$

in the notation of Section 1.2, we have

$$\mathcal{M} = \begin{pmatrix} \alpha^{-1}m_{12} + m_{11} & \alpha^{-1}m_{22} + m_{21} \\ \beta^{-1}m_{12} + m_{11} & \beta^{-1}m_{22} + m_{21} \end{pmatrix}.$$

The functions $L_{p,1}$ and $L_{p,2}$ can therefore be written as

$$L_{p,1} = \frac{(\beta^{-1}m_{22} + m_{21})\mathfrak{M}(\tilde{L}_{p,\alpha}) - (\alpha^{-1}m_{22} + m_{21})\mathfrak{M}(\tilde{L}_{p,\beta})}{(\beta^{-1} - \alpha^{-1})\det(M)} \tag{30}$$

$$L_{p,2} = \frac{(\beta^{-1}m_{12} + m_{11})\mathfrak{M}(\tilde{L}_{p,\alpha}) - (\alpha^{-1}m_{12} + m_{11})\mathfrak{M}(\tilde{L}_{p,\beta})}{(\alpha^{-1} - \beta^{-1})\det(M)} \tag{31}$$

Let $x \in \mathbb{D}(V_{\bar{f}}(k-1))^{\psi=1}$. On the one hand,

$$(1-\varphi)x = \underline{\mathrm{Col}}_1(x)\cdot[(1+\pi)\varphi(\pi^{1-k}n_1 \otimes e_{k-1})] + \underline{\mathrm{Col}}_2(x)\cdot[(1+\pi)\varphi(\pi^{1-k}n_2 \otimes e_{k-1})].$$

On the other hand, Proposition 3.22 says that

$$(1-\varphi)x = \mathfrak{M}\circ\mathcal{L}_{1,\nu_1\otimes(1+\pi)}(x)\bar{\nu}_2 \otimes t^{1-k}e_{k-1} - \mathfrak{M}\circ\mathcal{L}_{1,\nu_2\otimes(1+\pi)}(x)\bar{\nu}_1 \otimes t^{1-k}e_{k-1}.$$

Therefore, we have

$$\begin{pmatrix} \underline{\mathrm{Col}}_1(x) & \underline{\mathrm{Col}}_2(x) \end{pmatrix}\cdot[(1+\pi)M] = \begin{pmatrix} -\mathfrak{M}\circ\mathcal{L}_{1,\nu_2\otimes(1+\pi)}(x) & \mathfrak{M}\circ\mathcal{L}_{1,\nu_1\otimes(1+\pi)}(x) \end{pmatrix}.$$

Let $\underline{M} = (\underline{m}_{ij}) = \mathfrak{M}^{-1}[(1+\pi)M]$, then as elements of $\mathcal{H}(G_\infty)$

$$\begin{pmatrix} \underline{\mathrm{Col}}_1(x) & \underline{\mathrm{Col}}_2(x) \end{pmatrix}\underline{M} = \begin{pmatrix} -\mathcal{L}_{1,\nu_2\otimes(1+\pi)}(x) & \mathcal{L}_{1,\nu_1\otimes(1+\pi)}(x) \end{pmatrix}. \tag{32}$$

Therefore, by exactly the same calculation as above, we have the following theorem:

Theorem 3.25. *Define*

$$\underline{\mathcal{M}} = \begin{pmatrix} \alpha^{-1}\underline{m}_{12} + \underline{m}_{11} & \alpha^{-1}\underline{m}_{22} + \underline{m}_{21} \\ \beta^{-1}\underline{m}_{12} + \underline{m}_{11} & \beta^{-1}\underline{m}_{22} + \underline{m}_{21} \end{pmatrix}.$$

Then we have the decomposition

$$\begin{pmatrix} \tilde{L}_{p,\alpha} \\ \tilde{L}_{p,\beta} \end{pmatrix} = \underline{\mathcal{M}}\begin{pmatrix} \tilde{L}_{p,1} \\ \tilde{L}_{p,2} \end{pmatrix} \tag{33}$$

Again, in the notation of Section 1.2, we have

$$\underline{\mathcal{M}} = \begin{pmatrix} \alpha^{-1}\underline{m}_{12} + \underline{m}_{11} & \alpha^{-1}\underline{m}_{22} + \underline{m}_{21} \\ \beta^{-1}\underline{m}_{12} + \underline{m}_{11} & \beta^{-1}\underline{m}_{22} + \underline{m}_{21} \end{pmatrix}.$$

3.5.2. *Interpolating properties.* We calculate the values of our new p-adic L-functions at characters modulo p. We first state a lemma concerning such characters.

Lemma 3.26. *If $A \in (\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}$ is divisible by $\varphi(\pi)$, then $\mathfrak{M}^{-1}(A)$ is zero when evaluated at any character with conductor p.*

Proof. This is a special case of Theorem 5.4 as proved below. □

Notation 3.27. *For any element $x \in \mathbb{C}_p \otimes (\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}$ and η a character on G_∞, we write $\eta(x)$ for $\eta(\mathfrak{M}^{-1}(x))$.*

Proposition 3.28. *Let η be a primitive character modulo p, then*

$$\begin{aligned} \eta(L_{p,1}) &= \frac{\tau(\eta)}{p^{k-1}} \cdot \frac{L(f_{\eta^{-1}}, 1)}{\Omega_f^{\eta(-1)}}, \\ \eta(L_{p,2}) &= 0. \end{aligned}$$

Similarly, if η is the trivial character, then

$$\begin{aligned} \eta(L_{p,1}) &= \frac{a_p - p^{k-2} - 1}{p^{k-1}} \cdot \frac{L(f,1)}{\Omega_f^+}, \\ \eta(L_{p,2}) &= \left(\frac{1}{p} - 1\right) \cdot \frac{L(f,1)}{\Omega_f^+}. \end{aligned}$$

Proof. Since

$$M = (t/\pi q)^{k-1} P^T M'^{-1} = (t/\pi q)^{k-1} \varphi(M'^{-1}) A_\varphi^T$$

and $M'|_{\pi=0} = I$, we have $M|_{\pi=(\zeta-1)} = A_\varphi^T$ for any p-th root of unity ζ. In other words, we have $M \equiv A_\varphi^T \mod \varphi(\pi)$. Therefore, (30) and (31) imply that,

$$L_{p,1} \equiv \frac{(\beta^{-1}a_p - 1)\mathfrak{M}(\tilde{L}_{p,\alpha}) - (\alpha^{-1}a_p - 1)\mathfrak{M}(\tilde{L}_{p,\beta})}{(\beta^{-1} - \alpha^{-1})p^{k-1}} \mod \varphi(\pi) \tag{34}$$

$$L_{p,2} \equiv \frac{\beta^{-1}\mathfrak{M}(\tilde{L}_{p,\alpha}) - \alpha^{-1}\mathfrak{M}(\tilde{L}_{p,\beta})}{(\alpha^{-1} - \beta^{-1})} \mod \varphi(\pi) \tag{35}$$

Therefore, we are done by Lemma 3.26 and the values of $\eta(\tilde{L}_{p,\alpha})$ and $\eta(\tilde{L}_{p,\beta})$ given in [MTT86] for example. □

Corollary 3.29. *If $k \geq 3$, then $L_{p,i} \neq 0$ for $i \in \{1,2\}$. Moreover, if η is a character of Δ, then $L^\eta_{p,1} \neq 0$.*

Proof. Since $k \geq 3$, the result follows from the fact that $L(f_{\eta^{-1}}, 1) \neq 0$ (by [Shi76, Proposition 2]). □

Remark 3.30. *If $k = 2$ and $a_p = 0$, we will show that under the Mellin transform, $L_{p,1}$ and $L_{p,2}$ agree with Pollack's plus and minus p-adic L-functions up to a unit. Therefore, by* [Pol03, Corollary 5.11], *it is in fact enough to assume that assumption (A) holds in order for Corollary 3.29 to hold.*

Remark 3.31. *We see that the interpolating properties of $L_{p,1}$ and $L_{p,2}$ at a character modulo p are independent of the choice of n_1, n_2 as long as we have fixed a pair of 'good bases' for $\mathbb{D}_{\mathrm{cris}}(V_f)$ and $\mathbb{D}_{\mathrm{cris}}(V_{\bar{f}})$.*

Lemma 3.32. *If $z \in \Lambda_E(G_\infty)$ and $f \in (E \otimes \mathbb{B}_{\mathbb{Q}_p})^{\psi=0}$, then $z \cdot (f n_i) \equiv (z \cdot f) n_i \mod \varphi(\pi)$ for $i = 1, 2$.*

Proof. It follows from the fact that if $g \in G_\infty$, $g(\varphi\mathbb{N}(V)) \subset \varphi(\pi)\mathbb{N}(V)$ for any V. □

Corollary 3.33. *Proposition 3.28 (and hence Corollary 3.29) still hold after replacing $L_{p,i}$ by $\tilde{L}_{p,i}$ for $i = 1, 2$.*

Proof. By definitions, we have

$$(1-\varphi)(\mathbf{z}^{\mathrm{Kato}}) = \begin{pmatrix} L_{p,1} & L_{p,2} \end{pmatrix} M \begin{pmatrix} \bar{\nu}_1 \\ \bar{\nu}_2 \end{pmatrix} \otimes t^{1-k} e_{k-1} = \begin{pmatrix} \tilde{L}_{p,1} & \tilde{L}_{p,2} \end{pmatrix} \cdot \begin{pmatrix} (1+\pi)n_1 \\ (1+\pi)n_2 \end{pmatrix}$$

where $\mathbf{z}^{\mathrm{Kato}}$ is the localization of the Kato zeta element and M is as defined in (20). This implies

$$\begin{pmatrix} L_{p,1} & L_{p,2} \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{pmatrix} \tilde{L}_{p,1} & \tilde{L}_{p,2} \end{pmatrix} \cdot \begin{pmatrix} (1+\pi)n_1 \\ (1+\pi)n_2 \end{pmatrix}.$$

Therefore, by Lemma 3.32, we have $L_{p,i} \equiv \mathfrak{M}(\tilde{L}_{p,i}) \mod \varphi(\pi)$ and hence $\mathfrak{M}^{-1}(L_{p,i})$ agrees with $\tilde{L}_{p,i}$ at a character modulo p by Lemma 3.26. □

3.5.3. *Infinitude of zeros.* Let η be a character of Δ. Mazur proved that at least one of $\tilde{L}_{p,\alpha}$ and $\tilde{L}_{p,\beta}$ has infinitely many zeros if $v_p(\alpha) \neq v_p(\beta)$. This has been generalized to the case $a_p = 0$ ([Pol03, Theorem 3.5]). We show that our decomposition of $\tilde{L}_{p,\alpha}$ and $\tilde{L}_{p,\beta}$ can be used to give an alternative proof to Mazur's result as well as generalize Pollack's result to the case $a_p \neq 0$.

Proposition 3.34. *If f is a modular form as given in the beginning of Section 3.3 and η a character of Δ, then either $\tilde{L}^{\eta}_{p,\alpha}$ or $\tilde{L}^{\eta}_{p,\beta}$ has infinitely many zeros.*

Proof. Assume not, then [Pol03, Lemma 3.2] implies that $\tilde{L}^{\eta}_{p,\alpha}$ and $\tilde{L}^{\eta}_{p,\beta}$ are $O(1)$.

By [BB10, Lemmas 3.3.5 and 3.3.6], the entries of M are $O(\log_p^m)$ where $m = \max\{v_p(\alpha), v_p(\beta)\} < k-1$. Therefore, with the notation above, $m_{ij} = O(\log_p^m)$ for $i,j \in \{1,2\}$. In particular, the η-component of

$$(\beta^{-1}m_{22} + m_{21})\tilde{L}_{p,\alpha} - (\alpha^{-1}m_{22} + m_{21})\tilde{L}_{p,\beta}$$

is $O(\log_p)^m$. By (30), the quantity above is divisible by $(t/\pi q)^{k-1} \sim \log_p^{k-1}$ which forces $L^{\eta}_{p,1} = 0$ contradicting Corollary 3.28. □

As with [Pol03, Theorem 3.5], we have:

Corollary 3.35. *If $\alpha \notin E(\eta)$, then both $\tilde{L}^{\eta}_{p,\alpha}$ and $\tilde{L}^{\eta}_{p,\beta}$ have infinitely many zeros.*

3.6. **Good ordinary modular forms.** We now assume that f is good ordinary at p. We will pick different bases from the supersingular case to define our Coleman maps. Let α be the root of $X^2 - a_p X + p^{k-1}$ which is a p-adic unit and β is the one with p-adic valuation $k-1$. By a result of Deligne and Mazur-Wiles (see for example [Kat04, Section 17] for an exposition), there exists a 1-dimensional $G_{\mathbb{Q}_p}$-subrepresentation $V'_{\bar{f}}$ in $V_{\bar{f}}$. Moreover, $V'_{\bar{f}}$ has Hodge-Tate weight 0 and $\mathbb{D}_{\mathrm{cris}}(V'_{\bar{f}})$ can be identified with the α-eigenspace of φ in $\mathbb{D}_{\mathrm{cris}}(V_{\bar{f}})$. We fix a nonzero element $\bar{\nu}_1 \in \mathbb{D}_{\mathrm{cris}}(V'_{\bar{f}})$. Then, by (7), $n_1 = \bar{\nu}_1$ is a basis of $\mathbb{N}(V'_{\bar{f}})$ over $E \otimes \mathbb{B}^+_{\mathbb{Q}_p}$. Let $\bar{\nu}_2$ be a nonzero β-eigenvector of φ in $\mathbb{D}_{\mathrm{cris}}(V_{\bar{f}})$.

Proposition 3.36. *We may find $n_2 \in \mathbb{N}(V_{\bar{f}})$ lifting $\bar{\nu}_2$ such that n_1, n_2 is an $E \otimes \mathbb{B}^+_{\mathbb{Q}_p}$-basis of $\mathbb{N}(V_{\bar{f}})$, and $(1+\pi)\varphi(\pi^{1-k}n_1 \otimes e_{k-1}), (1+\pi)\varphi(\pi^{1-k}n_2 \otimes e_{k-1})$ is a $\Lambda_E(G_\infty)$-basis of $(\varphi^*\mathbb{N}(V_{\bar{f}}(k-1)))^{\psi=0}$.*

Proof. Let $N = \mathbb{N}(V_{\bar{f}})$ and $N' = \mathbb{N}(V'_{\bar{f}})$. Then the quotient $N'' = N/N'$ may be identified with the Wach module of the quotient $V_{\bar{f}}/V'_{\bar{f}}$, and we have an exact sequence

$$0 \longrightarrow (\varphi^* N'(k-1))^{\psi=0} \longrightarrow (\varphi^* N(k-1))^{\psi=0} \longrightarrow (\varphi^* N''(k-1))^{\psi=0} \longrightarrow 0.$$

It is clear that $(1+\pi)\varphi(n_1 \otimes \pi^{1-k}e_{k-1})$ is a basis of $(\varphi^* N'(k-1))^{\psi=0}$, and the result now follows on applying theorem 3.5 to N''. □

Hence the change of basis matrix M', with

$$\begin{pmatrix} \bar{\nu}_1 \\ \bar{\nu}_2 \end{pmatrix} = M' \begin{pmatrix} n_1 \\ n_2 \end{pmatrix},$$

is lower triangular, with $1, (t/\pi)^{k-1}$ on the diagonal. With respect to this basis, the Coleman maps given in Section 3.1 enable us to define:

Definition 3.37. *For $i = 1, 2$, define $L_{p,i} \in (E \otimes \mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$ to be the image of the localization of the Kato zeta element (on using the identification as given by (4)) under* Col_i. *Similarly, define $\tilde{L}_{p,i}$ to be the image of the localization of the Kato zeta element under* $\underline{\mathrm{Col}}_i$.

Since $\varphi(n_1) = \alpha n_1$, the matrix P as defined in Section 3.1 is upper triangular and there exists a unit u in $E \otimes \mathbb{B}^+_{\mathbb{Q}_p}$ such that

$$P = \begin{pmatrix} \alpha & * \\ 0 & uq^{k-1} \end{pmatrix}.$$

Therefore, (10) becomes

$$(1-\varphi)(x) = \begin{pmatrix} \mathrm{Col}_1(x) & \mathrm{Col}_2(x) \end{pmatrix} \begin{pmatrix} \alpha(\frac{t}{\pi q})^{k-1} & 0 \\ * & u \end{pmatrix} \begin{pmatrix} \bar{\nu}_1 \\ \bar{\nu}_2 \end{pmatrix} \otimes t^{1-k} e_{k-1}. \tag{36}$$

Lemma 3.38. *Let ν_1, ν_2 be a basis of $\mathbb{D}_{\mathrm{cris}}(V_f)$ such that $\varphi(\nu_1) = \alpha\nu_1$ and $\varphi(\nu_2) = \beta\nu_2$. Then*

$$[\nu_i \otimes t^{-1} e_1, \bar{\nu}_i \otimes t^{1-k} e_{k-1}] = 0$$

for $i = 1, 2$ where $[\ ,\ ]$ is the pairing defined in (19).

Proof. Assume $m_1 := [\nu_1 \otimes t^{-1} e_1, \bar{\nu}_1 \otimes t^{1-k} e_{k-1}] \neq 0$. Since $[\ ,\ ]$ is compatible with φ, we have

$$\begin{aligned} \varphi[\nu_1 \otimes t^{-1} e_1, \bar{\nu}_1 \otimes t^{1-k} e_{k-1}] &= [\varphi(\nu_1 \otimes t^{-1} e_1), \varphi(\bar{\nu}_1 \otimes t^{1-k} e_{k-1})] \\ p^{-1} m_1 &= [\alpha p^{-1} \nu_1 \otimes t^{-1} e_1, \alpha p^{1-k} \bar{\nu}_1 \otimes t^{1-k} e_{k-1}] \\ p^{k-1} m_1 &= \alpha^2 m_1. \end{aligned}$$

Hence, $\alpha^2 = p^{k-1}$, which is a contradiction. The proof for $i = 2$ is similar. □

As in Section 3.4, we may assume that $[\nu_1, \bar{\nu}_2] = -[\nu_2, \bar{\nu}_1] = 1$ and an analogue of Proposition 3.22 says that

$$\mathfrak{M}\begin{pmatrix} -\mathcal{L}_{\nu_2 \otimes (1+\pi)} \circ h^1_{\mathrm{Iw}} & \mathcal{L}_{\nu_1 \otimes (1+\pi)} \circ h^1_{\mathrm{Iw}} \end{pmatrix} = \begin{pmatrix} \mathrm{Col}_1 & \mathrm{Col}_2 \end{pmatrix} \begin{pmatrix} \alpha(\frac{t}{\pi q})^{k-1} & 0 \\ * & u \end{pmatrix}.$$

In particular, if we apply this to the Kato zeta element, we have

$$\begin{pmatrix} -\mathfrak{M}(\tilde{L}_{p,\beta}) & \mathfrak{M}(\tilde{L}_{p,\alpha}) \end{pmatrix} = \begin{pmatrix} L_{p,1} & L_{p,2} \end{pmatrix} \begin{pmatrix} \alpha(\frac{t}{\pi q})^{k-1} & 0 \\ * & u \end{pmatrix}$$

where $\tilde{L}_{p,\beta} = \mathcal{L}_{\nu_2}(\mathbf{z}^{\mathrm{Kato}})$. Similarly, we have

$$\begin{pmatrix} -\tilde{L}_{p,\beta} & \tilde{L}_{p,\alpha} \end{pmatrix} = \begin{pmatrix} \tilde{L}_{p,1} & \tilde{L}_{p,2} \end{pmatrix} \begin{pmatrix} \alpha \log_{p,k} & 0 \\ * & \tilde{u} \end{pmatrix} \tag{37}$$

where $\log_{p,k} = \prod_{j=0}^{k-2} \log_p(\chi(\gamma)^{-j}\gamma)/(\chi(\gamma)^{-j}\gamma - 1)$ and $\tilde{u} \in \Lambda_E(G_\infty)^\times$.

Therefore, as in Section 3.4, we can decompose $\tilde{L}_{p,\beta}$ into a linear combination of $\tilde{L}_{p,1}$ and $\tilde{L}_{p,2}$, whereas $\tilde{L}_{p,\alpha} = \tilde{L}_{p,2}$, up to a unit. We now say something about $\tilde{L}_{p,1}$. When V_f is not locally split at p, $\tilde{L}_{p,\beta}$ is conjecturally equal to the critical slope p-adic L-function constructed in [PoS09]. We itemize this condition since we will need it again later.

- **Assumption (A'):** V_f is not locally split at p and $k \geq 3$.

In this case, [Kat04, Theorem 16.4 and 16.6] imply that $\tilde{L}_{p,\beta}$ has the same interpolating properties as $\tilde{L}_{p,\alpha}$, namely:

$$\chi^r\eta(\tilde{L}_{p,\alpha}) = \frac{c_{\eta,r}}{\beta^n} L(f_{\eta^{-1}}, r+1) \qquad \text{and} \qquad \chi^r\eta(\tilde{L}_{p,\beta}) = \frac{c_{\eta,r}}{\beta^n} L(f_{\eta^{-1}}, r+1) \tag{38}$$

where η is a finite character of conduction $p^n > 1$, $0 \leq r \leq k-2$ and $c_{\eta,r}$ is some constant independent of α and β. Note that the values given by (38) do not determine $\tilde{L}_{p,\beta}$ uniquely. However, they allow us to show that $\tilde{L}_{p,1}, L_{p,1} \neq 0$.

Proposition 3.39. *If assumption (A') holds, then $\tilde{L}^\eta_{p,1}, L^\eta_{p,1} \neq 0$ for any character η on Δ.*

Proof. As in the proof of Proposition 3.28, $M'|_{\pi=0}$ implies that $M|_{\pi=(\zeta-1)} = A_\varphi^T$ for any $\zeta^p = 1$, where $A_\varphi = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ is the matrix of φ with respect to $\bar\nu_1$, $\bar\nu_2$. Therefore, $\mathfrak{M}(\tilde L_{p,\beta})(\zeta-1) = \alpha L_{p,1}(\zeta-1)$. Since V_f is not locally split and $k \geq 3$, by the above discussion, $\eta(\tilde L_{p,\beta}) = \frac{\tau(\eta)}{\beta} L(f_{\eta^{-1}}, 1) \neq 0$ as in the supersingular case. Therefore, $L_{p,1}(\zeta-1) \neq 0$. The statement about $\tilde L_{p,1}$ then follows as in Corollary 3.33. □

We see from the proof that the interpolating properties of $\mathfrak{M}^{-1}(L_{p,1})$ and $\tilde L_{p,1}$ at characters modulo p are the same as that of $\tilde L_{p,\beta}$ after multiplying a constant.

Remark 3.40. *If V_f does split locally at p, we can choose $n_2 = \bar\nu_2$ and both P and M' would be diagonal. Therefore, we have $\tilde L_{p,\beta} = \mathfrak{M}^{-1}((t/\pi q)^{k-1} L_{p,1}) = \log_{p,k} \tilde L_{p,1}$. But it is not known that whether $\tilde L_{p,\beta}$ is nonzero or not.*

4. Coleman maps for the Berger–Li–Zhu basis

In this section, we will prove some results on the images of the Coleman maps under the assumption that $v_p(a_p) > \lfloor \frac{k-2}{p-1} \rfloor$, using the explicit basis of $\mathbb{N}(V_{\bar f})$ written down in [BLZ04]. We shall also give an explicit proof that this particular basis satisfies the conclusions of theorem 3.15.

Write $m = \lfloor (k-2)/(p-1) \rfloor$ and define

$$\log^+(1+\pi) = \prod_{n\geq 0} \frac{\varphi^{2n+1}(q)}{p} = \prod_{\substack{n\geq 1 \\ n \text{ even}}} \frac{\Phi_n(1+\pi)}{p}$$

and

$$\text{and} \qquad \log^-(1+\pi) = \prod_{n\geq 0} \frac{\varphi^{2n}(q)}{p} = \prod_{\substack{n\geq 1 \\ n \text{ odd}}} \frac{\Phi_n(1+\pi)}{p}.$$

where $\Phi_n(X)$ is the p^n-th cyclotomic polynomial. Let z_i be elements of $\mathbb{Q}_p$ such that

$$p^m \left(\frac{\log^-(1+\pi)}{\log^+(1+\pi)} \right)^{k-1} = \sum_{i\geq 0} z_i \pi^i,$$

then as shown in [BLZ04, Proposition 3.1.1],

$$z = \sum_{i=0}^{k-2} z_i \pi^i \in \mathbb{Z}_p[[\pi]].$$

By [BLZ04], under assumption (C), i.e. $v_p(a_p) > m$, there is a lattice $T_{\bar f}$ in $V_{\bar f}$ and a basis of $\mathbb{N}(T_{\bar f})$ such that the matrix of φ with respect to this basis, P, is given by

$$\begin{pmatrix} 0 & -1 \\ q^{k-1} & \delta z \end{pmatrix}$$

where $\delta = a_p/p^m$. In particular, the reduction of this basis modulo π is a "good basis" in the sense of §3.3, and hence the Coleman maps may be defined integrally as in remark 3.16. By construction, for any $x \in \mathbb{D}(T_{\bar f}(k-1))^{\psi=1}$ with

$$x = \pi^{1-k} \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1},$$

we can express $\mathrm{Col}_i(x)$, $i = 1, 2$, in terms of x_1 and x_2:

$$\mathrm{Col}_1(x) = x_2 - \varphi(x_1) + \delta z x_1, \tag{39}$$

$$\mathrm{Col}_2(x) = -q^{k-1} x_1 - \varphi(x_2). \tag{40}$$

Remark 4.1. *The representation constructed in [BLZ04] is really $V_{\bar f}$ twisted by an unramified character. But since we assume that $\epsilon(p) = 1$, it does not affect the action of P and our calculations later on.*

4.1. **The image of Col_1.** We first give a few preliminary lemmas.

Lemma 4.2. *For all $n \geq 0$, we have $\varphi^n(M'^{-1})(A_\varphi^T)^n = \varphi^{n-1}(P^T)\cdots\varphi(P^T)P^T M'^{-1}$. Moreover, as $n \to \infty$, the quantity above tends to 0.*

Proof. The equality follows from (9) and induction. For the limit, note that $M'|_{\pi=0} = I$, hence $\varphi^n(M') \to I$ as $n \to \infty$. The eigenvalues of A_φ are α and β. But α^n, $\beta^n \to 0$ as $n \to \infty$, so we are done. $\square$

Lemma 4.3. *Let $x = \pi^{1-k}\begin{pmatrix} x_1 & x_2 \end{pmatrix}\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1}$. Then, $\psi(x)$ is given by*

$$\begin{pmatrix} \psi(x_1\delta z + x_2) & -\psi(q^{k-1}x_1) \end{pmatrix} \pi^{1-k}\begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$$

Proof. Recall that $\varphi(\pi) = \pi q$, we have

$$\begin{aligned} x &= \pi^{1-k}\begin{pmatrix} x_1 & x_2 \end{pmatrix}(P^T)^{-1}\begin{pmatrix} \varphi(n_1) \\ \varphi(n_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1\delta z + x_2 & -q^{k-1}x_1 \end{pmatrix}\varphi(\pi)^{1-k}\begin{pmatrix} \varphi(n_1) \\ \varphi(n_2) \end{pmatrix}, \end{aligned}$$

hence the result $\square$

Lemma 4.4. *For all $n \geq 1$, the constant term of $\psi(q^n)$ is p^{n-1}.*

Proof. Induction. $\square$

Lemma 4.5. *If $f(\pi) \in E \otimes \mathbb{B}^+_{\mathbb{Q}_p}$, then there exist unique $a_i \in E$ for $1 \leq i \leq k-1$ such that $f(\pi) = \sum_{i=1}^{k-1} a_i(\pi+1)^i \mod \pi^{k-1}$.*

Proof. Note that

$$(\pi+1)^k = \binom{k}{1}(\pi+1)^{k-1} - \cdots + (-1)^{k-2}\binom{k}{k-1}(\pi+1) + (-1)^{k-1} \mod \pi^k. \tag{41}$$

Suppose now that there exist $a_1, \ldots, a_{k-1} \in E$ such that $(\pi+1)^k = \sum_{i=1}^{k-1} a_i(\pi+1)^i \mod \pi^k$. Subtracting this sum from (41) shows that

$$\left(\binom{k}{1} - a_{k-1}\right)(\pi+1)^{k-1} + \cdots + \left((-1)^{k-2}\binom{k}{k-1} - a_1\right)(\pi+1) + (-1)^{k-1} = 0.$$

But this gives a contradiction since $\{(\pi+1)^i\}_{0\leq i<k}$ is a basis of the vector space of polynomials of degree $\leq k-1$. $\square$

Proposition 4.6. *Under assumption (C), the map $(\pi^{k-1}\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0} \subset \mathrm{Col}_1\left(\mathbb{D}(T_{\bar{f}}(k-1))^{\psi=1}\right)$.*

Proof. Recall that (6) says

$$(1-\varphi)x = \begin{pmatrix} y_1 & y_2 \end{pmatrix} \cdot (\pi q)^{1-k} P^T \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1}.$$

For any $y_1 \in (\pi^{k-1}\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$, we have

$$y := \begin{pmatrix} y_1 & 0 \end{pmatrix} \cdot (\pi q)^{1-k} P^T \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1} = \begin{pmatrix} 0 & y_1/\pi^{k-1} \end{pmatrix}\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1}.$$

Then,

$$\begin{aligned} \varphi^n(y) &= \begin{pmatrix} 0 & \varphi^n(y_1/\pi^{k-1}) \end{pmatrix}\varphi^{n-1}(P^T)\cdots\varphi(P^T)P^T\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1} \\ &= \begin{pmatrix} 0 & \varphi^n(y_1/\pi^{k-1}) \end{pmatrix}\varphi^n(M'^{-1})(A_\varphi^T)^n M'\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1}. \end{aligned}$$

Hence, Lemma 4.2 implies that $\varphi^n(y) \to 0$ as $n \to \infty$ and the series $x := \sum_{n\geq 0}\varphi^n(y)$ converges to an element of $\mathbb{D}(T_{\bar{f}}(k-1))^{\psi=1}$ with $(1-\varphi)x = y$. Therefore, $y_1 = \mathrm{Col}_1(x)$. $\square$

Proposition 4.7. *Under assumptions (B), (C) and (D), the map* $\mathrm{Col}_1 : \mathbb{D}(V_{\bar{f}}(k-1)) \to (E \otimes \mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$ *is surjective.*

Proof. By Proposition 4.6, if $y_1 \in (\pi^{k-1} E \otimes \mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$, then $y_1 \in \mathrm{Im}(\mathrm{Col}_1)$. For an arbitrary $y_1 \in (E \otimes \mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$, by Lemma 4.5 there exists y' in the E-linear span of $\{(1+\pi)^i\}_{1\le i<k}$ such that $y_1 + \varphi(y')$ is divisible by π^{k-1}. Hence, by the same argument as above, the sum

$$\sum_{n\ge 0} \varphi^n \left(\begin{pmatrix} 0 & (y_1+\varphi(y'))/\pi^{k-1} \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \right)$$

converges to an element $x \in \mathbb{N}(V_{\bar{f}}(k-1))$. By Lemma 4.3 and the fact that $\psi(y_1) = 0$, we have

$$\begin{aligned} \psi(x) - x &= \psi\left(\begin{pmatrix} 0 & (y_1+\varphi(y'))/\pi^{k-1} \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \right) \\ &= \pi^{1-k} \begin{pmatrix} y' & 0 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \end{aligned}$$

Let $x' = x + \pi^{1-k} \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$. Then

$$\psi(x') - x' = \pi^{1-k} \begin{pmatrix} y' - x_1 + \psi(x_1\delta z + x_2) & -x_2 - \psi(q^{k-1}x_1) \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}.$$

Hence, $x' \in \mathbb{D}(V_{\bar{f}}(k-1))^{\psi=1}$ if and only if

$$\begin{aligned} x_2 &= -\psi(q^{k-1}x_1) \\ y' &= x_1 - \psi(x_1\delta z) + \psi^2(q^{k-1}x_1) \end{aligned} \tag{42}$$

Assume that such x_1 exists in the E-linear span of $\{(1+\pi)^i\}_{1\le i<k}$, and let a be its degree in π. Since the degrees of δz and q^{k-1} are at most $k-2$ and $(p-1)(k-1)$ respectively, the degrees of $\psi(x_1\delta z)$ and $\psi^2(q^{k-1}x_1)$ are at most $(k-2+a)/p$ and $((p-1)(k-1)+a)/p^2$ respectively. But we assume that $p \ge k-1$, so the right-hand side of (42) has degree $\le a$. Since y' has degree at most $k-1$ and x_1 is in the E-linear span of $\{(1+\pi)^i\}_{1\le i<k}$, both $\psi(x_1\delta z)$ and $\psi^2(q^{k-1}x_1)$ are scalar multiples of $(1+\pi)$. We write

$$y' = \sum_{i=1}^{k-1} \alpha_i (1+\pi)^i, \qquad x_1 = \sum_{i=1}^{k-1} \beta_i (1+\pi)^i \qquad \text{and} \qquad \delta z = \sum_{i=0}^{k-2} \gamma_i (1+\pi)^i$$

where α_i, β_i, $\gamma_i \in E$. Then (42) says that

$$\begin{aligned} \alpha_i &= \beta_i \qquad \text{for } i \ge 2 \\ \alpha_1 &= \beta_1 - \sum_{i+j=p} \beta_i\gamma_j + \beta_{p^2-(k-1)(p-1)} \end{aligned}$$

where $\gamma_i = \beta_i = 0$ if $i < 0$. But $p^2 - (k-1)(p-1) > 1$ and $\gamma_{p-1} = 0$, the matrix relating $(\alpha_i)_{1\le i\le k-1}$ and $(\beta_i)_{1\le i\le k-1}$ is upper triangular with non-zero entries on the diagonal. Therefore, there is a bijection between $(\alpha_i)_{1\le i\le k-1} \in E^{k-1}$ and $(\beta_i)_{1\le i\le k-1} \in E^{k-1}$. In other words, given any y' as above, there exists a unique x_1 (and hence x_2) such that $x' \in \mathbb{D}(V_{\bar{f}}(k-1))^{\psi=1}$. For any $0 \le j \le k-2$, we can therefore choose y (and hence y') such that $x_1 \equiv \pi^j \mod \pi^{j+1}$. In this case,

$$\begin{aligned} \mathrm{Col}_1(x') &= y_1 + \varphi(y') - \psi(q^{k-1}x_1) - \varphi(x_1) + x_1\delta z \\ &\equiv -\psi(q^{k-1}x_1) - \varphi(x_1) + x_1\delta z \mod \pi^{k-1} \\ &\equiv (-p^{k-2-j} - p^j + a_p)\pi^j \mod \pi^{j+1}, \end{aligned}$$

where we deduce the last line from the previous one using Lemma 4.4 and the observation that $\pi q = \varphi(\pi)$. Therefore, our assumption on a_p implies that for all $y_1 \in (E \otimes \mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$, there exists some $x \in \mathbb{D}(V_{\bar{f}}(k-1))^{\psi=1}$ such that $\mathrm{Col}^+(x) \equiv y_1 \mod \pi^{j+1}$ by induction. Hence we are done. □

Corollary 4.8. *Under assumptions (B), (C) and (D), the image of* $\mathrm{Col}_1 : \mathbb{D}(T_{\bar{f}}(k-1))^{\psi=1} \to (\mathcal{O}_E \otimes \mathbb{A}_{\mathbb{Q}_p}^+)^{\psi=0}$ *is pseudo isomorphic to* $(\mathcal{O}_E \otimes \mathbb{A}_{\mathbb{Q}_p}^+)^{\psi=0}$.

Proof. It suffices to show that the said image has finite index in $(\mathcal{O}_E \otimes \mathbb{A}_{\mathbb{Q}_p}^+)^{\psi=0}$. The proof of Proposition 4.6 shows that $(\pi^{k-1}\mathcal{O}_E \otimes \mathbb{A}_{\mathbb{Q}_p}^+)^{\psi=0}$ lies in the image and for all $0 \le j \le k-2$, there exists $x_j \in \mathbb{D}(T_{\bar{f}}(k-1))^{\psi=1}$ such that $\mathrm{Col}_1(x_j) \equiv \alpha_j \pi^j \mod \pi^{j+1}$ for some $\alpha_j \neq 0$. Therefore, the quotient lies inside $\prod_{j=0}^{k-2} \mathcal{O}_E/\alpha_i \mathcal{O}_E$, so we are done. □

4.2. **The image of** Col_2**.** We now describe the image of Col_2. We will show that it is generated by two elements.

Lemma 4.9. *Let* $x = \pi^{1-k} \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1}$ *and* γ *a topological generator of* Γ*, then*

$$\gamma(x) = \pi^{1-k} \begin{pmatrix} \gamma(x_1) & \gamma(x_2) \end{pmatrix} G_\gamma \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1}$$

for some $G_\gamma \in I + \pi M(2, \mathbb{Z}_p[[\pi]])$.

Proof. By [BLZ04, Proposition 3.1.3], there exists $G_\gamma \in I + \pi M_2(\mathbb{Z}_p[[\pi]])$ such that $\begin{pmatrix} \gamma(n_1) \\ \gamma(n_2) \end{pmatrix} = G_\gamma^T \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$. Therefore,

$$\begin{aligned} \gamma(x) &= \gamma(\pi)^{1-k} \begin{pmatrix} \gamma(x_1) & \gamma(x_2) \end{pmatrix} G_\gamma^T \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes \chi(\gamma)^{k-1} e_{k-1} \\ &= \left(\frac{(1+\pi)^{\chi(\gamma)} - 1}{\chi(\gamma)} \right)^{1-k} \begin{pmatrix} \gamma(x_1) & \gamma(x_2) \end{pmatrix} G_\gamma^T \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1}. \end{aligned}$$

But $\chi(\gamma) \in 1 + p\mathbb{Z}_p$, which implies $((1+\pi)^{\chi(\gamma)} - 1)/\chi(\gamma) \in \pi(1 + p\mathbb{Z}_p[[\pi]])$. Hence the result. □

Lemma 4.10. *Let* $x = \pi^{1-k} \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1} \in \mathbb{D}(V_{\bar{f}}(k-1))^{\psi=1}$*. Write* $x_i = \sum_{j \ge 0} a_{i,j} \pi^j$*. Then* x_1 *has order* $< k-1$ *if and only if* x_2 *has order* $< k-1$*. If this is the case, they have the same order which we denote by* d_x*. Moreover,* $a_{2,d_x} = -p^{k-2-d_x} a_{1,d_x}$*.*

Proof. Since $x \in \mathbb{D}(V_{\bar{f}}(k-1))^{\psi=1}$, we have $x_2 = -\psi(q^{k-1}x_1)$, hence the result by Lemma 4.4. □

Proposition 4.11. *Under assumptions (C) and (D), the image of* $\mathrm{Col}_2 : \mathbb{D}(V_{\bar{f}}(k-1)) \to (E \otimes \mathbb{B}_{\mathbb{Q}_p}^+)^{\psi=0}$ *contains* $(\varphi(\pi)^{k-1} E \otimes \mathbb{B}_{\mathbb{Q}_p}^+)^{\psi=0}$ *and the quotient of the containment is a cyclic* $\Lambda_E(\Gamma)$*-module under the action of* Γ *described in Lemma 4.9.*

Proof. For any $y_2 \in (\varphi(\pi)^{k-1} E \otimes \mathbb{B}_{\mathbb{Q}_p}^+)^{\psi=0}$, we have

$$y := \begin{pmatrix} 0 & y_2 \end{pmatrix} \cdot (\pi q)^{1-k} P^T \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1} = \varphi(\pi)^{1-k} \begin{pmatrix} -y_2 & y_2 \delta z \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1}.$$

Hence, as in the proof of Proposition 4.6, $\sum_{n \ge 0} \varphi^n(y)$ converges which implies that y_2 lies in the image of Col_2.

Recall that if $x = \pi^{1-k} \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1}$, then $-\mathrm{Col}_2(x) = q^{k-1}x_1 + \psi(x_2)$. For $i = 1, 2$, write $x_i = \sum_{j \ge 0} a_{i,j} \pi^j$ and

$$\begin{aligned} \bar{\mathcal{C}}(x) &= q^{k-1}x_1 - \varphi(x_2) \mod \varphi(\pi)^{k-1} \\ &= (q^{k-1}a_{1,0} + a_{2,0}) + \varphi(\pi)(q^{k-2}a_{1,1} + a_{2,1}) + \cdots \varphi(\pi)^{k-2}(q a_{1,k-2} + a_{2,k-2}) \mod \varphi(\pi)^{k-1}. \end{aligned}$$

We now construct a generator f for $\bar{\mathcal{C}}(\mathbb{D}(V)^{\psi=1})$ over $\Lambda_E(\Gamma)$ inductively. By the proof of Proposition 4.6, there exists $x_i \in \mathbb{D}(V)^{\psi=1}$ of order i for all $0 \le i < k-1$. Let $f_0 = x_0$. For $i \ge 0$, suppose that we have constructed f_i. Write

$$\begin{aligned} f_i' &= \prod_{j=0}^{i} \left(\gamma - \chi(\gamma)^j\right)(f_i) \\ &= \pi^{1-k} \begin{pmatrix} f_{i,1}' & f_{i,2}' \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1} \end{aligned}$$

then it follows from Lemma 4.9 that f_i' is of order $\ge i+1$. Let $\alpha_{i+1,1}$ and $\alpha_{i+1,2}$ be the coefficients of π^{i+1} in the power series expansions of $f_{i,1}'$ and $f_{i,2}'$, respectively. There are two possibilities: either both $\alpha_{i+1,j}$ are non-zero, in which case we let $f_{i+1} = f_i$. Or both of them are zero, in which case we let $f_{i+1} = f_i + x_{i+1}$.

Let $f = f_{k-2}$. Then for all $0 \le i < k-1$, the order of $\prod_{j=0}^{i} \left(\gamma - \chi(\gamma)^j\right)(f)$ is i. To finish the proof, it is now sufficient to observe that by Lemma 4.10, for all $x \in \mathbb{D}(V_{\bar{f}}(k-1))^{\psi=1}$ there exist scalars $\alpha_i \in E$ for $0 \le i < k-1$ such that $x - \sum_{i=1}^{k-2} \alpha_i \prod_{j=1}^{i} (\gamma - \chi(\gamma)^j) f$ is of order $\ge k-1$. □

4.3. The Iwasawa transform.

Convention 4.12. *For the rest of this section as well as in Sections 4.4 and 4.5, we assume without loss of generality that $\chi(\gamma) = 1 + p$.*

Lemma 4.13.

$$\frac{q}{\gamma(q)} = 1 \mod (p\pi, \pi^{p-1}). \tag{43}$$

Proof. We have $q = \frac{\varphi(\pi)}{\pi}$, and $\gamma(1+\pi) = (1+\pi)(1+\varphi(\pi))$. Hence

$$\frac{q}{\gamma(q)} = \frac{1 + q + \varphi(\pi)}{1 + \varphi(q) + \varphi^2(\pi)}$$

It remains to notice that $q = \pi^{p-1} \mod p$. Moreover, the constant term of q (and hence of $\varphi(q)$) is p, and $\sum_{j=0}^{+\infty} (-p)^j$ is the multiplicative inverse of $1+p$, which implies the result. □

Corollary 4.14. *Both $\frac{\log^+}{\gamma(\log^+)}$ and $\frac{\log^-}{\gamma(\log^-)}$ are congruent to $1 \mod (p\pi, \pi^{p-1})$ (and hence in particular congruent to $1 \mod (p\pi, \pi^2)$ since we assume $p \ge 3$).*

Proof. Clear from Lemma 4.13 and the definition of $\log^\pm$. □

Define

$$G_\gamma^{(k-1)} = \begin{pmatrix} \left(\frac{\log^+}{\gamma(\log^+)}\right)^{k-1} & 0 \\ 0 & \left(\frac{\log^-}{\gamma(\log^-)}\right)^{k-1} \end{pmatrix}.$$

Lemma 4.15. $G_\gamma^{(k-1)} \simeq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod (p\pi, \pi^2)$.

Proof. Immediate from the definition and Corollary 4.14. □

Let ϖ_E be a uniformizer of E.

Proposition 4.16. $G_\gamma \simeq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod (\varpi_E \pi, \pi^2)$.

Proof. We first review the construction of G_γ as in [BLZ04, §3.1]. For $l \ge k$, we define recursively

$$G_\gamma^{(l)} = G_\gamma^{(l-1)} + \pi^{l-1} H^{(l)}$$

for some $H^{(l)} \in M(2, \mathbb{Z}_p[[X]])$ where $X = a_p/p^m$ and $m = \lfloor \frac{k-2}{p-1} \rfloor$. Note that $X \in \mathfrak{m}_E$ by assumption (C). The matrix G_γ is then given by the limit of $G_\gamma^{(l)}$ as $l \to \infty$. Therefore, when $k > 2$, the result is immediate from Lemma 4.15.

When $k = 2$, it suffices to show that $H^{(2)} \equiv 0 \mod \varpi_E$. By construction (see [BLZ04, Lemma 3.1.2 and Proposition 3.1.3]), $H^{(2)}$ satisfies the following:

$$H^{(2)} - P_0 H^{(2)} \left(pP_0\right)^{-1} = -R^{(1)} \mod \pi \tag{44}$$

for some matrix $R^{(1)} \in XM(2, \mathbb{Z}_p[[\pi, X]])$ and $P_0 = \begin{pmatrix} 0 & 1 \\ p & a_p \end{pmatrix}$. If we write $H = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix}$, then (44) says that

$$\begin{pmatrix} h_{11} & h_{12} + h_{21} \\ h_{21} & h_{22} \end{pmatrix} \equiv 0 \mod X,$$

and hence we are done since $\varpi_E | X$. □

Let $n_i' = \varphi(n_i \otimes \pi^{1-k} e_{k-1})$ for $i = 1, 2$. Let $T = T_{\bar{f}}(k-1)$ and $V = V_{\bar{f}}(k-1)$. (In fact, the proof works for $T = T_{\bar{f}}(m)$ for any integer m.) Recall that $\chi(\gamma) = 1 + p$.

Proposition 4.17. *We have* $\gamma\big[(1+\pi)n_i'\big] = (1 + \varphi(\pi))(1 + \pi)n_i' \mod (\varpi_E \varphi(\pi), \varphi(\pi)^2)$ *for* $i = 1, 2$.

Proof. We know that $\begin{pmatrix} n_1' \\ n_2' \end{pmatrix} = P^T \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes \varphi(\pi)^{1-k} e_{k-1}$. Since the actions of γ and φ commute, we have $\gamma(P^T)G_\gamma^T = \varphi(G_\gamma^T)P^T$, which implies

$$\begin{pmatrix} \gamma n_1' \\ \gamma n_2' \end{pmatrix} = \chi(\gamma)^{k-1} \varphi\left(\frac{\pi}{\gamma(\pi)}\right)^{k-1} \varphi(G_\gamma^T) \begin{pmatrix} n_1' \\ n_2' \end{pmatrix}.$$

Now

$$\begin{aligned} \chi(\gamma)\frac{\pi}{\gamma(\pi)} &= \frac{\chi(\gamma)}{1 + q + \varphi(\pi)} \\ &\equiv 1 \mod (p\pi, \pi^2) \end{aligned} \tag{45}$$

where the congruence comes from the fact that the constant term of q is p, and hence the constant term of $\frac{1}{1+q+\varphi(\pi)}$ is $\sum_{j=0}^{+\infty}(-p)^j$, which is equal to $\chi(\gamma)^{-1}$. Hence $\varphi\left(\frac{\chi(\gamma)\pi}{\gamma(\pi)}\right) \equiv 1 \mod (p\varphi(\pi), \varphi(\pi)^2)$. Moreover, $\gamma(1+\pi) = (1+\pi)^{\chi(\gamma)} = (1+\pi)(1+\varphi(\pi))$. Hence

$$\gamma\big[(1+\pi)n_1'\big] \equiv (1+\varphi(\pi))(1+\pi)n_1' \mod (\varpi_E\varphi(\pi), \varphi(\pi)^2)$$

by Corollary 4.16 □

We will now show that we can adapt the arguments form Proposition 4.17 to pass from $\varphi(\pi)(1+\pi)n_i'$ to $\varphi(\pi)^2(1+\pi)n_i' \mod (\varpi_E\varphi(\pi), \varphi(\pi)^3)$ for $i = 1, 2$.

Lemma 4.18. *We have* $(\gamma - 1)\big[\varphi(\pi)(1+\pi)n_i'\big] = \varphi(\pi)^2(1+\pi)n_i' \mod (\varpi_E\varphi(\pi), \varphi(\pi)^3)$ *for* $i = 1, 2$.

Proof. We have $\gamma(\pi) = (1+\pi)(1+\varphi(\pi)) - 1 = \pi + \varphi(\pi) + \pi\varphi(\pi)$, so

$$\begin{aligned} \varphi(\gamma(\pi)) &= \varphi(\pi)(1 + \varphi(q) + \varphi(\pi)\varphi(q)) \\ &\equiv \varphi(\pi) \mod (\varpi_E\varphi(\pi), \varphi(\pi)^3). \end{aligned}$$

Therefore,

$$\begin{aligned} \gamma\big[\varphi(\pi)(1+\pi)n_1'\big] &\equiv \varphi(\pi)(1 + \varphi(q) + \varphi(\pi)\varphi(q))(1+\pi)(1+\varphi(\pi))n_1' \mod (\varpi_E\varphi(\pi)^2, \varphi(\pi)^3) \\ &\equiv \varphi(\pi)(1+\pi)(1+\varphi(\pi))n_1' \mod (\varpi_E\varphi(\pi), \varphi(\pi)^3) \end{aligned}$$

and hence

$$(\gamma - 1)\big[\varphi(\pi)(1+\pi)n_1'\big] \equiv \varphi(\pi)^2(1+\pi)n_1' \mod (\varpi_E\varphi(\pi), \varphi(\pi)^3). \tag{46}$$

□

The lemma generalizes as follows for arbitrary $r \geq 1$.

Proposition 4.19. *We have* $(\gamma - 1)\big[\varphi(\pi)^r(1+\pi)n_i'\big] \equiv \varphi(\pi)^{r+1}(1+\pi)n_i' \mod (\varpi_E\varphi(\pi)^r, \varphi(\pi)^{r+2})$ *for* $i = 1, 2$.

Proof. Be the same calculations as in Lemma 4.18, we have

$$\begin{aligned}\gamma\big[\varphi(\pi)^r(1+\pi)n_1'\big] &\equiv \varphi(\pi)^r(1+\varphi(q)+\varphi(\pi)\varphi(q))^r(1+\pi)(1+\varphi(\pi))n_1' \mod (\varpi_E\varphi(\pi)^{r+1}, \varphi(\pi)^{r+2})\\ &\equiv \varphi(\pi)^r(1+\pi)(1+\varphi(\pi))n_1' \mod (\varpi_E\varphi(\pi)^r, \varphi(\pi)^{r+2})\end{aligned}$$

□

Definition 4.20. *For all* $r \geq 2$*, denote by* I_r *the ideal of* $\varphi(\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})$ *generated by the elements*

$$\varpi_E^{r-1}\varphi(\pi), \varpi_E^{r-2}\varphi(\pi)^2, \ldots, \varpi_E\varphi(\pi)^{r-1}, \varphi(\pi)^{r+1},$$

and let $\mathfrak{I}_r = I_r(\varphi^*\mathbb{N}(T))^{\psi=0}$.

Note that $\mathfrak{I}_r$ is stable under the action of G_∞.

Lemma 4.21. *We have* $(\gamma - 1)\mathfrak{I}_r \subset \mathfrak{I}_{r+1}$.

Proof. It is enough to show that $(\gamma-1)\big[x\varphi(\pi)^m(1+\pi)n_i'\big] \in \mathfrak{I}_{r+1}$ for any $m \geq 0$, any $x \in I_r$ and $i = 1, 2$.

Let $x = \varpi_E^{r-j}\varphi(\pi)^j$ where $1 \leq j \leq r-1$. By Proposition 4.19, we have

$$\begin{aligned}(\gamma-1)\big[\varpi_E^{r-j}\varphi(\pi)^{m+j}(1+\pi)n_i'\big] \equiv& \varpi_E^{r-j}\varphi(\pi)^{m+j+1}(1+\pi)n_i' \mod (\varpi_E^{r-j+1}\varphi(\pi)^{m+j}, \varpi_E^{r-j}\varphi(\pi)^{m+j+2})\\ \equiv& 0 \mod \mathfrak{I}_{r+1}\end{aligned}$$

for all $m \geq 0$. Similarly, the same holds for $x = \varphi(\pi)^{r+1}$. Hence the result. □

Proposition 4.22. *We have*

$$(\gamma-1)^r\left[(1+\pi)n_i'\right] \equiv \varphi(\pi)^r(1+\pi)n_i' \mod \mathfrak{I}_r$$

for all $r \geq 2$.

Proof. We proceed by induction on r. Let $r = 2$. By Proposition 4.17, we have

$$(\gamma-1)\left[(1+\pi)n_i'\right] \equiv \varphi(\pi)(1+\pi)n_i' \mod (\varpi_E\varphi(\pi), \varphi(\pi)^2).$$

It therefore follows from Lemma 4.18 and Proposition 4.19 that

$$(\gamma-1)^2\left[(1+\pi)n_i'\right] \equiv \varphi(\pi)^2(1+\pi)n_i' \mod (\varpi_E\varphi(\pi), \varphi(\pi)^3).$$

Assume now that the result is true for $r-1 \geq 2$, so

$$(\gamma-1)^{r-1}\left[(1+\pi)n_i'\right] \equiv \varphi(\pi)^{r-1}(1+\pi)n_i' \mod \mathfrak{I}_{r-1}.$$

Now

$$\begin{aligned}(\gamma-1)\left[\varphi(\pi)^{r-1}(1+\pi)n_i'\right] &\equiv \varphi(\pi)^r(1+\pi)n_i' \mod (\varpi_E\varphi(\pi)^{r-1}, \varphi(\pi)^{r+1})\\ &\equiv \varphi(\pi)^r(1+\pi)n_i' \mod \mathfrak{I}_r\end{aligned}$$

by Proposition 4.19. The result therefore follows from Lemma 4.21. □

To simplify the notation, let $X = \varphi(\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})(1+\pi)n_1' + \varphi(\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})(1+\pi)n_2'$.

Corollary 4.23. *For all* $x \in X$*, there exist* $\omega_1, \omega_2 \in \Lambda_{\mathcal{O}_E}(\Gamma)$ *such that*

$$\omega_1\big((1+\pi)n_1'\big) + \omega_2\big((1+\pi)n_2'\big) - x \in \varpi_E X.$$

Proof. $(\varphi^*\mathbb{N}(T))^{\psi=0}$ is complete in the $(\varpi_E, \varphi(\pi))$-adic topology, and the $\mathfrak{I}_r$, $r \geq 1$ form a neighbourhood of zero in $(\varphi^*\mathbb{N}(T))^{\psi=0}$. Hence the result follows from Proposition 4.22. □

Note that $(\varphi^*\mathbb{N}(T))^{\psi=0}$ is the Δ-orbit of X. The previous corollary therefore implies the following result:

Theorem 4.24. *$(\varphi^*\mathbb{N}(T))^{\psi=0}$ is a free $\Lambda_{\mathcal{O}_K}(G_\infty)$-module of rank 2, and a basis is given by $(1+\pi)n_1'$ and $(1+\pi)n_2'$.*

Proof. Let $y \in (\varphi^*\mathbb{N}(T))^{\psi=0}$. It follows from Corollary 4.23 and the fact that $\Lambda_{\mathcal{O}_E}(G_\infty)$ is p-adically complete that there exists $\omega_1, \omega_2 \in \Lambda_E(G_\infty)$ such that $y = \omega_1\big((1+\pi)n_1'\big) + \omega_2\big((1+\pi)n_2'\big)$. As shown in [PR94], $\mathbb{N}(T)^{\psi=1}$ is a free $\Lambda_E(G_\infty)$-module of rank 2, and the map $1-\varphi : \mathbb{N}(T)^{\psi=1} \to (\varphi^*\mathbb{N}(T))^{\psi=0}$ is injective since $V^{H_{\mathbb{Q}_p}} = \{0\}$. Hence the result. □

It therefore follows that after tensoring with $\mathbb{Q}$, there is an isomorphism of $\Lambda_E(G_\infty)$-modules (the *Iwasawa transform*)

$$\mathfrak{J} : (\varphi^*\mathbb{N}(V))^{\psi=0} \longrightarrow \Lambda_E(G_\infty)^{\oplus 2}$$

which satisfies the following condition: if $y = y_1(1+\pi)n_1' + y_2(1+\pi)n_2'$ with $y_i \in \varphi(E \otimes_{\mathbb{Q}_p} \mathbb{B}^+_{\mathbb{Q}_p})$ (write $y = (y_1, y_2)$) and $(z_1, z_2) = \mathfrak{J}(y_1, y_2)$, then $y = z_1[(1+\pi)n_1'] + z_2[(1+\pi)n_2']$. In particular, $\mathfrak{J}$ is additive and linear over E.

4.4. **An algorithm for $\mathfrak{J}$.** We now summarize the results of the previous section to give an explicit description of $\mathfrak{J}$ when restricted to $\varphi(E \otimes_{\mathbb{Q}_p} \mathbb{B}^+_{\mathbb{Q}_p})(1+\pi)n_1' \oplus \varphi(E \otimes_{\mathbb{Q}_p} \mathbb{B}^+_{\mathbb{Q}_p})(1+\pi)n_1' \cong \varphi(E \otimes_{\mathbb{Q}_p} \mathbb{B}^+_{\mathbb{Q}_p})^{\oplus 2}$. For a non-zero $y = (y_1, y_2) \in \varphi(E \otimes_{\mathbb{Q}_p} \mathbb{B}^+_{\mathbb{Q}_p})^{\oplus 2}$, we write

$$y_1 = \sum_{n=0}^{\infty} a_n \varphi(\pi)^n \qquad \text{and} \qquad y_2 = \sum_{n=0}^{\infty} b_n \varphi(\pi)^n.$$

On multiplying by a power of ϖ_E, we may assume that $y \in \varphi(\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})^{\oplus 2}$ but $\varpi_E \nmid y$. For such a y, we define the order $\mathrm{ord}(y)$ of y to be the minimum integer n such that either a_n or b_n is a unit in $\mathcal{O}_E$.

Proposition 4.25. *For y as above, there exists $z^{(n)} \in (\gamma-1)^n \Lambda_{\mathcal{O}_E}(\Gamma)^2$ such that $y - \mathfrak{J}^{-1}(z^{(n)})$ has order strictly greater than n.*

Proof. This is simply a reformulation of Proposition 4.22. In particular, one could take

$$z^{(n)} = (a_n(\gamma-1)^n, b_n(\gamma-1)^n).$$

□

Corollary 4.26. *For y as above, there exists a sequence $z^{(0)}, z^{(1)}, \ldots$ in $\Lambda_{\mathcal{O}_E}(\Gamma)^{\oplus 2}$ such that $z^{(i)} \to 0$ as $i \to \infty$ and*

$$y - \mathfrak{J}^{-1}\left(\sum_{i=0}^{\infty} z^{(i)}\right) \in \varpi_E \varphi(\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})^2$$

We write $y^{(0)} = y$ and $u^{(0)}$ for the infinite sum given by Corollary 4.26. Define a sequence $y^{(n)}$ recursively: for $n \geq 0$, let $y^{(n+1)} = (y^{(n)} - \mathfrak{J}^{-1}(u^{(n)}))/\varpi_E$ where $u^{(n)}$ to be the sum given by Corollary 4.26 on applying it to $y^{(n)}$. Then, we have

$$\mathfrak{J}(y) = \sum_{i=0}^{\infty} \varpi_E^i u^{(i)}.$$

4.5. **The image of $\underline{\mathrm{Col}}_1$.** Throughout this section, we assume that assumptions (B), (C) and (D) are satisfied.

Definition 4.27. *Let $\underline{\mathrm{Col}} = \mathfrak{J} \circ \mathbf{Col} : \mathbb{N}(T)^{\psi=1} \to \Lambda_{\mathcal{O}_E}(G_\infty)^{\oplus 2}$, and for $i = 1, 2$, define*

$$\underline{\mathrm{Col}}_i : \mathbb{N}(T)^{\psi=1} \longrightarrow \Lambda_{\mathcal{O}_E}(G_\infty)$$

as the composition $\mathrm{pr}_i \circ \underline{\mathrm{Col}}$, where pr_i is the projection from $\Lambda_{\mathcal{O}_E}(G_\infty)^{\oplus 2}$ onto the i-th coefficient.

By abuse of notation, we also write $\underline{\mathrm{Col}}_i$ for the natural extension $\mathbb{N}(V)^{\psi=1} \to \Lambda_E(G_\infty)$. The aim of this section is to prove the following theorem.

Theorem 4.28. *The map $\underline{\mathrm{Col}}_1 : \mathbb{N}(V)^{\psi=1} \to \Lambda_E(G_\infty)$ is surjective.*

The idea of the proof is to translate Proposition 4.7 using the explicit description of $\mathfrak{J}$ given in Section 4.4. Note that since $\mathfrak{J}$ is a $\Lambda_E(G_\infty)$-homomorphism, it is sufficient to show that $\varpi_E^m \in \mathrm{Im}(\underline{\mathrm{Col}}_1)$ for some $m \in \mathbb{Z}$.

Proposition 4.29. *Let $y_2 \in \varphi(\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})$. Then there exists a sequence $z^{(i)} \in \Lambda_{\mathcal{O}_E}(\Gamma)$ tending to 0 as $i \to +\infty$ and $\tilde{x} \in \mathbb{N}(T)^{\psi=1}$ and $y_2' \in \varphi(\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})$ such that*

$$\mathfrak{J}(0, y_2) - \mathfrak{J} \circ \mathrm{Col}(\tilde{x}) = \sum_{i \geq 0} (0, z^{(i)}) + \varpi_E \mathfrak{J}(0, y_2').$$

Proof. If $(0, y_2) = +\infty$, then $\varpi_E | y_2$ and we are done. Assume that $\mathrm{ord}(y_2) = n$ and write $y_2 = \sum_{r \geq 0} b_r \varphi(\pi)^r$. Then, by Lemma 4.25,

$$\mathfrak{J}(0, y_2) = \mathfrak{J}(y_1^{(1)}, y_2^{(1)}) + (0, b_n(\gamma - 1)^n). \tag{47}$$

where $y_2^{(i)}$ has order strictly greater than n. By applying $\mathfrak{J}^{-1}$ to (47), we see that

$$y_2(1+\pi)n_2' = y_1^{(1)}(1+\pi)n_1' + y_2^{(1)}(1+\pi)n_2' + b_n(\gamma-1)^n[(1+\pi)n_2'].$$

Since G_γ is diagonal $\mod \pi^{k-1}$, this implies that $y_1^{(1)} \equiv 0 \mod \varphi(\pi)^{k-1}$. In particular, the proof of Proposition 4.6 implies that there exists $x_1 \in \mathbb{N}(T)^{\psi=1}$ such that $(1-\varphi)x_1 = y_1^{(1)}(1+\pi)n_1'$. Hence, we have

$$\mathfrak{J}(0, y_2) - \mathfrak{J} \circ \mathrm{Col}(x_1) = \mathfrak{J}(0, y_2^{(1)}) + (0, z^{(1)})$$

where $z^{(1)} = b_n(\gamma - 1)^n$.

On applying the above to $y_2^{(1)}$ and repeat, we obtain sequences $\{x_n \in \mathbb{N}(T)^{\psi=1}\}$, $\{z^{(n)} \in \Lambda_{\mathcal{O}_E}(\Gamma)\}$ and $\{y_2^{(n)} \in \varphi(\mathbb{A}^+_{\mathbb{Q}_p})\}$ such that

$$\mathfrak{J}(0, y_2^{(n-1)}) - \mathfrak{J} \circ \mathrm{Col}(x_n) = \mathfrak{J}(0, y_2^{(n)}) + (0, z^{(n)}),$$

the sequence $m_n = \mathrm{ord}(y_2^{(n)})$ is strictly increasing, $z^{(n)} \in (\gamma-1)^{m_{n-1}}\Lambda_{\mathcal{O}_E}(\Gamma)$ and $\mathrm{Col}(x_n) + (y_2^{(n)} - y_2^{(n-1)})(1+\pi)n_2' = z^{(n)}[(1+\pi)n_2']$. Now $\mathrm{Col}(x_n) \in \varphi(\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})(1+\pi)n_1'$, so (i) $x_n \to 0$ and (ii) $(y_2^{(n)} - y_2^{(n-1)}) \to 0$. By completeness, (ii) implies that $y_2^{(n)}$ converges to an element in $\varpi_E \varphi(\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})$. (The limit must be in $\varpi_E \varphi(\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})$ because the order of the limit is $+\infty$ by construction.) Now, on taking sums, we have for all $n \geq 1$,

$$\mathfrak{J}(0, y_2) - \sum_{i=1}^{n} \mathfrak{J} \circ \mathrm{Col}(x_i) = \mathfrak{J}(0, y_2^{(n)}) + \sum_{i=1}^{n} (0, z^{(i)}).$$

We obtain the result by letting $n \to \infty$. $\square$

Corollary 4.30. *Let $y_2 \in \varphi(\mathcal{O}_K \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})$. Then there exists a sequence $z^{(i)} \in \Lambda_{\mathcal{O}_E}(\Gamma)$ tending to 0 as $i \to +\infty$ and $\tilde{x} \in \mathbb{N}(T)^{\psi=1}$ such that*

$$\mathfrak{J}(0, y_2) - \mathfrak{J} \circ \mathrm{Col}(\tilde{x}) = \sum_{i \geq 0} (0, z^{(i)}).$$

Proof. Iterate the result in Proposition 4.29 for $\mathfrak{J}(0, y_2')$ etc. and use that both $\Lambda_{\mathcal{O}_E}(\Gamma)$ and $\varphi^*(\mathbb{N}(T))^{\psi=0}$ are p-adically complete. $\square$

Corollary 4.31. *Let $y \in (\varphi^*\mathbb{N}(T))^{\psi=0}$ be of the form $y = y_2 n_2'$ for some $y_2 \in (\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$. Then there exists a sequence $z^{(i)} \in \Lambda_{\mathcal{O}_E}(G_\infty)$ tending to 0 as $i \to +\infty$ and $\tilde{x} \in \mathbb{N}(T)^{\psi=1}$ such that*

$$\mathfrak{J}(y) - \mathfrak{J} \circ \mathrm{Col}(\tilde{x}) = \sum_{i \geq 0} (0, z^{(i)}).$$

Proof. Immediate from the previous corollary and the observation that $(\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0} n_2'$ is the Δ-orbit of $\varphi(\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})(1+\pi)n_2'$. $\square$

We can now prove Theorem 4.28. By Proposition 4.7 there exists $x \in \mathbb{N}(T)^{\psi=1}$ such that $\mathrm{Col}(x) = \varpi_E^m(1+\pi)n'_1 + y_2 n'_2$ for some $y_2 \in (\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$. It is clear that $\mathfrak{J}(\varpi_E^m(1+\pi)n'_1) = (\varpi_E^m, 0)$. Also, we know by Corollary 4.31 that there exists a sequence $z^{(i)} \in \Lambda_{\mathcal{O}_E}(G_\infty)$ tending to 0 as $i \to +\infty$ and $\tilde{x} \in \mathbb{N}(T)^{\psi=1}$ such that

$$\mathfrak{J}(y_2 n'_2) - \mathfrak{J} \circ \mathrm{Col}(\tilde{x}) = \sum_{i \geq 0} (0, z^{(i)}).$$

Hence $\mathfrak{J} \circ \mathrm{Col}(x) - \mathfrak{J} \circ \mathrm{Col}(\tilde{x}) = (\varpi_E^m, 0) + \sum_{i\geq 0}(0, z^{(i)})$, i.e.

$$\mathfrak{J} \circ \mathrm{Col}(x - \tilde{x}) = (\varpi_E^m, 0) + \sum_{i \geq 0} (0, z^{(i)}).$$

Remark 4.32. *Alas so far we don't know how to translate Proposition 4.11 into a statement about* $\operatorname{Im} \underline{\mathrm{Col}}_2$.

Remark 4.33. *In a forthcoming paper* [LLZ10]*, we give a description of the images of the* $\underline{\mathrm{Col}}_i$ *using Perrin-Riou's p-adic regulator.*

5. Relations to existing work

5.1. **Fourier transforms.** In this section, we prove a compatibility result in p-adic Fourier theory (theorem 5.4 below) which will allows us to relate divisibility of elements in $\mathcal{H}(G_\infty)$ and of their images in $(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}$ under the Mellin tranform. This will allow us to compare our results above to the ones in [Kob03], [Lei09] and [Spr09]. Throughout, E is a complete extension of $\mathbb{Q}_p$.

5.1.1. *The Fourier transform for $\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$.* We recall some standard results of p-adic Fourier theory. These results are due to Amice [AV75]; see also [Col10] for a more modern account. We denote by $C^{\mathrm{la}}(\mathbb{Z}_p, E)$ the space of locally analytic E-valued functions on $\mathbb{Z}_p$, with the topology it acquires as the locally convex direct limit as $n \to \infty$ of the Banach algebras of functions analytic on cosets of $p^n\mathbb{Z}_p$. A *distribution* on $\mathbb{Z}_p$ is a continuous E-linear functional $C^{\mathrm{la}}(\mathbb{Z}_p, E) \to E$; we write $D^{\mathrm{la}}(\mathbb{Z}_p, E)$ for the space of distributions.

Proposition 5.1 ([Col10, theorem 2.3])**.** *There is an isomorphism between $D^{\mathrm{la}}(\mathbb{Z}_p, E)$ and the subset of functions $f \in E[[T]]$ converging for all T in the open unit disc of $\mathbb{C}_p$, given by $\mu \mapsto F_\mu(T) = \sum_{n \geq 0} T^n \mu\left(\binom{x}{n}\right)$. The value of F_μ at a point $x \in E$ (with $|x| < 1$) is $\mu(\kappa_x)$, where κ_x is the unique character of $\mathbb{Z}_p$ such that $\kappa(1) = 1 + x$.*

Thus we may identify $D^{\mathrm{la}}(\mathbb{Z}_p, E)$ with $E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$. Under this identification, the subspace $D^{\mathrm{la}}(\mathbb{Z}_p^\times, E)$ of distributions supported in $\mathbb{Z}_p^\times$ corresponds to $(E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}$ [Col10, §2.4.5].

Suppose $p \neq 2$. An alternative description of $D^{\mathrm{la}}(\mathbb{Z}_p^\times, E)$ is given by the isomorphism $\mathbb{Z}_p^\times = (1+p\mathbb{Z}_p) \times \Delta \cong \mathbb{Z}_p \times \Delta$, where Δ is the group of $(p-1)$st roots of unity in $\mathbb{Z}_p$. If we fix a topological generator γ of $1 + p\mathbb{Z}_p$, we thus have an isomorphism

$$D^{\mathrm{la}}(\mathbb{Z}_p^\times, E) \cong E \otimes \mathcal{H}(G_\infty),$$

where as in section 3.4 above, $\mathcal{H}(G_\infty)$ is the ring of formal series $f(\gamma - 1)$, for $f \in \mathbb{Q}_p[\Delta][[X]]$ converging for all $|X| < 1$.

Thus for a distribution μ on $\mathbb{Z}_p^\times$, we obtain two power series

$$F^+_\mu(\pi) \in (E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}$$

and

$$F^\times_\mu(X) \in E \otimes \mathcal{H}(G_\infty).$$

These are related by the Mellin transform of lemma 3.7: we have $\mathfrak{M}(F^\times_\mu(\gamma)) = F^+_\mu$.

5.1.2. *Step functions.* Let $n \geq 0$ be an integer. We say a function $f : \mathbb{Z}_p \to E$ is a *step function of order* n if it is constant on any coset $a + p^n\mathbb{Z}_p$; the space $\mathrm{Step}_n(\mathbb{Z}_p)$ of such functions is clearly a subspace of $C^{\mathrm{la}}(\mathbb{Z}_p, E)$ of dimension p^n.

For each n we have an inclusion $\mathrm{Step}_n(\mathbb{Z}_p) \to \mathrm{Step}_{n+1}(\mathbb{Z}_p)$. A section of this is given by the "averaging" map $I : \mathrm{Step}_{n+1}(\mathbb{Z}_p) \to \mathrm{Step}_n(\mathbb{Z}_p)$ defined by

$$I(f)(x) = \frac{1}{p} \sum_{y \in \mathbb{Z}/p\mathbb{Z}} f(x + p^n y).$$

For $n \geq 1$, we say a function $f \in \mathrm{Step}_n(\mathbb{Z}_p)$ is a *primitive step function* if it is in the kernel of this map, and write $\mathrm{PStep}_n(\mathbb{Z}_p)$ for the space of such functions, which clearly has dimension $p^{n-1}(p-1)$. For consistency we take $\mathrm{PStep}_0(\mathbb{Z}_p) = \mathrm{Step}_0(\mathbb{Z}_p) = K$.

Lemma 5.2. *Let $n \geq 0$ and suppose E contains a primitive p^n-th root of unity ζ_{p^n}. Then a basis for $\mathrm{Step}_n(\mathbb{Z}_p)$ is given by the functions $x \mapsto (\zeta_{p^n})^{xt}$, as t varies through $\mathbb{Z}/p^n\mathbb{Z}$. The subset corresponding to $t \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ is a basis for $\mathrm{PStep}_n(\mathbb{Z}_p)$.*

Proof. This follows immediately from the fact that $x \mapsto \frac{1}{p^n} \sum_{t \in \mathbb{Z}/p^n\mathbb{Z}} (\zeta_{p^n})^{xt} (\zeta_{p^n})^{-at}$ is the characteristic function of $a + p^n\mathbb{Z}_p$. □

We also have a "multiplicative" version. For $n \geq 1$, we define $\mathrm{Step}_n(\mathbb{Z}_p^\times)$ as the functions in $\mathrm{Step}_n(\mathbb{Z}_p)$ which are supported in $\mathbb{Z}_p^\times$. For $n \geq 2$ the averaging map restricts to a map $\mathrm{Step}_n(\mathbb{Z}_p^\times) \to \mathrm{Step}_n(\mathbb{Z}_p^\times)$, and we define $\mathrm{PStep}_n(\mathbb{Z}_p^\times)$ to be its kernel. We take $\mathrm{PStep}_1(\mathbb{Z}_p^\times) = \mathrm{Step}_1(\mathbb{Z}_p^\times)$, so for all $n \geq 1$ restriction to $\mathbb{Z}_p^\times$ defines a surjective map $\mathrm{PStep}_n(\mathbb{Z}_p) \to \mathrm{PStep}_n(\mathbb{Z}_p^\times)$.

Lemma 5.3. *A basis for $\mathrm{Step}_n(\mathbb{Z}_p^\times)$ is given by the Dirichlet characters modulo p^n. For $n \geq 2$ the subset of primitive characters modulo p^n gives a basis for $\mathrm{PStep}_n(\mathbb{Z}_p^\times)$.*

Proof. Similar to the previous lemma. □

5.1.3. *Relating the additive and multiplicative transforms.* We now suppose we are given a distribution $\mu \in D^{\mathrm{la}}(\mathbb{Z}_p^\times, E)$. Let $F_\mu^\times$ and F_μ^+ be the corresponding transforms.

Theorem 5.4. *For $n \geq 2$, the following are equivalent:*

(1) *F_μ^+ is divisible by the cyclotomic polynomial $\Phi_n(1+\pi)$ in $\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$.*
(2) *μ annihilates $\mathrm{PStep}_n(\mathbb{Z}_p)$.*
(3) *μ annihilates $\mathrm{PStep}_n(\mathbb{Z}_p^\times)$.*
(4) *$F_\mu^\times(\chi)$ is zero for all primitive Dirichlet characters $\chi \bmod p^n$.*
(5) *$F_\mu^\times$ is divisible by $\Phi_{n-1}(1+X)$ in $E \otimes \mathcal{H}(G_\infty)$.*

For $n = 1$, the same holds with the last two statements replaced by:

(4') *$F_\mu^\times(\chi)$ is zero for all Dirichlet characters $\chi \bmod p$.*
(5') *$F_\mu^\times$ is divisible by X in $E \otimes \mathcal{H}(G_\infty)$.*

Proof. It is clear that (1) ⇔ (2) for arbitrary $\mu \in D^{\mathrm{la}}(\mathbb{Z}_p, E)$ (not necessarily supported in $\mathbb{Z}_p^\times$), because of Lemma 5.2. Since restriction of functions gives a surjective map $\mathrm{PStep}_n(\mathbb{Z}_p) \twoheadrightarrow \mathrm{PStep}_n(\mathbb{Z}_p^\times)$, we have (2) ⇔ (3). The equivalence (3) ⇔ (4) follows from Lemma 5.3.

To show (4) ⇔ (5) for $n \geq 2$, let us write $F_\mu^\times = \sum_{i=1}^{p-1} [\tau(i)] F_i(X)$, where $F_i \in E[[X]]$ and $\tau(i) \in \Delta$ is the Teichmüller lift of i. For any primitive p^{n-1}st root of unity ζ, there are exactly $p-1$ primitive Dirichlet charcters modulo p^n mapping γ to ζ, and their restrictions to Δ are given by $\tau(i) \mapsto \tau(i)^k$ for $k \in \mathbb{Z}/(p-1)\mathbb{Z}$. So (4) is equivalent to

$$\sum_{i=1}^{p-1} \tau(i)^k F_i(\zeta - 1) = 0$$

for all $k = 0 \dots p-2$ and all primitive p^{n-1}st roots of unity ζ, which is equivalent to $F_i(\zeta - 1) = 0$ for each $i = 1, \dots, p-1$. In other words, each of the functions $F_i(X)$ vanishes at every root of the polynomial $\Phi_{n-1}(1+X)$, which is clearly equivalent to $F_\mu^\times$ being divisible by $\Phi_{n-1}(1+X)$ in $E \otimes \mathcal{H}(G_\infty)$.

(The only change necessary for $n = 1$ is to note that $\mathrm{PStep}_1(\mathbb{Z}_p^\times)$ is the linear span of all Dirichlet characters modulo p, not just the primitive ones.) □

We also have an accompanying result:

Lemma 5.5. *Let $F \in (E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0}$. Then $\Phi_1(1+\pi)$ divides $F(\pi)$ if and only if $\varphi(\pi) = \pi\Phi_1(1+\pi)$ divides $F(\pi)$.*

Proof. Since $\psi(F)(0) = 0$, we have

$$F(0) + \sum_{\substack{\zeta \in \mu_p \\ \zeta \neq 1}} F(\zeta - 1) = 0.$$

Hence if F vanishes at the points $\zeta - 1$ for primitive $\zeta \in \mu_p$, then it must also vanish at 0. □

5.2. **The case $a_p = 0$.** We now relate the construction of Coleman maps in this paper to the construction given in [Lei09] for modular forms with $a_p = 0$.

5.2.1. *Construction of the Coleman maps.* Consider f a normalized new eigenform as in Section 3.3 with $a_p = 0$. To ease notation, we assume that $E = \mathbb{Q}_p$. The plus and minus Coleman maps in [Lei09] are constructed as follows.

Let $u = \chi(\gamma)$. In [Pol03], Pollack defines the following elements of $\mathcal{H}(G_\infty)$:

$$\log^+_{p,k} = \prod_{j=0}^{k-2} \frac{1}{p} \prod_{n=1}^{+\infty} \frac{\Phi_{2n}(u^{-j}\gamma)}{p}$$

$$\log^-_{p,k} = \prod_{j=0}^{k-2} \frac{1}{p} \prod_{n=1}^{+\infty} \frac{\Phi_{2n-1}(u^{-j}\gamma)}{p}.$$

Let $\nu^- = \bar{\nu}_1$, $\nu^+ = \bar{\nu}_2$ be the basis of $\mathbb{D}_{\mathrm{cris}}(V_{\bar{f}})$ as in Section 3.3 and let $\eta^\pm = (1+\pi)\otimes\nu^\pm \in (\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})^{\psi=0} \otimes \mathbb{D}_{\mathrm{cris}}(V)$. Let

$$\mathcal{L}_{1,\eta^\pm} : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V_{\bar{f}}(k-1)) \longrightarrow \mathcal{H}(G_\infty)$$

be the map defined by (18).

Lemma 5.6. $\log^\pm_{p,k} \mid \mathcal{L}_{1,\eta^\pm}(z)$ *for any* $z \in H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V_{\bar{f}}(k-1))$.

Proof. See [Lei09, Lemma 2.2]. □

One can therefore define

$$\begin{aligned} \mathrm{Col}^\pm : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V_{\bar{f}}(k-1)) &\longrightarrow \Lambda_{\mathbb{Q}_p}(G_\infty) \\ z &\longmapsto \frac{\mathcal{L}_{1,\eta^\pm}(z)}{\log^\pm_{p,k}}. \end{aligned} \tag{48}$$

In this setting, we can work out the matrix M in (20) explicitly. As in section 4 above, we let n_1, n_2 be the basis of $\mathbb{N}(V_{\bar{f}})$ constructed in [BLZ04]. The results of *op.cit.* imply that the $\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p}$-span of n_1, n_2 is $\mathbb{N}(T_{\bar{f}})$ for a $G_{\mathbb{Q}_p}$-stable $\mathcal{O}_E$-lattice $T_{\bar{f}} \subset V_{\bar{f}}$.

Recall that $M \in M_2(\varphi(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}))$ is the matrix satisfying $\begin{pmatrix} \varphi(n_1) \\ \varphi(n_2) \end{pmatrix} = M \begin{pmatrix} \nu_1 \\ \nu_2 \end{pmatrix}$.

Lemma 5.7. *The matrix M is given by*

$$\begin{pmatrix} 0 & (\log^+(1+\pi))^{k-1} \\ -(\log^-(1+\pi)/q)^{k-1} & 0 \end{pmatrix}.$$

Proof. With respect to the basis n_1, n_2 of $\mathbb{N}(V_{\bar{f}})$ over $\mathbb{B}^+_{\mathbb{Q}_p}$, as chosen in [BLZ04], the matrices of φ and $\gamma \in G_\infty$ are given by

$$P = \begin{pmatrix} 0 & -1 \\ q^{k-1} & 0 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} \left(\frac{\log^+(1+\pi)}{\gamma(\log^+(1+\pi))}\right)^{k-1} & 0 \\ 0 & \left(\frac{\log^-(1+\pi)}{\gamma(\log^-(1+\pi))}\right)^{k-1} \end{pmatrix} \tag{49}$$

respectively. Then,

$$\bar{\nu}_1 = (\log^+(1+\pi))^{k-1} n_1 \qquad \text{and} \qquad \bar{\nu}_2 = (\log^-(1+\pi))^{k-1} n_2,$$

so the base-change matrix M' (defined in (8)) is given by

$$\begin{pmatrix} (\log^+(1+\pi))^{k-1} & 0 \\ 0 & (\log^-(1+\pi))^{k-1} \end{pmatrix} \tag{50}$$

and the result follows from explicit calculations, using that $M = \left(\frac{t}{\pi q}\right)^{k-1} P^T M'^{-1}$. ☐

Lemma 5.8. *We have $\varphi(\log^-(1+\pi)) = \log^+(1+\pi)$ and $\varphi(\log^+(1+\pi)) = \frac{p}{q}\log^-(1+\pi)$.*

Proof. Immediate. ☐

Lemma 5.9. *For $i \in \{1, \dots, p-1\}$ we have*

$$\mathfrak{M}^{-1}\left((1+\pi)^i \log^+(1+\pi)^{k-1} \cdot \varphi(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})\right) = \tau(i) \log^-_{p,k}(\gamma) \cdot \mathcal{H}(\Gamma)$$

and

$$\mathfrak{M}^{-1}\left((1+\pi)^i \log^-(1+\pi)^{k-1}/q^{k-1} \cdot \varphi(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})\right) = \tau(i) \log^+_{p,k}(\gamma) \cdot \mathcal{H}(\Gamma),$$

where $\tau(i) \in \Delta$ is the Teichmuller lift of i.

Proof. Let us suppose first that $k = 2$. Any element $f \in (1+\pi)^i \log^+(1+\pi) \cdot \varphi(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})$ is F^+_μ for some distribution μ on $\mathbb{Z}_p$, supported in $i + p\mathbb{Z}_p \subseteq \mathbb{Z}_p^\times$; hence we have a corresponding multiplicative Fourier transform $F^\times_\mu = \mathfrak{M}^{-1}(f)$, lying in $\tau(i)\mathcal{H}(\Gamma)$. Moreover, we have the implications

$$\begin{aligned} & \log^+(1+\pi) \mid f \text{ in } \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p} \\ \iff & \Phi_n(1+\pi) \mid f \text{ for all even } n \geq 2 \\ \iff & \Phi_n(1+X) \mid \mathfrak{M}^{-1}(f) \text{ for all odd } n \geq 1 \text{ (by theorem 5.4)} \\ \iff & \log^-(1+X) \mid \mathfrak{M}^{-1}(f). \end{aligned}$$

The second statement is similar, noting that $q = \Phi_1(1+\pi)$ and hence $\log^-(1+\pi)/q$ divides f if and only if f vanishes at the primitive p^n-th roots of unity for all odd $n \geq 3$.

For general $k \geq 2$, we note that $f \in \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$ vanishes to order $k-1$ at a point z if and only if $\partial^j f$ vanishes at z for $j = 0, \dots, k-2$, where ∂ is the differential operator $(1+\pi)\frac{\mathrm{d}}{\mathrm{d}\pi}$ introduced in §2.2. Applying the preceding argument to each of the functions $\partial^j f$, we see that $\log^+(1+\pi) \mid f$ if and only if $\mathfrak{M}^{-1}(\partial^j f)$ is divisible by $\log^-(1+X)$ for $0 \leq j \leq k-2$. Since $\mathfrak{M}^{-1}(\partial^j f)(z) = \mathfrak{M}^{-1}(f)(u^j(1+z)-1)$ where $u = \chi(\gamma)$, this is equivalent to the divisibility of f by $\log^-_{p,k}$. Again, the second statement follows very similarly to the first. ☐

Proposition 5.10. *There exists $a^\pm \in \Lambda_E(G_\infty)^\times$ such that*

$$\underline{M} = \begin{pmatrix} 0 & -a^- \log^-_{p,k} \\ a^+ \log^+_{p,k} & 0 \end{pmatrix}.$$

Proof. By Lemma 5.9, $\mathfrak{M}$ restricts to an isomorphism of $\mathcal{H}(G_\infty)$-modules between the subspaces $X^\pm = (1+\pi)\varphi(\log^\pm(1+\pi))^{k-1}\cdot\varphi(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})$ and $Y^\pm = \log^\pm_{p,k}\cdot\mathcal{H}(G_\infty)$. In particular, there exist $a^\pm \in \mathcal{H}(G_\infty)$ such that

$$\mathfrak{M}^{-1}((1+\pi)\varphi(\log^\pm(1+\pi))^{k-1}) = a^\pm \log^\pm_{p,k}.$$

Furthermore, $(1+\pi)\varphi(\log^\pm(1+\pi))^{k-1}$ are $\Lambda_E(G_\infty)$-module generators of $(1+\pi)\varphi(\log^\pm(1+\pi))^{k-1}\cdot\varphi(\mathbb{B}^+_{\mathbb{Q}_p})$, by Proposition 4.24. Since any finitely-generated submodule of $\mathcal{H}(G_\infty)$ is closed, they must be $\mathcal{H}(G_\infty)$-module generators of the closures of these spaces, which are clearly $X^\pm$. Therefore the images of $(1+\pi)\varphi(\log^\pm(1+\pi))^{k-1}$ under $\mathfrak{M}^{-1}$ must be generators of $Y^\pm$, so the factors $a^\pm$ are units. □

Therefore, by (32), we have:

Corollary 5.11. *Let $a^\pm$ be as in Proposition 5.10, then $a^- \,\underline{\mathrm{Col}}_1 = \mathrm{Col}^-$ and $a^+\,\underline{\mathrm{Col}}_2 = \mathrm{Col}^+$.*

5.2.2. *Description of the kernels.* The aim of this section is to give a simple description of $\ker(\mathrm{Col}_i)$ for $i = 1, 2$. Recall that the basis $\bar\nu_1, \bar\nu_2$ of $\mathbb{D}_{\mathrm{cris}}(V_{\bar f})$ determines a basis of $\mathbb{D}_{\mathrm{cris}}(V_{\bar f}(k-1))$ via the map $\bar\nu_i \mapsto \bar\nu_i \otimes e_{k-1}t^{1-k}$. We first need to know a bit more about $\mathbb{N}(V_{\bar f})$. As stated in [Ber03, Section II.3], we have a comparison isomorphism

$$\iota : \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}[t^{-1}] \otimes_{\mathbb{B}^+_{\mathbb{Q}_p}} \mathbb{N}(V_{\bar f}(k-1)) \cong \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}[t^{-1}] \otimes_{\mathbb{Q}_p} \mathbb{D}_{\mathrm{cris}}(V_{\bar f}(k-1)).$$

By (20) and (10), if $x \in \mathbb{D}(V_{\bar f}(k-1))^{\psi=1}$, then we can write $\iota(x) = x_1(\bar\nu_1 \otimes e_{k-1}t^{1-k}) + x_2(\bar\nu_2 \otimes e_{k-1}t^{1-k})$ where

$$x_1 = x_1'(\log^-(1+\pi))^{k-1}$$
$$x_2 = x_2'(\log^+(1+\pi))^{k-1}$$

for some $x_1', x_2' \in \mathbb{B}^+_{\mathbb{Q}_p}$.

We will need the following auxiliary lemma.

Lemma 5.12. *Let x be as above. Then $p^{k-2}\theta(x_1) + \theta(x_2) = 0$.*

Proof. By [Ber03, Theorem II.6], we have

$$\exp^*_{\mathbb{Q}_p, V_{\bar f}(k-1)}\left(h^1_{\mathbb{Q}_p, V_{\bar f}(k-1)}(x)\right) = (1 - p^{-1}\varphi^{-1})\partial_V(x). \tag{51}$$

Since $\partial_V(x) = \theta(x_1)\bar\nu_1 \otimes e_{k-1}t^{1-k} + \theta(x_2)\bar\nu_2 \otimes e_{k-1}t^{1-k}$, we have

$$(1-p^{-1}\varphi^{-1})\partial_V(x) = \big(\theta(x_1) - p^{-1}\theta(x_2)\big)\nu_1 + \big(p^{k-2}\theta(x_1) + \theta(x_2)\big)\nu_2.$$

The image of $\exp^*_{\mathbb{Q}_p, V_{\bar f}(k-1)}$ is contained in $\mathrm{Fil}^0\,\mathbb{D}_{\mathrm{cris}}(V_{\bar f}(k-1))$, which implies that $p^{k-2}\theta(x_1) + \theta(x_2) = 0$. □

Lemma 5.13. *Let $x \in \mathbb{D}(V_{\bar f}(k-1))^{\psi=1}$, and write $\iota(x) = x_1(\bar\nu_1 \otimes e_{k-1}t^{1-k}) + x_2(\bar\nu_2 \otimes e_{k-1}t^{1-k})$ as above. Then*

(i) *$x \in \ker(\mathrm{Col}_1)$ if and only if $\varphi(x_1) = -p^{k-1}\psi(x_1)$;*
(ii) *$x \in \ker(\mathrm{Col}_2)$ if and only if $\varphi(x_2) = -p^{k-1}\psi(x_2)$.*

Proof. We will prove the proposition for Col_1; the proof for Col_2 is analogous. Note that the condition that $\psi(x) = x$ translates as $\psi(x_1) = -p^{1-k}x_2$ and $\psi(x_2) = x_1$. By Lemma 5.8, $\mathrm{Col}_1(x) = x_2' - \varphi(x_1') = 0$ if and only if $x_2 = \varphi(x_1)$. Hence, $\mathrm{Col}_1(x) = 0$ if and only if $\varphi(x_1) = -p^{k-1}\psi(x_1)$. □

Proposition 5.14. *Let x be as above, and write $x_i = f_i(\pi)$ with $f_i(X) \in \mathbb{Q}_p[[X]]$. Then*

(i) *$x \in \ker(\mathrm{Col}_1)$ if and only if*

$$\mathrm{Tr}_{\mathbb{Q}_{p,n}/\mathbb{Q}_{p,n-1}}\left(f_1(\zeta_{p^n}-1)\right) = -p^{2-k}f_1(\zeta_{p^{n-2}}-1) \text{ for all } n \ge 2, \text{ and} \tag{52}$$

$$\mathrm{Tr}_{\mathbb{Q}_{p,1}/\mathbb{Q}_p}(f_1(\zeta_p - 1)) = -(1+p^{2-k})f_1(0); \tag{53}$$

(ii) $x \in \ker(\mathrm{Col}_2)$ *if and only if*

$$\mathrm{Tr}_{\mathbb{Q}_{p,n}/\mathbb{Q}_{p,n-1}}\left(f_2(\zeta_{p^n}-1)\right) = -p^{2-k} f_2(\zeta_{p^{n-2}}-1) \text{ for all } n \geq 2, \text{ and}$$
$$\mathrm{Tr}_{\mathbb{Q}_{p,1}/\mathbb{Q}_p}(f_2(\zeta_p-1)) = -(1+p^{2-k})f_2(0).$$

Proof. We prove the proposition for Col_1. Recall that

$$\varphi\psi(x_1) = p^{-1}\sum_{\zeta^p=1} f_1\big(\zeta(1+\pi)-1\big).$$

Hence, $\varphi(x_1) = -p^{k-1}\psi(x_1)$ implies that

$$\sum_{\zeta^p=1} f_1\big(\zeta(1+\pi)-1\big) = -p^{2-k}\varphi^2\big(f_1(\pi)\big). \tag{54}$$

Let $n \geq 2$. On applying $\theta\circ\varphi^{-n}$ to (54) implies that

$$\mathrm{Tr}_{\mathbb{Q}_{p,n}/\mathbb{Q}_{p,n-1}}\left(f_1(\zeta_{p^n}-1)\right) = \sum_{\zeta^p=1} f_1(\zeta\zeta_{p^n}-1) = -p^{2-k}f_1(\zeta_{p^{n-2}}-1).$$

Similarly, we obtain the second condition by applying θ to (54).

Conversely, assume that (52) holds for all $n \geq 2$, then $\varphi(f_1)+p^{k-1}\psi(f_1) = 0$ at $\zeta_{p^n}-1$. Recall that $x_1 = x_1'(\log^-(1+\pi))^{k-1}$ where $x_1' \in \mathbb{B}^+_{\mathbb{Q}_p}$. By Lemma 5.8,

$$\varphi(x_1)+p^{k-1}\psi(x_1) = (\varphi(x_1')+\psi(q^{k-1}x_1'))(\log^+(1+\pi))^{k-1}.$$

Hence, the power series in $\mathbb{Q}\otimes\mathbb{Z}_p[[X]]$ corresponding to $(\varphi(x_1')+\psi(q^{k-1}x_1'))$ has infinitely many zeros, so it must be zero itself and we are done. □

As a corollary, we obtain the following descriptions of $\ker(\mathrm{Col}_i)$.

Corollary 5.15. *For $x \in \mathbb{D}(V_{\bar f}(k-1))^{\psi=1}$, write $e_n(x) = \exp^*_{n,V_{\bar f(k-1)}}\circ\mathrm{Pr}_n\circ h^1_{\mathbb{Q}_p,\mathrm{Iw}}(x)$ where Pr_n is the projection from $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V_{\bar f}(k-1))$ to $H^1(\mathbb{Q}_{p,n}, V_{\bar f}(k-1))$. Let $i=1$ (respectively $i=2$), then*

$$\ker(\mathrm{Col}_i) = \{x\in\mathbb{D}(V_{\bar f}(k-1))^{\psi=1} : e_0(x) = 0 \text{ and } e_{n+1}(x) = p^{-1}e_n(x)\forall \text{ odd (respectively even) } n\geq 1\}.$$

Proof. Again, we only prove this for $i=1$. By [CC99, Théorème IV.2.1], we have $e_n(x) = p^{-n}\partial_V(\varphi^{-n}(x))$ for all $n\geq 1$. But φ^{-2} is the multiplication by $-p^{k-1}$ on $\mathbb{D}_{\mathrm{cris}}(V_{\bar f}(k-1))$. Using again that $\mathrm{Im}(\exp^*_{n,V_{\bar f(k-1)}}) \subset \mathrm{Fil}^0\,\mathbb{D}_{\mathrm{cris}}(V)$, we see that

$$e_{2n}(x) = p^{-2n}\cdot(-p)^{n(k-1)}f_1(\zeta_{p^{2n}}-1)\bar\nu_1\otimes t^{1-k}e_{k-1}$$
$$e_{2n+1}(x) = p^{-2n-1}\cdot(-p)^{n(k-1)}f_2(\zeta_{p^{2n+1}}-1)\bar\nu_1\otimes t^{1-k}e_{k-1}$$

and $f_2(\zeta_{p^{2n}}-1) = f_1(\zeta_{p^{2n-1}}-1) = 0$ for all $n\geq 1$. Therefore, (52) holds for $2n-1$ and for $2n$ if and only if $e_{2n}(x) = \mathrm{Tr}_{F_{2n+1}/F_{2n}}(e_{2n+1}(x)) = p^{-1}e_{2n-1}(x)$.

Now $e_0(x) = (f_1(0)-p^{-1}f_2(0))\bar\nu_1\otimes t^{1-k}e_{k-1}$ by (51) and $p^{k-2}f_1(0)+f_2(0) = 0$ by Lemma 5.12, so

$$e_0(x) = (1+p^{k-3})f_1(0)\bar\nu_1\otimes t^{1-k}e_{k-1} = -(p^{2-k}+p^{-1})f_2(0)\bar\nu_1\otimes t^{1-k}e_{k-1}$$

The condition (53) is therefore equivalent to $f_1(0)=0$, which in turns is equivalent to $e_0(x)=0$. □

In the rest of this section, we will relate Corollary 5.15 to the description of $\ker(\mathrm{Col}^\pm)$ in [Lei09, Section 2.2]. Recall that $H^1_f(\mathbb{Q}_{p,n}, T_f(1))^\pm$ is defined by

$$\left\{x\in H^1_f(\mathbb{Q}_{p,n},T_f(1)) : \mathrm{cor}_{n/m+1}x \in H^1_f(\mathbb{Q}_{p,m},T_f(1))\ \forall m \text{ even (odd)}, m<n\right\}.$$

Denote by $H^1_\pm(\mathbb{Q}_{p,n}, T_{\bar f}(k-1))$ the annihilator of $H^1_f(\mathbb{Q}_{p,n},T_f(1))^\pm$ under the pairing

$$[,]_n : H^1(\mathbb{Q}_{p,n},T_f(1))\times H^1(\mathbb{Q}_{p,n},T_{\bar f}(k-1)) \to \mathbb{Z}_p. \tag{55}$$

As shown in [Lei09, Section 2.2.4], we have $\ker(\mathrm{Col}^\pm) = \varprojlim_n H^1_\pm(\mathbb{Q}_{p,n},T_{\bar f}(k-1))$. Hence, we can identify the kernels described in Corollary 5.15 with $\ker(\mathrm{Col}^\pm)$ described in [Lei09] via the isomorphism $h^1_{\mathrm{Iw},V_{\bar f}(k-1)}$:

Proposition 5.16. *For any $x \in H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ and $m \le n$, let $e_m(x) = \exp^*_{m,V_{\bar{f}}(k-1)}(\mathrm{cor}_{n/m}(x))$. Then, $H^1_\pm(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ coincides with the following set:*

$$\{x \in H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1)) : e_0(x) = 0 \text{ and } e_m(x) = p^{-1}e_{m-1}(x) \forall m \text{ odd (even)}, m \le n\}$$

Proof. On the one hand, (55) factors through

$$H^1_f(\mathbb{Q}_{p,n}, T_f(1)) \times \frac{H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))}{H^1_f(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))} \to \mathbb{Z}_p.$$

On the other hand, the pairing

$$[\sim,\sim]'_n : \Big(\mathbb{Q}_{p,n} \otimes \mathbb{D}_{\mathrm{cris}}(V_f(1))\Big) \times \Big(\mathbb{Q}_{p,n} \otimes \mathbb{D}_{\mathrm{cris}}(V_{\bar{f}}(k-1))\Big) \to \mathbb{Q}_{p,n} \xrightarrow{\mathrm{Tr}_{n/0}} \mathbb{Q}_p$$

factors through

$$\Big(\mathbb{Q}_{p,n} \otimes \mathbb{D}_{\mathrm{cris}}(V_f(1))/\mathbb{D}^0_{\mathrm{cris}}(V_f(1))\Big) \times \Big(\mathbb{Q}_{p,n} \otimes \mathbb{D}^0_{\mathrm{cris}}(V_{\bar{f}}(k-1))\Big) \to \mathbb{Q}_p.$$

Hence, the compatibility of the two pairings, namely $[\exp_{n,V_f(1)}(\sim),\sim]_n = \mathrm{Tr}_{n/0}[\sim, \exp^*_{n,V_{\bar{f}}(k-1)}(\sim)]'_n$, implies that $H^1_\pm(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ is the $\exp^*_{n,V_{\bar{f}}(k-1)}$-preimage of $\Big(\mathbb{Q}^\pm_{p,n} \otimes \mathbb{D}_{\mathrm{cris}}(V_f(1))/\mathbb{D}^0_{\mathrm{cris}}(V_f(1))\Big)^\perp$ where

$$\mathbb{Q}^\pm_{p,n} = \{x \in \mathbb{Q}_{p,n} : \mathrm{Tr}_{n/m+1}(x) \in \mathbb{Q}_{p,m} \ \forall m \text{ even (odd)}, m < n\}.$$

But we have:

$$\Big(\mathbb{Q}^\pm_{p,n} \otimes \mathbb{D}_{\mathrm{cris}}(V_f(1))/\mathbb{D}^0_{\mathrm{cris}}(V_f(1))\Big)^\perp = \Big(\mathbb{Q}^\pm_{p,n}\Big)^\perp \otimes \mathbb{D}^0_{\mathrm{cris}}(V_{\bar{f}}(k-1))$$

where $\Big(\mathbb{Q}^\pm_{p,n}\Big)^\perp$ is the orthogonal complement of $\mathbb{Q}^\pm_{p,n}$ under the pairing

$$\begin{aligned} \mathbb{Q}_{p,n} \times \mathbb{Q}_{p,n} &\to \mathbb{Q}_p \\ (x,y) &\mapsto \mathrm{Tr}_{n/0}(xy). \end{aligned}$$

By simple linear algebra, we have

$$\Big(\mathbb{Q}^\pm_{p,n}\Big)^\perp = \{x \in \mathbb{Q}_{p,n} : \mathrm{Tr}_{n/0}(x) = 0 \text{ and } \mathrm{Tr}_{n/m+1}(x) \in \mathbb{Q}_{p,m} \ \forall m \text{ odd (even)}, m < n\},$$

hence the lemma. □

5.3. **Elliptic curves with $a_p = 0$.** We now specialize to the case when f corresponds to an elliptic curve E over $\mathbb{Q}$ with $a_p = 0$. Then $V_{\bar{f}}(k-1) = V_f(1) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$, where $T = T_p(E)$. Furthermore, $E[p]$ is irreducible as a mod p representation of $G_{\mathbb{Q}_p}$; thus T is the unique $G_{\mathbb{Q}_p}$-stable lattice in $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(E)$ up to scaling, and in particular we may take the lattice $T_f(1)$ constructed in [BLZ04] (which is only defined up to scaling) to coincide with T.

In this situation, we can recover results of Kobayashi [Kob03] which give a precise description of the images $\mathbb{D}(T)^{\psi=1}$ under the Coleman maps. Recall that if $x \in \mathbb{D}(V)^{\psi=1}$, say $x = (x_1 n_1 + x_2 n_2) \otimes \pi^{-1} e_1$, then we have

$$\begin{aligned} \mathrm{Col}_1(x) &= x_2 - \varphi(x_1) \\ \mathrm{Col}_2(x) &= q x_1 + \varphi(x_1) \end{aligned}$$

where we have replaced Col_2 by $-\mathrm{Col}_2$ for simplicity.

Proposition 5.17. *The map $\mathrm{Col}_1 : \mathbb{D}(T)^{\psi=1} \to (\mathbb{A}^+_{\mathbb{Q}_p})^{\psi=0}$ is surjective.*

Proof. We first show that $\big(\pi\mathbb{A}^+_{\mathbb{Q}_p}\big)^{\psi=0} \subset \mathrm{Im}(\mathrm{Col}_1)$. If $y \in \big(\pi\mathbb{A}^+_{\mathbb{Q}_p}\big)^{\psi=0}$, then the series $\sum_{i\ge1}(-1)^i \frac{\varphi^{2i-1}(y)}{q\ldots\varphi^{2i-2}(q)}$ and $\sum_{i\ge0}(-1)^i \frac{\varphi^{2i}(y)}{\varphi(q)\ldots\varphi^{2i-1}(q)}$ converge in $\mathbb{A}^+_{\mathbb{Q}_p}$ to elements x_1 and x_2, respectively, and it is easy to see that $\psi(qx_2) = -x_1$ and $\psi(x_1) = x_2$. It follows that if we let $x = x_1 \log^-(1+\pi)\nu_1 + x_2 \log^+(1+\pi)\nu_2$, then $x \in \mathbb{D}(T)^{\psi=1}$, and moreover $\mathrm{Col}_1(x) = x_2 - \varphi(x_1) = y$.

In order to prove surjectivity of Col_1, it is hence sufficient to show that there exists $y \in \mathrm{Im}(\mathrm{Col}_1)$ with $y \equiv 1 \mod \pi$. Let $y \in \mathbb{A}_{\mathbb{Q}_p}^{+,\psi=0}$ such that $\pi \mid ((1+\pi)^p + y)$. As above, the series $\sum_{i\geq 1}(-1)^i \frac{\varphi^{2i-1}(y)+\varphi^{2i}(1+\pi)}{q\ldots\varphi^{2i-2}(q)}$ and $\sum_{i\geq 0}(-1)^i \frac{\varphi^{2i}(y)+\varphi^{2i+1}(1+\pi)}{\varphi(q)\ldots\varphi^{2i-1}(q)}$ converge in $\mathbb{A}_{\mathbb{Q}_p}^{+}$. Let

$$z_1 = \frac{1}{2}\left((1+\pi) + \sum_{i\geq 1}(-1)^i \frac{\varphi^{2i-1}(y)+\varphi^{2i}(1+\pi)}{q\ldots\varphi^{2i-2}(q)}\right),$$

$$z_2 = \frac{1}{2}\left(-\psi(q(1+\pi)) + \sum_{i\geq 0}(-1)^i \frac{\varphi^{2i}(y)+\varphi^{2i+1}(1+\pi)}{\varphi(q)\ldots\varphi^{2i-1}(q)}\right).$$

It is easy to see that $\psi^2(q(1+\pi)) = 0$, so $\psi(qz_1) = -z_2$ and $\psi(z_2) = z_1$. It follows that if we let $x = z_1 \log^-(1+\pi)\nu_1 + z_2\log^+(1+\pi)\nu_2$, then $x \in \mathbb{D}(T)^{\psi=1}$, and moreover

$$\mathrm{Col}_1(x) = z_2 - \varphi(z_1) = 1 \mod \pi.$$

□

Corollary 5.18. *The map* $\underline{\mathrm{Col}}_1 : \mathbb{D}(T)^{\psi=1} \to \Lambda(G_\infty)$ *is surjective.*

Proof. By Proposition 5.17, there exists $x \in \mathbb{N}(T)^{\psi=1}$ such that $\mathrm{Col}_1(x) = 1+\pi$. The result therefore follows by precisley the same argument as in the proof of Theorem 4.28. □

Proposition 5.19. *The image of* $\mathrm{Col}_2 : \mathbb{D}(T)^{\psi=1} \to \left(\mathbb{A}_{\mathbb{Q}_p}^{+}\right)^{\psi=0}$ *is equal to* $\left(\mathbb{A}_{\mathbb{Q}_p}^{+,\psi=0}\right)^{\Delta} + \varphi(\pi)\mathbb{A}_{\mathbb{Q}_p}^{+,\psi=0}$.

Proof. A similar argument to the one in the proof of Proposition 4.6 shows that $\varphi(\pi)\mathbb{A}_{\mathbb{Q}_p}^{+,\psi=0} \subset \mathrm{Im}(\mathrm{Col}_2)$. In [Fon90], Fontaine shows that $\left(\mathbb{A}_{\mathbb{Q}_p}^{+}\right)^{\Delta} = \mathbb{Z}_p[[\pi_0]]$, where $\pi_0 = -p + \sum_{a\in\mathbb{F}_p}[\varepsilon]^{[a]}$. Note that $\theta(\pi_0) = 0$ and $\theta \circ \varphi^{-1}(\pi_0) = -p$, so $\pi_0 = -p + \alpha q$ for some $\alpha \in \mathbb{A}_{\mathbb{Q}_p}^{+}$ satisfying $\alpha = 1 \mod \pi$. Now $\{[\varepsilon]^{[a]}\}_{a\in\mathbb{F}_p^\times}$ is a basis for $\mathbb{A}_{\mathbb{Q}_p}^{+}$ over $\varphi(\mathbb{A}_{\mathbb{Q}_p}^{+})$, so $\psi(\pi_0) = 1-p$, and hence $\pi_0 + p - 1 \in \mathbb{A}_{\mathbb{Q}_p}^{+,\psi=0}$. In order to prove that $\left(\mathbb{A}_{\mathbb{Q}_p}^{+,\psi=0}\right)^{\Delta} \subset \mathrm{Im}(\mathrm{Col}_2)$, it is therefore sufficient to prove the following results:

(1) $\pi_0 + p - 1 \in \mathrm{Im}(\mathrm{Col}_2)$;
(2) If $y \in \left(\mathbb{A}_{\mathbb{Q}_p}^{+,\psi=0}\right)^{\Delta}$, then $y = c(\pi_0 + p - 1) \mod \varphi(\pi)$ for some $c \in \mathbb{Z}_p$.

Proof of claim 1. Note that since $\pi_0 + p - 1 = -1 + q \mod \varphi(\pi)$, (a) is equivalent to showing that there exists $y \in \mathrm{Im}(\mathrm{Col}_2)$ such that $y = -1 + q \mod \varphi(\pi)$. If $i(x) = x_1\log^-(1+\pi)\nu_1 + x_2\log^+(1+\pi)\nu_2$ for some $x \in \mathbb{D}(T)^{\psi=1}$, then $\mathrm{Col}_2(x) = qx_1 + \varphi(x_2)$. As shown in Lemma 5.12, we have $\theta(x_1) = -\theta(x_2)$, so

$$\mathrm{Col}_2(x) \equiv \theta(x_2)(1-q) \mod \varphi(\pi).$$

Suppose now that $\theta(x_2) = 0$ for all $x \in \mathbb{D}(T)^{\psi=1}$. Then, the fact that $\mathrm{Col}_1(x) \equiv \theta(x_2) - \theta(x_1) \mod \pi$ implies that $\mathrm{Col}_1(x) \in \pi\mathbb{A}_{\mathbb{Q}_p}^{+}$ for all $x \in \mathbb{D}(T)^{\psi=1}$, which contradicts the surjectivity of Col_1. □

Proof of claim 2. We will show that if $y \in \left(\mathbb{A}_{\mathbb{Q}_p}^{+,\psi=0}\right)^{\Delta}$, then

$$y = c(-1+q) \mod \varphi(\pi) \tag{56}$$

for some $c \in \mathbb{Z}_p$. Write $y = f(\pi_0) = g(\pi)$. In order to show (56), it is sufficient to prove that $g(0) = -(p-1)g(\zeta_p - 1)$. The condition that $y \in \ker(\psi)$ translates as

$$\frac{1}{p}\sum_{\xi^p=1} f\big(-p + \sum_{a\in\mathbb{F}_p}\xi^a(\pi+1)^{[a]}\big) = 0.$$

Evaluating this condition at $\pi = 0$ shows that $f(0) + (p-1)f(-p) = 0$. By definition, we have $\pi_0 = -p + \sum_{a\in\mathbb{F}_p}(\pi+1)^{[a]}$, so $g(0) = f(0)$ and $g(\zeta_p - 1) = f(-p)$, which finishes the proof. □

This completes the proof of proposition 5.19. □

Let $\eta : \Delta \to (\mathbb{Z}/p\mathbb{Z})^\times$ be a tame character. For a $\Lambda(G_\infty)$-module A, denote by A^η the $\Lambda(G_\infty)$-submodule of A on which Δ acts via η. The following result is an immediate consequence of Proposition 5.19.

Corollary 5.20. *We have*

$$\mathrm{Im}(\mathrm{Col}_2)^\eta = \begin{cases} \left(\mathbb{A}_{\mathbb{Q}_p}^{+,\psi=0}\right)^\Delta & \text{if } \eta = 1 \\ \left(\varphi(\pi)\mathbb{A}_{\mathbb{Q}_p}^{+,\psi=0}\right)^\eta & \text{otherwise} \end{cases}$$

We can translate Proposition 5.19 and Corollary 5.20 into a statement about $\mathrm{Im}(\underline{\mathrm{Col}}_2)$.

Proposition 5.21. *The image of $\underline{\mathrm{Col}}_2 : \mathbb{D}(T)^{\psi=1} \to \Lambda(G_\infty)$ is equal to $\left(\sum_{i=1}^{p-1}\delta^i\right)\Lambda(G_\infty) + (\gamma-1)\Lambda(G_\infty)$.*

Proof. Let $y_2 = \varphi(\pi)(1+\pi) \in \mathrm{Im}(\mathrm{Col}_2)$. As shown in the proof of Proposition 5.19, $y = (0, y_2) \in \mathrm{Im}(\mathrm{Col})$; more precisely, there exists $x \in \mathbb{N}(T)^{\psi=1}$ such that $\mathrm{Col}(x) = y$. Applying the algorithm for $\mathfrak{J}$ (see Section 4.4) to y shows that $\underline{\mathrm{Col}}_2(x) = (\gamma - 1) \mod (p, (\gamma-1)^2)$, so the $\Lambda(G_\infty)$-submodule of $\Lambda(G_\infty)$ generated by $\underline{\mathrm{Col}}_2(x)$ is equal to the ideal generated by $(\gamma - 1)$.

Furthermore, $y_2' \sum_{i=1}^{p-1}(\pi+1)^i \in \mathrm{Im}(\mathrm{Col}_2)$ by Proposition 5.19, and every $y \in \mathrm{Im}(\mathrm{Col}_2)$ is congruent to a scalar multiple of $y_2' \mod \varphi(\pi)$. If $x' \in \mathbb{N}(T)^{\psi=1}$ satisfies $\mathrm{Col}_2(x') = y_2'$, then again the algorithm for $\mathfrak{J}$ implies that $\underline{\mathrm{Col}}_2(x) = \sum_{i=1}^{p-1}\delta^i \mod (\gamma - 1)$. This finishes the proof. ∎

Corollary 5.22. *We have*

$$\mathrm{Im}(\underline{\mathrm{Col}}_2)^\eta = \begin{cases} \Lambda(G_\infty)^\Delta = \left(\sum_{i=1}^{p-1}\delta^i\right)\Lambda(G_\infty) & \text{if } \eta = 1 \\ \left((\gamma-1)\Lambda(G_\infty)\right)^\eta & \text{otherwise} \end{cases}$$

Note that the results of Corollaries 5.18 and 5.22 are equivalent to Theorem 6.2 in [Kob03].

5.4. **The case $k = 2$.** In this section we consider the case of modular forms which have weight 2 and are non-ordinary at p. For modular forms with trivial character and coefficients in $\mathbb{Q}$ (hence corresponding to elliptic curves), but with $a_p \neq 0$, this case was studied in detail by Sprung.

5.4.1. *Coleman maps via the Perrin-Riou pairing.* We first review Sprung's construction of the Coleman maps for elliptic curves over $\mathbb{Q}$ with $p \mid a_p$ but $a_p \neq 0$, and explain how we can rewrite these Coleman maps using Perrin-Riou's pairing.

Let f be a modular form as in Section 3.3 with $k = 2$. Define for $n \geq 1$

$$\begin{pmatrix} \Theta_n^1 & \Upsilon_n^1 \\ \Theta_n^0 & \Upsilon_n^0 \end{pmatrix} = \begin{pmatrix} 0 & \Phi_n(\gamma) \\ -1 & a_p \end{pmatrix} \cdots \begin{pmatrix} 0 & \Phi_1(\gamma) \\ -1 & a_p \end{pmatrix} \in M_2(\mathcal{H}(G_\infty)).$$

Then, we have:

Lemma 5.23. *Let $i \in \mathbb{Z}$ and write*

$$A_n^i = \begin{pmatrix} 0 & p \\ -1 & a_p \end{pmatrix}^i \begin{pmatrix} \Theta_n^1 & \Upsilon_n^1 \\ \Theta_n^0 & \Upsilon_n^0 \end{pmatrix}.$$

Then, A_n^{i-n} converges in $M_2(\mathcal{H}(G_\infty))$ as $n \to \infty$ for a fixed i. Write A_∞^i for the limit, then all entries of A_∞^i are $O(\log_p^{1/2})$. Moreover, if η is a character on G_∞ which factors through G_n but not G_{n-1}, then $\eta(A_\infty^i) = \eta(A_m^{i-m})$ for any $m \geq n-1$.

Proof. [Spr09, Lemma 3.21] ∎

Proposition 5.24. *For any $\mathbf{z} \in H^1_{\mathrm{Iw}}(V_{\bar{f}}(1))$ and $0 \neq \omega \in \mathbb{D}^1_{\mathrm{cris}}(V_f)$, the entries of the row vector*

$$\begin{pmatrix} \frac{1}{p}\mathcal{L}_{1,(1+\pi)\otimes\varphi(\omega)}(z) & -\mathcal{L}_{1,(1+\pi)\otimes\omega}(z) \end{pmatrix} A_\infty^{-1}$$

are both divisible by $\log_p(\gamma)/(\gamma-1)$.

Proof. For $n \in \mathbb{Z}$, write $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ where α and β are the roots of $X^2 - a_pX + p$. Then, $\varphi^n = u_n\varphi - pu_{n-1}$ and

$$\begin{pmatrix} 0 & p \\ -1 & a_p \end{pmatrix}^n = \begin{pmatrix} -pu_{n-1} & pu_n \\ -u_n & u_{n+1} \end{pmatrix}.$$

Therefore, if $n > 1$ and η is a character of G_∞ which factors through G_n but not G_{n-1} (so $\eta(\gamma)$ is a primitive p^{n-1}-th root of unity), we have

$$\eta(A_\infty^{-1}) = \begin{pmatrix} -pu_{-n-1} & pu_{-n} \\ -u_{-n} & u_{-n+1} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ -1 & a_p \end{pmatrix} \eta \begin{pmatrix} \Theta_{n-2}^1 & \Upsilon_{n-2}^1 \\ \Theta_{n-2}^0 & \Upsilon_{n-2}^0 \end{pmatrix}$$

where the last matrix is the identity if $n = 2$.

By [Lei09, Section 1.1.4], we have

$$\eta(\mathcal{L}_{1,(1+\pi)\otimes v}(\mathbf{z})) = \frac{1}{\tau(\eta^{-1})} \sum_{\sigma \in G_n} \eta^{-1}(\sigma)[\varphi^{-n}(v), \exp_{n,1}^*(z_n^\sigma)]_n$$

for any $v \in \mathbb{D}_{\mathrm{cris}}(V_f)$ and $z \in H^1_{\mathrm{Iw}}(V_{\bar{f}}(1))$. Hence, if $\omega \in \mathbb{D}^1_{\mathrm{cris}}(V_f)$, then

$$\eta\left(\begin{pmatrix} \frac{1}{p}\mathcal{L}_{1,(1+\pi)\otimes\varphi(\omega)}(z) & -\mathcal{L}_{1,(1+\pi)\otimes\omega}(z) \end{pmatrix} A_\infty^{-1}\right) = 0$$

because

$$\begin{pmatrix} \frac{1}{p}u_{-n+1} & -u_{-n} \end{pmatrix} \begin{pmatrix} -pu_{-n-1} & pu_{-n} \\ -u_{-n} & u_{-n+1} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ -1 & a_p \end{pmatrix} = 0,$$

which implies that

$$\begin{pmatrix} \frac{1}{p}\varphi^{-n+1}(\omega) & -\varphi^{-n}(\omega) \end{pmatrix} \begin{pmatrix} -pu_{-n-1} & pu_{-n} \\ -u_{-n} & u_{-n+1} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ -1 & a_p \end{pmatrix} \equiv 0 \mod \mathbb{D}^1_{\mathrm{cris}}(V_f).$$

□

By [PR94], the image of $\mathcal{L}_{1,(1+\pi)\otimes v}$ is $O(\log_p^{1/2})$ for any $v \in \mathbb{D}_{\mathrm{cris}}(V_f)$, so we obtain two Coleman maps:

Definition 5.25. *Fix a non-zero element $\omega \in \mathbb{D}^1_{\mathrm{cris}}(V_f)$. For $* = \vartheta, \upsilon$ and $z \in H^1_{\mathrm{Iw}}(V_{\bar{f}}(1))$, $\mathrm{Col}^*(z) \in \Lambda_E(G_\infty)$ is defined by*

$$\begin{pmatrix} \mathrm{Col}^\vartheta(z) & \mathrm{Col}^\upsilon(z) \end{pmatrix} \cdot \log_p(\gamma)/p(\gamma - 1) = \begin{pmatrix} \frac{1}{p}\mathcal{L}_{(1+\pi)\otimes\varphi(\omega)}(z) & -\mathcal{L}_{(1+\pi)\otimes\omega}(z) \end{pmatrix} A_\infty^{-1}. \tag{57}$$

In particular, we can define two p-adic L-functions

$$\tilde{L}_p^* = \mathrm{Col}^*(\mathbf{z}^{\mathrm{Kato}}) \in \Lambda_E(G_\infty)$$

where $\mathbf{z}^{\mathrm{Kato}}$ is the localization of the Kato zeta element and $* = \vartheta, \upsilon$.

Remark 5.26. *The results above hold for any modular forms with $k = 2$, $p \nmid N$ and $v_p(a_p) \geq 1/2$. This setting is slightly more general than that in [Spr09].*

5.4.2. *Compatibility of Coleman maps.* Since condition (C) holds and $k = 2$, with respect to the canonical basis of $\mathbb{N}(V_f)$ given above, P is simply

$$\begin{pmatrix} 0 & -1 \\ q & a_p \end{pmatrix}. \tag{58}$$

Write B_∞^i (respectively B_n^i) for the matrix obtained from A_∞^i (respectively A_n^i) by replacing $\Phi_m(\gamma)$ by $\varphi^{m-1}(q)$ for all m. Then, we have:

Lemma 5.27. *Under the notation above, $M' = B_\infty^0$.*

Proof. By (58), $(B_n^{-n})^T = P\varphi(P)\cdots\varphi^{n-1}(P)A_\varphi^{-n}$. For $\gamma \in G_\infty$, we write $G_\gamma^{(n)} = (B_n^{-n})^T \cdot \gamma\left((B_n^{-n})^T\right)^{-1}$. Then,

$$P \cdot \varphi\left(G_\gamma^{(n)}\right) \cdot \gamma(P)^{-1} = G_\gamma^{(n+1)}.$$

Hence, if we write G_γ for the limit of $G_\gamma^{(n)}$ as $n \to \infty$, then

$$P \cdot \varphi\left(G_\gamma\right) \cdot \gamma(P)^{-1} = G_\gamma,$$

It is easy to check that G_γ satisfies $G_{\gamma_1\gamma_2} = G_{\gamma_1} \cdot \gamma_1(G_{\gamma_2})$ for any $\gamma_1, \gamma_2 \in G_\infty$. Hence, we recover the action of G_∞ on the Wach module $\mathbb{N}(V_f)$. In other words, G_γ is the matrix of γ with respect to the basis n_1, n_2 chosen in [BLZ04]. Since $G_\gamma = (B_\infty^0)^T \cdot \gamma\left((B_\infty^0)^T\right)^{-1}$ and $G_\gamma|_{\pi=0} = I$, we have

$$B_\infty^0 \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \left((E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}) \otimes \mathbb{N}(V_f)\right)^{G_\infty} = \mathbb{D}_{\mathrm{cris}}(V_f)$$

and $M' = B_\infty^0$. □

We write $A^c = \det(A)A^{-1}$ if A is an invertible matrix, then we have:

Corollary 5.28. *The matrix M can be obtained from $(A_\infty^{-1})^c$ by replacing Φ_m by $\varphi(q)^m$.*

Proof. Recall that

$$M = \frac{t}{\pi q} P^T (M')^{-1} = \frac{t}{\pi q}\varphi(M'^{-1})A_\varphi^T.$$

By Lemma 5.27, $\det(M') = \det(B_\infty^0) = \prod_{n\geq 0} \frac{\varphi^n(q)}{p} = t/\pi$. But $\det A_{vp} = p$ and $A_\infty^{i+1} = A_\varphi^T A_\infty^i$ for all i. Hence, we have

$$M = \varphi\left((A_\varphi^T)^{-1}B_\infty^0\right)^c = \varphi(B_\infty^{-1})^c$$

and we are done. □

On setting $\nu_1 = -\omega$ in (57), (32) implies that

$$\begin{pmatrix} \underline{\mathrm{Col}}_1 & \underline{\mathrm{Col}}_2 \end{pmatrix} \underline{M} A_\infty^{-1} = \begin{pmatrix} \mathrm{Col}^\vartheta \circ h^1_{\mathrm{Iw}} & \mathrm{Col}^\upsilon \circ h^1_{\mathrm{Iw}} \end{pmatrix} \log_p(\gamma)/p(\gamma-1). \tag{59}$$

By [Spr09],

$$\mathrm{Im}(\mathrm{Col}^\vartheta) = \mathrm{Im}(\mathrm{Col}^\upsilon) = \Lambda_E(G_\infty)$$

and (59) implies that the matrix $\underline{M}A_\infty^{-1}$ defines a $\Lambda_E(G_\infty)$-linear map from $\Lambda_E(G_\infty)^{\oplus 2}$ onto $(\log_p(\gamma)/p(\gamma - 1)\Lambda_E(G_\infty))^{\oplus 2}$. Hence, there exists $A \in GL_2(\Lambda_E(G_\infty))$, $\underline{M}A_\infty^{-1} = [\log_p(\gamma)/p(\gamma-1)]A$. This implies

$$\begin{pmatrix} \underline{\mathrm{Col}}_1 & \underline{\mathrm{Col}}_2 \end{pmatrix} A = \begin{pmatrix} \mathrm{Col}^\vartheta \circ h^1_{\mathrm{Iw}} & \mathrm{Col}^\upsilon \circ h^1_{\mathrm{Iw}} \end{pmatrix}.$$

We also see that $\underline{M}$ and $(A_\infty^{-1})^c$ agree up to an element in $GL_2(\Lambda_E(G_\infty))$ which is a generalization of Proposition 5.10 because of the description of M in Corollary 5.28.

6. Main conjectures

6.1. **Kato's main conjecture.** In general, if V is a p-adic representation of $G_\mathbb{Q}$ unramified outside a finite set of primes, and T is a $\mathbb{Z}_p$-lattice in V stable under $G_\mathbb{Q}$, we write

$$\mathbb{H}^i(T) = \varprojlim_n H^i_{\text{ét}}\left(\operatorname{Spec}\mathbb{Z}[\zeta_{p^n}, \tfrac{1}{p}], j_*T\right),$$

$$\mathbb{H}^i(V) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{H}^i(T).$$

for $i = 1, 2$; see [Kat04, §§8.2 & 12.2]. Here j is the natural map $\operatorname{Spec}\mathbb{Q}(\zeta_{p^n}) \to \operatorname{Spec}\mathbb{Z}[\zeta_{p^n}, \frac{1}{p}]$. Note that $\mathbb{H}^i(V)$ is independent of the choice of lattice T.

We now continue under the notation of Section 3.3 and Section 3.6. Fix a uniformizer ϖ of $\mathcal{O}_E$. Let $\mathbb{Z}(T_f) \subset \mathbb{H}^1(T_f)$ denote the $\Lambda_{\mathcal{O}_E}(G_\infty)$-module generated by the Kato zeta elements as defined in [Kat04, Theorem 12.5] and write $\mathbb{Z}(V_f) = \mathbb{Z}(T_f) \otimes \mathbb{Q}$. The following assumption will be needed for some of the results below.

- **Assumption (E)**: there exists a basis of T_f for which the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_\infty)$ in $\mathrm{GL}_2(\mathcal{O}_E)$ contains $\mathrm{SL}_2(\mathbb{Z}_p)$.

Theorem 6.1 ([Kat04, theorem 12.5]). *Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character, then:*

(a) *$\mathbb{H}^2(T_f)$ is a torsion $\Lambda_{\mathcal{O}_E}(G_\infty)$-module.*
(b) *$\mathbb{H}^1(T_f)$ is a torsion free $\Lambda_{\mathcal{O}_E}(G_\infty)$-module and $\mathbb{H}^1(V_f)$ is a free $\Lambda_E(G_\infty)$-module of rank 1.*
(c) *The quotient $\mathbb{H}^1(V_f)/\mathbb{Z}(V_f)$ is a torsion $\Lambda_E(G_\infty)$-module.*
(d) $\mathrm{Char}_{\Lambda_E(\Gamma)}(\mathbb{H}^1(V_f)^\eta/\mathbb{Z}(V_f)^\eta) \subset \mathrm{Char}_{\Lambda_E(\Gamma)}(\mathbb{H}^2(V_f)^\eta)$.
(e) *If assumption (E) holds, then $\mathbb{Z}(T_f) \subset \mathbb{H}^1(T_f)$. Moreover, $\mathbb{H}^1(T_f)$ is a free $\Lambda_{\mathcal{O}_E}(G_\infty)$-module of rank 1 and*
$$\mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathbb{H}^1(T_f)^\eta/\mathbb{Z}(T_f)^\eta) \subset \mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathbb{H}^2(T_f)^\eta).$$

Kato's main conjecture states that:

Conjecture 6.2. *Let $\eta : \Delta \to \mathbb{Z}_p^\times$ be a character, then $\mathbb{Z}(T_f)^\eta \subset \mathbb{H}^1(T_f)^\eta$ and*
$$\mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathbb{H}^1(T_f)^\eta/\mathbb{Z}(T_f)^\eta) = \mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathbb{H}^2(T_f)^\eta).$$

Remark 6.3. *The above formulation of the conjecture can be found in* [Kob03, §5]*; it is more convenient for our purposes than the original formulation (Conjecture 12.10 of* [Kat04]*).*

6.2. **Reformulation of Kato's main conjecture.** Let K be a number field. The p-Selmer group of f over K is defined by
$$\mathrm{Sel}_p(f/K) = \ker\left(H^1(K, V_f/T_f(1)) \to \prod_\nu \frac{H^1(K_\nu, V_f/T_f(1))}{H^1_f(K_\nu, V_f/T_f(1))}\right)$$
where ν runs through all the places of K.

We choose a "good basis" ν_1, ν_2 of $\mathbb{D}_{\mathrm{cris}}(V_{\bar{f}})$ in the sense of subsection 3.3. Lemma 3.15 shows that we may find a lift n_1, n_2 of this to a basis of $\mathbb{N}(V_{\bar{f}})$ such that $(1+\pi)\varphi(\pi^{1-k}n_1 \otimes e_{k-1}), (1+\pi)\varphi(\pi^{1-k}n_2 \otimes e_{k-1})$ is a Λ_E-basis of $\mathbb{N}(V_{\bar{f}}(k-1))$. We choose such basis (n_1, n_2).

With respect to this basis, we write $H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(1))^i$ for the annihilator of the projection of $\ker(\underline{\mathrm{Col}}_i)$ in $H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ under the pairing
$$H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1)) \times H^1(\mathbb{Q}_{p,n}, V_f/T_f(1)) \to E/\mathcal{O}_E.$$
This enables us to make the following definition:

Definition 6.4.
$$\mathrm{Sel}^i_p(f/\mathbb{Q}(\mu_{p^n})) = \ker\left(\mathrm{Sel}_p(f/\mathbb{Q}(\mu_{p^n})) \to \frac{H^1(\mathbb{Q}_{p,n}, V_f/T_f(1))}{H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(1))^i}\right)$$
$$\mathrm{Sel}^i_p(f/\mathbb{Q}_\infty) = \varinjlim_n \mathrm{Sel}^i_p(f/\mathbb{Q}(\mu_{p^n})).$$

By the Poitou-Tate exact sequence (see [Kob03, Section 7] and [Lei09, Section 4]), we have
$$\mathbb{H}^1(T_{\bar{f}}(k-1)) \to \mathrm{Im}(\underline{\mathrm{Col}}_i) \to \mathrm{Sel}^i_p(f/\mathbb{Q}_\infty)^\vee \to \mathbb{H}^2(T_{\bar{f}}(k-1)) \to 0 \tag{60}$$
where $(\cdot)^\vee$ denotes the Pontryagin dual.

Theorem 6.5. *Under assumption (A) (if f is supersingular at p) or assumption (A') (if f is ordinary at p), $\mathrm{Sel}^i_p(f/\mathbb{Q}_\infty)$ is $\Lambda_{\mathcal{O}_E}(G_\infty)$-cotorsion. Moreover, there exist some $n_i \geq 0$ such that*
$$\varpi^{n_i}\tilde{L}^\eta_{p,i} \in \mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathrm{Sel}^i_p(f/\mathbb{Q}_\infty)^{\vee,\eta})$$
where η is any character on Δ when $i=1$ and it is the trivial character when $i=2$.

Proof. Assume f is supersingular at p. By Corollary 3.29, assumption (A) implies that $\tilde{L}_{p,i}^{\eta} \neq 0$. Hence, the cokernel of the first map in (60) is $\Lambda_{\mathcal{O}_E}(G_\infty)$-torsion. But $\mathbb{H}^2(T_{\bar{f}}(k-1))$ is also $\Lambda_{\mathcal{O}_E}(G_\infty)$-torsion by [Kat04], so $\mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)^\vee$ is $\Lambda_{\mathcal{O}_E}(G_\infty)$-torsion, too.

As in [Kob03, Theorem 7.3], the first arrow of (60) is now injective and there exist $n \geq 0$ such that

$$0 \to \mathbb{H}^1(T_{\bar{f}}(k-1))/\mathbb{Z}(T_{\bar{f}}(k-1)) \to \mathrm{Im}(\underline{\mathrm{Col}}_i)/(\varpi^{n_i}\tilde{L}_{p,i}) \to \mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)^\vee \to \mathbb{H}^2(T_{\bar{f}}(k-1)) \to 0. \tag{61}$$

Hence, the second part of the theorem follows from Theorem 6.1(d) on taking η-components. The proof for the ordinary case is analogous. □

Corollary 6.6. *Let η be a character on Δ as above. If assumptions (A) (or (A') depending on whether f is supersingular or ordinary at p) and (E) hold, then Kato's main conjecture is equivalent to*

$$\mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)^{\vee,\eta}) = \mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathrm{Im}(\underline{\mathrm{Col}}_i)^\eta/(\tilde{L}_{p,i}^{\eta})).$$

Proof. It follows immediately from (61). □

Remark 6.7. *We do* not *assume that n_1, n_2 is an $\mathcal{O}_E \otimes \mathbb{A}_{\mathbb{Q}_p}^+$-basis for $\mathbb{N}(T_{\bar{f}})$. Hence $\mathrm{Im}(\underline{\mathrm{Col}}_i)$ need not be contained in $\Lambda_{\mathcal{O}_E}(G_\infty)$; but it is still clearly a $\Lambda_{\mathcal{O}_E}(G_\infty)$-submodule of $\Lambda_E(G_\infty)$.*

By Theorem 4.28, if f is supersingular at p, then assumptions (B), (C) and (D) imply that $\mathrm{Im}(\underline{\mathrm{Col}}_1) = \Lambda_E(G_\infty)$. Therefore, we can reformulate Kato's main conjecture in the following form:

Corollary 6.8. *If f is supersingular at p and assumptions (A)-(D) all hold, then Kato's main conjecture (after tensoring by $\mathbb{Q}$) is equivalent to the assertion that $\mathrm{Char}_{\Lambda_E(\Gamma)}(\mathrm{Sel}_p^1(f/\mathbb{Q}_\infty)^{\vee,\eta})$ is generated by $\tilde{L}_{p,1}^{\eta}$.*

Acknowledgements

We would like to thank John Coates and Tony Scholl for their interest and encouragement and Laurent Berger for sending us his proof of Theorem 3.5 and for answering our questions about Wach modules. The ideas of the paper were developed while the third author was visiting the Newton Institute in Cambridge in autumn 2009. She would like to thank the organizers of the programme on 'Non-abelian fundamental groups' for their hospitality. We are also grateful to the anonymous referee for his or her extremely careful reading of the paper and numerous helpful comments.

References

[AV75] Yvette Amice and Jacques Vélu, *Distributions p-adiques associées aux séries de Hecke*, Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, 1974), Astérisque, vol. 24-25, Soc. Math. France, Paris, 1975, pp. 119–131.

[Ber02] Laurent Berger, *Représentations p-adiques et équations différentielles*, Invent. Math. **148** (2002), no. 2, 219–284.

[Ber03] ———, *Bloch and Kato's exponential map: three explicit formulas*, Doc. Math. Extra Vol. **3** (2003), 99–129, Kazuya Kato's fiftieth birthday.

[Ber04] ———, *Limites de représentations cristallines*, Compos. Math. **140** (2004), no. 6, 1473–1498.

[BB10] Laurent Berger and Christophe Breuil, *Sur quelques représentations potentiellement cristallines de* $\mathrm{GL}_2(\mathbf{Q}_p)$, Astérisque **330** (2010), 155–211.

[BLZ04] Laurent Berger, Hanfeng Li, and Hui June Zhu, *Construction of some families of 2-dimensional crystalline representations*, Math. Ann. **329** (2004), no. 2, 365–377.

[CC99] Frédéric Cherbonnier and Pierre Colmez, *Théorie d'Iwasawa des représentations p-adiques d'un corps local*, J. Amer. Math. Soc. **12** (1999), no. 1, 241–268.

[Col10] Pierre Colmez, *Fonctions d'une variable p-adique*, Astérisque **330** (2010), 13–59.

[Del69] Pierre Deligne, *Formes modulaires et représentations ℓ-adiques*, Séminaire Bourbaki **11** (1968/69), Exp. No. 355, 139–172.

[Fon90] Jean-Marc Fontaine, *Représentations p-adiques des corps locaux. I*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 249–309.

[Kat93] Kazuya Kato, *Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via* B_{dR}*. I*, Arithmetic algebraic geometry (Trento, 1991), Lecture Notes in Math., vol. 1553, Springer, Berlin, 1993, pp. 50–163.

[Kat04] ———, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), ix, 117–290, Cohomologies p-adiques et applications arithmétiques. III.

[Kob03] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36.

[Lei09] Antonio Lei, *Iwasawa theory for modular forms at supersingular primes*, to appear in Compos. Math., 2009, `arXiv:0904.3938`.

[LLZ10] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Coleman maps and the p-adic regulator*, preprint, 2010, `arXiv:1006.5163`.

[LZ10] Antonio Lei and Sarah Livia Zerbes, *The $\mathfrak{M}_H(G)$-conjecture for supersingular elliptic curves*, in preparation, 2010.

[MSD74] Barry Mazur and Peter Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

[MTT86] Barry Mazur, John Tate, and Jeremy Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48.

[PR93] Bernadette Perrin-Riou, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 4, 945–995.

[PR94] ———, *Théorie d'Iwasawa des représentations p-adiques sur un corps local*, Invent. Math. **115** (1994), no. 1, 81–161, With an appendix by Jean-Marc Fontaine.

[PR95] ———, *Fonctions L p-adiques des représentations p-adiques*, Astérisque **229** (1995), 1–198.

[PR01] ———, *Théorie d'Iwasawa des représentations p-adiques semi-stables*, Mém. Soc. Math. Fr. (N.S.) **84** (2001), 1–111.

[Pol03] Robert Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558.

[PoR04] Robert Pollack and Karl Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, Ann. of Math. (2) **159** (2004), no. 1, 447–464.

[PoS09] Robert Pollack and Glenn Stevens, *Critical slope p-adic l-functions*, preprint, 2009.

[Sch90] Anthony Scholl, *Motives for modular forms*, Invent. Math. **100** (1990), no. 2, 419–430.

[Shi76] Goro Shimura, *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. **29** (1976), no. 6, 783–804.

[Spr09] Ian Sprung, *Iwasawa theory for elliptic curves at supersingular primes: beyond the case $a_p = 0$*, preprint, 2009, `arXiv:0903.3419`.

[Viš76] Misha Višik, *Nonarchimedean measures associated with Dirichlet series*, Mat. Sb. (N.S.) **99(141)** (1976), no. 2, 248–260, 296.

[Wac96] Nathalie Wach, *Représentations p-adiques potentiellement cristallines*, Bull. Soc. Math. France **124** (1996), no. 3, 375–400.

(Lei) Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Cambridge CB3 0WB, UK

Current address: School of Mathematical Sciences, Monash University, Clayton, VIC 3800, Australia

E-mail address: `antonio.lei@monash.edu`

(Loeffler) Warwick Mathematics Institute, Zeeman Building, University of Warwick, Coventry CV4 7AL, UK

E-mail address: `d.loeffler.01@cantab.net`

(Zerbes) Department of Mathematics, Harrison Building, University of Exeter, Exeter EX4 4QF, UK

E-mail address: `s.zerbes@exeter.ac.uk`