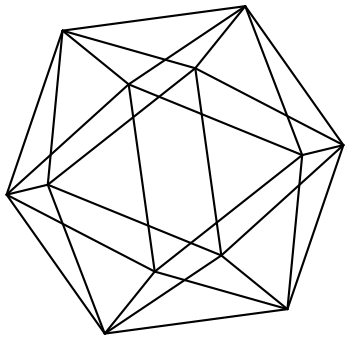
Max-Planck-Institut für Mathematik Bonn

Integral Iwasawa theory of Galois representations for non-ordinary primes

by

Kâzim Büyükboduk
Antonio Lei



Max-Planck-Institut für Mathematik
Preprint Series 2014 (37)

Integral Iwasawa theory of Galois representations for non-ordinary primes

Kâzim Büyükboduk
Antonio Lei

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Koç University
Mathematics
Rumeli Feneri Yolu
34450 Sariyer, Istanbul
Turkey

Department of Mathematics and Statistics
Burnside Hall
McGill University
Montreal, QC H3A 0B9
Canada

MPIM 14-37

INTEGRAL IWASAWA THEORY OF GALOIS REPRESENTATIONS FOR NON-ORDINARY PRIMES

KÂZIM BÜYÜKBODUK AND ANTONIO LEI

Abstract. In this paper, we study the Iwasawa theory of a motive at a non-ordinary prime, over the cyclotomic tower of a number field that is either totally real or CM. In particular, under certain technical assumptions, we construct Sprung-type Coleman maps on the local Iwasawa cohomology groups and use them to define (conjectural) integral p-adic L-functions and cotorsion Selmer groups. This allows us to reformulate Perrin-Riou's main conjecture in terms of these objects, in the same fashion as Kobayashi's $\pm$-Iwasawa theory for supersingular elliptic curves. By the aid of the rank-r Euler system machinery adapted to this setting, we deduce parts of Perrin-Riou's main conjecture from her special element conjecture.

1. Introduction

Fix forever an odd rational prime p. Let F be either a totally real or a CM number field which is unramified at all primes above p. Let $\mathcal{M}_{/F}$ be a motive defined over F which has coefficients in $\mathbb{Q}$. The goal of this article is to study the cyclotomic Iwasawa theory of $\mathcal{M}$ for primes p such that the p-adic realization of $\mathcal{M}$ is crystalline but non-ordinary, much in the spirit of the integral theory initiated by Pollack [Pol03] and Kobayashi [Kob03].

The archetypical example of a motive that fits in our treatment is the motive associated to an abelian variety A defined over F which has supersingular reduction at all primes above p. In the case when $F = \mathbb{Q}$ and the variety A is one-dimensional (i.e., an elliptic curve) the works of Kobayashi [Kob03] and Pollack [Pol03] provides us with a satisfactory set of results. Our initial objective writing this article and its companion [BL14] was to extend their work to the general study of supersingular abelian varieties.

We first follow the ideas due to Sprung [Spr12] to construct *signed* Coleman maps (in §2.3 below) for a class of p-adic Galois representations that verify certain conditions. We incorporate this construction with Perrin-Riou's (conjectural) treatment of p-adic L-functions so as to

- provide a definition of the signed (integral) p-adic L-functions attached to motives at non-ordinary primes (see particularly Definition 3.15 and Theorem 3.17), conditional on the existence of Perrin-Riou's special element;

The first author is partially supported by the Turkish Academy of Sciences, TÜBİTAK and FONDECYT. The second author is supported by a CRM-ISM postdoctoral fellowship.

- formulate a signed main conjecture in this setting (Conjecture 3.32) that is equivalent to Perrin-Riou's main conjecture [PR95, §4];
- utilizing the rank-r Euler system machinery developed in our companion article [BL14] and assuming the *special element conjecture* (Conjecture 3.22 below) of Perrin-Riou, verify one containment of the signed main conjecture (see Theorem 3.35) and deduce a similar result on Perrin-Riou's main conjecture.

We shall explain our results in detail below. Let us first introduce some notation.

1.1. **Setup and notation.** For any field k, let $\overline{k}$ denote a fixed separable closure of k and $G_k := \mathrm{Gal}(\overline{k}/k)$ denote its absolute Galois group. Fix forever a G_F-stable $\mathbb{Z}_p$-lattice contained inside $\mathcal{M}_p$, the p-adic realization of $\mathcal{M}$. Let $\mathcal{M}^*(1)$ denote the dual motive.

Let $g := \dim_{\mathbb{Q}_p}\left(\mathrm{Ind}_{F/\mathbb{Q}}\mathcal{M}_p\right)$ and let $g_+ := \dim_{\mathbb{Q}_p}\left(\mathrm{Ind}_{F/\mathbb{Q}}\mathcal{M}_p\right)^+$, the dimension of the $+1$-eigenspace under the action of a fixed complex conjugation on $\mathrm{Ind}_{F/\mathbb{Q}}\mathcal{M}_p$. Set $g_- = g - g_+$. Similarly for any prime $\mathfrak{p}$ of F above p, define $g_{\mathfrak{p}} := \dim_{\mathbb{Q}_p}\left(\mathrm{Ind}_{F_{\mathfrak{p}}/\mathbb{Q}_p}\mathcal{M}_p\right)$ so that $g = \sum_{\mathfrak{p}|p} g_{\mathfrak{p}}$.

Let $T = \mathcal{M}_p$. For any unramified extension K of $\mathbb{Q}_p$ that contains F, we write $\mathbb{D}_K(T)$ for its Dieudonné module and fix a $\mathbb{Z}_p$-basis $\mathfrak{B} = \{v_i\}$ of this module.

1.1.1. *Iwasawa algebras.* Let Γ be the Galois group $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$. Given any unramified extension K of $\mathbb{Q}_p$, we shall abuse notation and write Γ for the Galois group $\mathrm{Gal}(K(\mu_{p^\infty})/K)$ as well. We may decompose Γ as $\Delta \times \overline{\langle\gamma\rangle}$, where Δ is cyclic of order $p-1$ and $\overline{\langle\gamma\rangle}$ is isomorphic to the additive group $\mathbb{Z}_p$. We write Λ for the Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$. We may identify it with the set of power series $\sum_{n\geq 0,\sigma\in\Delta} a_{n,\sigma}\cdot\sigma\cdot(\gamma-1)^n$ where $a_{n,\sigma}\in\mathbb{Z}_p$. We shall identify $\gamma-1$ with the indeterminate X.

For $n\geq 0$, we write $\mathbb{Q}_{p,n} = \mathbb{Q}_p(\mu_{p^n})$ and $G_n = \mathrm{Gal}(\mathbb{Q}_{p,n}/\mathbb{Q}_p)$. Denote $\mathbb{Z}_p[G_n]$ by Λ_n. We have in particular $\Lambda = \varprojlim \Lambda_n$. For any field k, define $H^1_{\mathrm{Iw}}(k,T)$ to be $\varprojlim H^1(k(\mu_{p^n}),T)$, where the limit is taken with respect to the corestriction maps.

We define $\mathcal{H}$ to be the set of elements $\sum_{n\geq 0,\sigma\in\Delta} a_{n,\sigma}\cdot\sigma\cdot(\gamma-1)^n$ where $a_{n,\sigma}\in\mathbb{Q}_p$ are such that the power series $\sum_{n\geq 0} a_{n,\sigma}X^n$ converges on the open unit disc for all $\sigma\in\Delta$.

Let $|\bullet|_p$ denote the normalised p-adic norm with $|p|_p = 1/p$. For a real number $h\geq 0$ and an element $F = \sum_{n\geq 0,\sigma\in\Delta} a_{n,\sigma}\cdot\sigma\cdot(\gamma-1)^n \in \mathcal{H}$, if $\sup_{n\geq 1}\frac{|a_{n,\sigma}|_p}{n^h} < \infty$ for all $\sigma\in\Delta$, we say that F is $O(\log^h)$.

1.1.2. *Isotypic components and characteristic ideals.* Let M be a Λ-module, η a Dirichlet character modulo p. We write $e_\eta = \frac{1}{p-1}\sum_{\sigma\in\Delta}\eta(\sigma)^{-1}\sigma \in \mathbb{Z}_p[\Delta]$. The η-isotypic component of M is defined to be $e_\eta\cdot M$ and denoted by M^η. Note that we may regard M^η as a $\mathbb{Z}_p[[X]]$-module.

Following [PR95], we write e_+ and e_- for the idempotents $(1+c)/1$ and $(1-c)/2$ respectively, where c is the complex conjugation of Δ. For any Λ-module M, we write $M_\pm = e_\pm M$.

Given an element $F = \sum_{n\geq 0,\sigma\in\Delta} a_{n,\sigma}\cdot\sigma\cdot(\gamma-1)^n$ of $\mathcal{H}$, we shall identify $e_\eta\cdot F$ with the element

$$\sum_{n\geq 0}\left(\sum_{\sigma\in\Delta} a_{n,\sigma}\eta(\sigma)\right)X^n \in \mathbb{Q}_p[[X]].$$

Given a torsion $\mathbb{Z}_p[[X]]$-module N, we write $\mathrm{char}_{\mathbb{Z}_p[[X]]}N$ for its characteristic ideal.

1.2. **Statements of the results.**

Theorem 1.1 (Corollary 2.12 and (8) below)**.** *Let $\mathfrak{p}$ be a prime of F above p. Fix a $\mathbb{Z}_p$-basis $\{v_i\}$ of $\mathbb{D}_{F_\mathfrak{p}}(T)$. Assume that the Hodge-Tate weights of $T|F_\mathfrak{p}$ are inside $\{0,1\}$ and that the Frobenius on $\mathbb{D}_{F_\mathfrak{p}}(T)$ have slope inside $(-1,0]$ and 1 is not an eigenvalue. There exists a Λ-module homomorphism*

$$\mathrm{Col}_{T|F_\mathfrak{p}} : H^1_{\mathrm{Iw}}(F_\mathfrak{p},T)\longrightarrow \Lambda^{\oplus g_\mathfrak{p}}$$

and a matrix $M_{T|F_\mathfrak{p}}\in M_{g_\mathfrak{p}\times g_\mathfrak{p}}(\mathcal{H})$ such that we have the following decomposition of Perrin-Riou's regulator map $\mathcal{L}_T^{F_\mathfrak{p}}$ (defined as in §2.1 below):

$$\mathcal{L}_T^{F_\mathfrak{p}} = \begin{pmatrix} v_1 & \cdots & v_{g_\mathfrak{p}}\end{pmatrix}\cdot M_{T|F_\mathfrak{p}}\cdot \mathrm{Col}_{T|F_\mathfrak{p}}\,.$$

See §2.4 and Corollary 3.26 for a detailed discussion on the kernels and images of the Coleman maps $\mathrm{Col}_{T|F_\mathfrak{p}}$.

In addition to the assumptions on T above, assume that the following hypotheses hold true:

(H.Leop) T satisfies the weak Leopoldt conjecture, as stated in [PR95, §1.3].
(H.nA) For every prime $\mathfrak{p}$ of F above p. we have

$$H^0(F_\mathfrak{p},T/pT) = H^2(F_\mathfrak{p},T/pT) = 0\,.$$

Let $\mathbb{D}_p(T)$ be the direct sum $\oplus_{\mathfrak{p}|p}\mathbb{D}_{F_\mathfrak{p}}(T)$. We assume until the end that the following form of the *Panchishkin condition* holds true:

(H.P.) $\dim\left(\mathrm{Fil}^0\mathbb{D}_p(T)\otimes\mathbb{Q}_p\right) = g_-\,.$

Remark 1.2. *Note that the hypotheses* (H.nA) *and* (H.P.) *hold true for the p-adic Tate-module of an abelian variety defined over F. The hypothesis* (H.Leop) *is expected to hold for any T.*

Let $\underline{I}\subset\{1,\cdots,g\}$ be any subset of size g_-. Using the Coleman maps $\mathrm{Col}_{T|F_\mathfrak{p}}$, we may define (see Definiton 3.15) the *signed* (integral) p-adic L-function

$$L_{\underline{I}}(\mathcal{M}^*(1))\in\Lambda\,.$$

We do not provide its precise definition here in the introduction but contend ourselves to the remark that its definition relies on the truth of Perrin-Riou's *Special Element Conjecture* (Conjecture 3.22), which we implicitly assume henceforth in this introduction. We may also use the Coleman maps to define the *modified Selmer groups* $\mathrm{Sel}_{\underline{I}}(T^\vee/F(\mu_{p^\infty}))$ as in Definition 3.29.

Theorem 1.3 (Theorem 3.34 below)**.** *For every even Dirichlet character η of Δ and every $\underline{I}$ as above, the following assertion is equivalent to η-part of Perrin-Riou's Main Conjecture 3.7:*

$$\text{(1)} \qquad \mathrm{char}_{\mathbb{Z}_p[[X]]}\mathrm{Sel}_{\underline{I}}(T^\vee/F(\mu_{p^\infty}))^{\vee,\eta} = \left(L_{\underline{I}}(\mathcal{M}^*(1))^\eta/X^{n(\underline{I},\eta)}\right)\mathbb{Z}_p[[X]]$$

where $n(\underline{I},\eta)\in\mathbb{Z}_{\geq 0}$ is as in Lemma 3.14.

The assertion (1) in the statement of Theorem 1.3 will be referred to as the *signed main conjecture*.

Using the *rank-g_- Euler system machinery* developed in [BL14, Appendix B] (which in turn builds on the methods of [Büy10, Büy13]) we prove the following regarding the η-part of Perrin-Riou's conjecture:

Theorem 1.4 (See Corollary 3.36 and its proof below)**.** *Under the hypotheses of Theorem 1.3 and the hypotheses* **(H1)-(H4)** *of* [MR04, §3.5] *on T, the containment*

$$\left(L_{\underline{I}}(\mathcal{M}^*(1))^\eta/X^{n(\underline{I},\eta)}\right)\mathbb{Z}_p[[X]] \subset \mathrm{char}_{\mathbb{Z}_p[[X]]}\mathrm{Sel}_{\underline{I}}(T^\vee/F(\mu_{p^\infty}))^{\vee,\eta}$$

in (1) *and the containment*

$$\text{(2)} \qquad e_\eta\cdot L_p(A^\vee)\cdot\Lambda \subset e_\eta\cdot\mathbb{I}_{\mathrm{arith}}(A)$$

in the statement of Perrin-Riou's Main Conjecture 3.7 hold true for every even Dirichlet character η of Δ.

Remark 1.5. *See* [BL14] *for an example where we obtain an explicit version of Theorem 1.4. In loc.cit., we study more closely the motive attached to the Hecke character associated to a CM abelian variety that has supersingular reduction at all primes above p. In this particular case, the hypotheses* **(H1)-(H4)** *of* [MR04, §3.5], (H.F.-L.), (H.S.), (H.P.) *and* (H.nA) *hold true. The (conjectural) special elements in that setting are expected to be a form of (conjectural) Rubin-Stark elements.*

Remark 1.6. *In order to deduce the containment* (2) *for odd characters η of Δ, one needs to replace g_- with g_+ everywhere. Note also that upon studying the motive $\mathcal{M}\otimes\omega$ (where ω is the Teichmüller character) in place of $\mathcal{M}$, one may reduce the consideration for odd characters to the case of even characters.*

To deduce the assertion (2) for every character η of Δ (and therefore, by the semi-simplicity of $\mathbb{Z}_p[\Delta]$, to conclude with the containment $\Lambda\cdot L_p(A^\vee)\subset\mathbb{I}_{\mathrm{arith}}(A)$ in Conjecture 3.7), we would need in our proof that $g_- = g_+$, as a result of our running hypothesis (H.P.)*. Note that this condition holds true for motives associated to abelian varieties.*

2. Construction of Coleman maps

In this section, we generalize the construction of *signed* Coleman maps in [Kob03, Spr12] to higher dimensional p-adic representations that satisfy certain hypotheses. This maps decompose the regulator maps of Perrin-Riou, which we recall below.

2.1. **Perrin-Riou's regulator map.** Let T be a free $\mathbb{Z}_p$-module of rank d that is equipped with a crystalline continuous action by the absolute Galois group of a finite unramified extension K of $\mathbb{Q}_p$ whose Hodge-Tate weights are all non-negative.

Let $r = [K : \mathbb{Q}_p]$. Recall that we write $\mathbb{D}_K(T)$ for its Dieudonné module and $H^1_{\mathrm{Iw}}(K,T) := \varprojlim H^1(K(\mu_{p^n}),T)$.

Let

$$\langle \sim, \sim \rangle_n : H^1((K(\mu_{p^n}),T) \times H^1((K(\mu_{p^n}),T^*(1)) \to \mathbb{Z}_p$$

be the local Tate pairing for $n \geq 0$. This gives a pairing

$$\begin{aligned}\langle \sim, \sim \rangle : H^1_{\mathrm{Iw}}(K,T) \times H^1_{\mathrm{Iw}}(K,T^*(1)) &\to \Lambda \\ ((x_n)_n,(y_n)_n) &\mapsto \left(\sum_{\sigma \in G_n} \langle x_n, y_n^\sigma \rangle_n \cdot \sigma \right)_n,\end{aligned}$$

which can be extended $\mathcal{H}$-linearly to a pairing

$$\langle \sim, \sim \rangle : \mathcal{H} \otimes_\Lambda H^1_{\mathrm{Iw}}(K,T) \times \mathcal{H} \otimes_\Lambda H^1_{\mathrm{Iw}}(K,T^*(1)) \to \mathcal{H}.$$

Assume that the eigenvalues of φ on $\mathbb{D}_K(T)$ are not powers of p. Let

$$\mathcal{L}^K_T : H^1_{\mathrm{Iw}}(K,T) \to \mathcal{H} \otimes_{\mathbb{Z}_p} \mathbb{D}_K(T)$$

be Perrin-Riou's p-adic regulator given as in [LLZ11, Definition 3.4]. We may describe this map concretely in the following way. Fix a $\mathbb{Z}_p$-basis $v_1, \dots, v_{rd}$ of $\mathbb{D}_K(T)$ and let $v'_1, \dots, v'_{rd}$ be the dual basis of $\mathbb{D}_K(T^*(1))$. For $i \in \{1, \dots, rd\}$, we write $\mathcal{L}^K_{T,i} : H^1_{\mathrm{Iw}}(T) \to \mathcal{H}$ for the map obtained by composing $\mathcal{L}^K_T$ and the projection of $\mathcal{H} \otimes \mathbb{D}_K(T)$ to the v_i-component. The Colmez-Perrin-Riou reciprocity law (stated in [PR94] and proved in [Col98]) implies that

$$\mathcal{L}^K_{T,i}(z) = \langle z, \Omega_{T^*(1)}(v'_i) \rangle,$$

where $\Omega_{T^*(1)}$ is the Perrin-Riou exponential map

$$\Omega_{T^*(1)} : \mathcal{H} \otimes_{\mathbb{Z}_p} \mathbb{D}(T^*(1)) \to \mathcal{H} \otimes_{\mathbb{Z}_p} H^1_{\mathrm{Iw}}(T^*(1))$$

defined in [PR94]. Note that our assumption on the eigenvalues of φ means that we may state the properties of Perrin-Riou's exponential map in a slightly simpler way than [PR94]. Recall that if θ is a Dirichlet character of conductor p^n, [Lei11, Lemma 3.5] implies that

$$\theta(\mathcal{L}^K_{T,i}(z)) = \begin{cases} \left[\exp^*_0(z), (1-p^{-1}\varphi^{-1})(1-\varphi)^{-1} v'_i\right] & \text{if } n = 0, \\ \frac{1}{\tau(\theta^{-1})} \left[\sum_{\sigma \in G_n} \theta^{-1}(\sigma) \exp^*_n(z^\sigma), \varphi^{-n}(v'_i)\right] & \text{otherwise} \end{cases} \tag{3}$$

where $[\sim, \sim]$ is the natural pairing

$$\mathbb{D}_K(T) \times \mathbb{D}_K(T^*(1)) \to \mathbb{Z}_p,$$

which is extended linearly to

$$\mathbb{Q}_{p,n} \otimes_{\mathbb{Z}_p} \mathbb{D}_K(T) \times \mathbb{Q}_{p,n} \otimes_{\mathbb{Z}_p} \mathbb{D}_K(T^*(1)) \to \mathbb{Q}_{p,n}.$$

In order to define the *signed* Coleman maps, we assume further that T verifies the following conditions.

(H.F.-L.) The Hodge-Tate weights of T are 0 and 1.

(H.S.) The slopes of φ on $\mathbb{D}_K(T)$ lie in the interval $(-1,0]$ and 1 is not an eigenvalue.

Remark 2.1. *These hypotheses are satisfied by the p-adic Tate module of an abelian variety which has supersingular reduction at all primes above p.*

Remark 2.2. *The hypothesis (H.F.-L.) implies that T is Fontaine-Laffaille. Hence,*

$$\varphi(\mathbb{D}_K(T)) \subset \frac{1}{p}\mathbb{D}_K(T) \quad \textit{and} \quad \varphi(\mathrm{Fil}^0\,\mathbb{D}_K(T)) \subset \mathbb{D}_K(T) \tag{4}$$

Moreover,

$$\mathbb{D}_K(T) = p\varphi(\mathbb{D}_K(T)) + \varphi(\mathrm{Fil}^0\,\mathbb{D}_K(T)) \tag{5}$$

2.2. **Logarithmic matrix.** We fix a $\mathbb{Z}_p$-basis $v_1, v_2, \dots, v_{rd}$ of $\mathbb{D}_K(T)$ such that $v_1, \dots, v_{rd_0}$ is a basis of $\mathrm{Fil}^0\,\mathbb{D}_K(T)$. Let C_φ be the matrix of φ with respect to this basis. By (4) and (5), C_φ is of the form

$$\left(\begin{array}{c|c} I_{rd_0} & 0 \\ \hline 0 & \frac{1}{p} I_{r(d-d_0)} \end{array}\right) C \tag{6}$$

for some $C \in \mathrm{GL}_{rd}(\mathbb{Z}_p)$.

For $n \geq 1$, we write $\Phi_{p^n}(1+X)$ for the cyclotomic polynomial

$$\sum_{i=0}^{p-1} (1+X)^{ip^{n-1}}$$

and $\omega_n(X) = (1+X)^{p^n} - 1$.

Definition 2.3. *For $n \geq 1$, we define*

$$C_n = C^{-1} \left(\begin{array}{c|c} I_{rd} & 0 \\ \hline 0 & \Phi_{p^n}(1+X) I_{r(d-d_0)} \end{array}\right) \quad \textit{and} \quad M_n = (C_\varphi)^{n+1}\, C_n \cdots C_1.$$

Proposition 2.4. *The sequence of matrices $\{M_n\}_{n\geq 1}$ converges entry-wise with respect to the sup-norm topology on $\mathcal{H}$. If M_T denotes the limit of the sequence, each entry of M_T are $o(\log)$. Moreover, $\det(M_T)$ is, up to a constant in $\mathbb{Z}_p^\times$, equal to $\left(\frac{\log(1+X)}{pX}\right)^{r(d-d_0)}$.*

Proof. For all $m > n$, we have

$$\Phi_{p^m}(1+X) \equiv p \mod \omega_n,$$

which implies that

$$C_m \equiv (C_\varphi)^{-1} \mod \omega_n.$$

Therefore, we deduce that

$$M_m \equiv M_n \mod \omega_n.$$

Note that all entries of $C_1 \cdots C_n$ are in $\mathbb{Z}_p[[X]]$. By (H.S.), there exists a constant $m < 1$ such that $v_p(\alpha) \geq -m$ for all eigenvalues of α of C_φ. Therefore, all entries of $(C_\varphi)^{n+1}$ are in $\frac{R}{p^{mn}}\mathbb{Z}_p$ for some constant R. The coefficients of the entries of M_n are $O(p^{-mn})$, so the result follows from [PR94, §1.2.1]. □

Remark 2.5. *The matrix M_T is uniquely determined by the matrix C.*

2.3. **Decomposing Perrin-Riou's regulator map.** We shall use the matrix M_T to decompose Perrin-Riou's regulator map in the following sense. For all $z \in H^1_{\mathrm{Iw}}(K,T)$, we shall find $\mathrm{Col}^K_T(z) \in \Lambda^{\oplus rd}$ such that

$$\mathcal{L}^K_T(z) = \begin{pmatrix} v_1 & \cdots & v_{rd} \end{pmatrix} \cdot M_T \cdot \mathrm{Col}^K_T(z).$$

Throughout this section, we shall fix an element $z \in H^1_{\mathrm{Iw}}(K,T)$. Its image under Perrin-Riou's regulator has the following interpolation properties.

Lemma 2.6. *If θ is a Dirichlet character of conductor p^n, then*

$$\theta(\mathcal{L}^K_T(z)) = \begin{cases} \sum_{i=1}^{rd} [\exp_0^*(z), v_i'] \, (1-\varphi)(1-p^{-1}\varphi^{-1})^{-1}(v_i) & \text{if } n = 0, \\ \frac{p^n}{\tau(\theta^{-1})} \sum_{i=1}^{rd} \left[\sum_{\sigma \in G_n} \theta^{-1}(\sigma) \exp_n^*(z^\sigma), v_i'\right] \varphi^n(v_i) & \text{otherwise.} \end{cases}$$

Proof. Note that the adjoints of $(1-p^{-1}\varphi^{-1})(1-\varphi)^{-1}$ and φ^{-1} under $[\sim,\sim]$ are $(1-\varphi)(1-p^{-1}\varphi^{-1})^{-1}$ and $p\varphi$ respectively. Hence, the result follows from (3). □

Proposition 2.7. *For $n \geq 1$, there exists a unique $\mathcal{L}^{(n)}_T(z) \in \Lambda_n \otimes_{\mathbb{Z}_p} \mathbb{D}_K(T)$ such that*

$$\varphi^{-n-1}\left(\mathcal{L}^K_T(z)\right) \equiv \mathcal{L}^{(n)}_T(z) \mod \omega_n.$$

Proof. It is enough to show that for all Dirichlet characters θ of conductor p^m with $m \leq n+1$, $\theta\left(\varphi^{-n-1}\left(\mathcal{L}^K_T(z)\right)\right)$ is p-adically integral.

If $m = 0$, we have

$$\begin{aligned} \theta\left(\varphi^{-n-1}\left(\mathcal{L}^K_T(z)\right)\right) &= \sum_{i=1}^{rd} [\exp_0^*(z), v_i'] \, (1-\varphi)(1-p^{-1}\varphi^{-1})^{-1}\varphi^{-n-1}(v_i) \\ &= \sum_{i=1}^{rd} [\exp_0^*(z), v_i'] \, (\varphi^{-1}-1)(\varphi-p^{-1})^{-1}\varphi^{-n+1}(v_i). \end{aligned}$$

(H.S.) implies that the slope of $(\varphi^{-1}-1)(\varphi-p^{-1})^{-1}\varphi^{-n+1}$ on $\mathbb{D}_K(T)$ is positive, so $\theta\left(\varphi^{-n-1}\left(\mathcal{L}^K_T(z)\right)\right) \in \mathbb{D}_K(T)$.

If $m \geq 1$, then

$$\theta\left(\varphi^{-n-1}\left(\mathcal{L}^K_T(z)\right)\right) = \frac{p^m}{\tau(\theta^{-1})} \sum_{i=1}^{rd} \left[\sum_{\sigma \in G_m} \theta^{-1}(\sigma) \exp_m^*(z^\sigma), v_i'\right] \varphi^{m-n-1}(v_i).$$

Since φ^{m-n-1} has positive slope on $\mathbb{D}_K(T)$, we have $\varphi(v_i) \in \mathbb{D}_K(T)$. All the other terms are p-adically integral, so we are done. □

We write $\mathcal{L}^{(n)}_{T,1}(z), \ldots, \mathcal{L}^{(n)}_{T,rd}(z)$ for the elements in Λ_n that are given by the projections of $\mathcal{L}^{(n)}_T(z) \mod \omega_n$ to the v_i-component as i runs from 1 to rd.

For $n \geq 1$, we identify $\Lambda_n^{\oplus rd}$ with the column vectors of dimension rd with entries in Λ_n. Define h_n to be the Λ_n-endomorphism on $\Lambda_n^{\oplus rd}$ given by the left multiplication by the product of matrices $C_n \cdots C_1$. Let π_n denote the projection map $\Lambda_{n+1}^{\oplus rd} \to \Lambda_n^{\oplus rd}$.

Proposition 2.8. *For $n \geq 1$, there exists a unique element $\mathrm{Col}_T^{(n)}(z) \in \Lambda_n^{\oplus rd}/\ker h_n$ such that*

$$\begin{pmatrix} \mathcal{L}_{T,1}^{(n)}(z) \\ \vdots \\ \mathcal{L}_{T,rd}^{(n)}(z) \end{pmatrix} \equiv C_n \cdots C_1 \cdot \mathrm{Col}_T^{(n)} \mod \ker h_n.$$

Proof. By [LLZ11, Proposition 4.8], if θ is a Dirichlet character of conductor p^{n+1}, then $\theta\left(\varphi^{-n-1}\left(\mathcal{L}_T^K(z)\right)\right) \in \mathbb{Q}_{p,n} \otimes_{\mathbb{Z}_p} \mathrm{Fil}^0 \mathbb{D}_K(T)$. In other words, $\varphi^{-n-1}\left(\mathcal{L}_T^K(z)\right)$ is of the form $\sum_{i=1}^d F_i v_i$ for some $F_i \in \mathcal{H}$ where $\Phi_{p^n}(1+X)|F_i$ for $i = rd_0+1, \ldots, rd$. But

$$\varphi^{-n-1}\left(\mathcal{L}_T^K(z)\right) = \begin{pmatrix} v_1 & \cdots & v_{rd} \end{pmatrix} \cdot (C_\varphi)^{-n-1} \cdot \begin{pmatrix} \mathcal{L}_{T,1}^K(z) \\ \vdots \\ \mathcal{L}_{T,rd}^K(z) \end{pmatrix}$$

and

$$(C_\varphi)^{-n-1} \cdot \begin{pmatrix} \mathcal{L}_{T,1}^K(z) \\ \vdots \\ \mathcal{L}_{T,rd}^K(z) \end{pmatrix} \equiv \begin{pmatrix} \mathcal{L}_{T,1}^{(n)}(z) \\ \vdots \\ \mathcal{L}_{T,rd}^{(n)}(z) \end{pmatrix} \mod \omega_n.$$

Therefore, $\mathcal{L}_{T,rd_0+1}^{(n)}(z), \ldots, \mathcal{L}_{T,rd}^{(n)}$ are all congruent to 0 modulo $\Phi_{p^n}(1+X)$. Hence, there exists a unique element $\mathrm{Col}_T^{(n,1)}(z) \in \Lambda_n^{\oplus rd}/\ker C_n$ such that

$$\begin{pmatrix} \mathcal{L}_{T,1}^{(n)}(z) \\ \vdots \\ \mathcal{L}_{T,rd}^{(n)}(z) \end{pmatrix} \equiv C_n \cdot \mathrm{Col}_T^{(n,1)}(z) \mod \ker C_n.$$

But $C_n \equiv (C_\varphi)^{-1} \mod \omega_{n-1}$, so

$$\mathrm{Col}_T^{(n,1)}(z) \equiv (C_\varphi)^{-n} \cdot \begin{pmatrix} \mathcal{L}_{T,1}^K(z) \\ \vdots \\ \mathcal{L}_{T,rd}^K(z) \end{pmatrix} \mod (\omega_{n-1}, \ker C_n).$$

Once again, by [LLZ11, Proposition 4.8], we may find $\mathrm{Col}_T^{(n,2)}(z) \in \Lambda_n^{\oplus rd}/\ker C_n C_{n-1}$ such that

$$\mathrm{Col}_T^{(n,1)}(z) \equiv C_{n-1} \cdot \mathrm{Col}_T^{(n,2)} \mod \ker C_n C_{n-1}.$$

On repeating this for n times, we obtain the result. □

We shall show that the sequence $\left\{\mathrm{Col}_T^{(n)}(z)\right\}_{n\geq 1}$ gives us an element in $\Lambda^{\oplus rd}$. To do this, we need the following lemmas.

Lemma 2.9. *The projection map π_n induces a map on the quotients*

$$\pi_n' : \Lambda_{n+1}^{\oplus rd}/\ker h_{n+1} \to \Lambda_n^{\oplus rd}/\ker h_n.$$

Proof. Let $x \in \ker h_{n+1}$. Recall that

$$C_{n+1} \equiv (C_\varphi)^{-1} \mod \omega_n,$$

so we have

$$\pi_n(C_{n+1}\cdots C_1\cdot x) = C^{-1}\left(\begin{array}{c|c} I_{rd_0} & 0 \\ \hline 0 & pI_{r(d-d_0)}\end{array}\right) C_n\cdots C_1(\pi_n(x)).$$

Since Λ_n has no p-torsion, we deduce that $\pi_n(x)\in\ker h_n$ as required. □

Lemma 2.10. *The inverse limit* $\varprojlim_{\pi_n'}\left(\Lambda_n^{\oplus rd}/\ker h_n\right)$ *is equal to* $\Lambda^{\oplus rd}$.

Proof. The map π_n' is surjective since π_n is so. Hence, we have an isomorphism

$$\varprojlim \Lambda_n^{\oplus rd}/\ker h_n \cong \Lambda^{\oplus rd}/\varprojlim \ker h_n.$$

Indeed, if x is an element of $\Lambda^{\oplus rd}$ that lies inside $\varprojlim \ker h_n$, we have $M_T\cdot x = 0$ as elements in $\mathcal{H}^{\oplus rd}$. But M_T has non-zero determinant, so $x=0$. □

Theorem 2.11. *There exists a unique* $\mathrm{Col}_T^K(z)\in\Lambda^{\oplus rd}$ *such that*

$$\begin{pmatrix}\mathcal{L}_{T,1}^K(z)\\ \vdots \\ \mathcal{L}_{T,rd}^K(z)\end{pmatrix} = M_T\cdot\mathrm{Col}_T^K(z).$$

Proof. By Propositions 2.7 and 2.8, we have

$$\begin{pmatrix}\mathcal{L}_{T,1}^K(z)\\ \vdots \\ \mathcal{L}_{T,rd}^K(z)\end{pmatrix} \equiv M_n\cdot\mathrm{Col}_T^{(n)}(z) \mod (\omega_n, \ker h_n).$$

On letting $n\to\infty$, the theorem follows from Proposition 2.4 and Lemma 2.10. □

Corollary 2.12. *We have* $\mathcal{L}_T^K(z) = \begin{pmatrix} v_1 & \cdots & v_{rd}\end{pmatrix}\cdot M_T\cdot\mathrm{Col}_T^K(z)$.

Note that since $\mathcal{L}_T^K$ is a Λ-homomorphism, the map

$$\begin{aligned} H^1_{\mathrm{Iw}}(K,T) &\to \Lambda^{\oplus rd}\\ z &\mapsto \mathrm{Col}_T^K(z)\end{aligned}$$

is also a Λ-homomorphism.

2.4. **Images of the Coleman maps.**

2.4.1. *Determinants of* Λ*-modules.* We first recall the definition of the determinant of a $\mathbb{Z}_p[[X]]$-module as given in [PR94, §3.1.5]. If M is a finitely generated projective $\mathbb{Z}_p[[X]]$-module, $\det(M)$ is simply the maximal exterior power of M. More generally, if M is simply a finitely generated $\mathbb{Z}_p[[X]]$-module, let

$$0\to M_r\to\cdots\to M_1\to M_0\to M\to 0$$

be a projective resolution, then $\det(M)$ is defined to be $\bigotimes_{i=0}^r\det(M_i)^{(-1)^i}$. This definition is independent of the choice of the projective resolution.

If $0\to M_1\to M_2\to M_3\to 0$ is a short exact sequence of Λ-modules, then

$$\det(M_2) = \det(M_1)\otimes\det(M_2).$$

For example, if $M = \mathbb{Z}_p[[X]]/f\mathbb{Z}_p[[X]]$ where $f \in \mathbb{Z}_p[[X]]$, then by considering the exact sequence

$$0 \to f\mathbb{Z}_p[[X]] \to \mathbb{Z}_p[[X]] \to \mathbb{Z}_p[[X]] \to 0,$$

we see that $\det(M) = f^{-1}\mathbb{Z}_p[[X]]$. More generally, if M is a torsion $\mathbb{Z}_p[[X]]$-module, we see that

$$\mathrm{char}_{\mathbb{Z}_p[[X]]} M = \det(M)^{-1}.$$

Let $M = (f_1, \dots, f_r)$ be a $\mathbb{Z}_p[[X]]$-submodule of $\mathbb{Z}_p[[X]]^{\oplus r}$ such that $\mathbb{Z}_p[[X]]^{\oplus r}/M$ is $\mathbb{Z}_p[[X]]$-torsion. Write $f_i = (f_{i,j})_{j=1,\dots,r}$ where $f_{i,j} \in \mathbb{Z}_p[[X]]$, then $\det(M)$ is the $\mathbb{Z}_p[[X]]$-module generated by the determinant of the $r \times r$ matrix whose entries are given by $f_{i,j}$.

More generally, if M is a finitely generated Λ-module, we define $\det_\Lambda(M)$ to be

$$\sum_\eta e_\eta \cdot \det(M^\eta)$$

where the sum runs over all characters of Δ.

2.4.2. *Description of the images.* Let η be a character modulo p. We will now describe the η-isotypical component of the image of the Coleman map Col_T^K.

Lemma 2.13. *If η is non-trivial, then*

$$e_\eta \mathrm{Col}_{T,i}^K(z) \in X\mathbb{Z}_p[[X]]$$

for $i = rd_0 + 1, \dots, rd$. If η is trivial, then the last $r(d-d_0)$ entries of

$$(1 - C_\varphi)^{-1}(C_\varphi - p^{-1}) e_\eta \mathrm{Col}_T^K(z)$$

are zeros when evaluated at $X = 0$.

Proof. Let us first remark that $\eta(F) = e_\eta \cdot F|_{X=0}$ for any element $F \in \mathcal{H}$. Furthermore,

$$\eta \begin{pmatrix} \mathcal{L}_{T,1}(z) \\ \vdots \\ \mathcal{L}_{T,rd}(z) \end{pmatrix} = C_\varphi \cdot \eta(\mathrm{Col}_T^K(z)) \tag{7}$$

by Corollary 2.12 and the fact that $\eta(C_n) = C_\varphi^{-1}$ for all $n \geq 1$.

If η is non-trivial, we have

$$\varphi^{-1}\left(\eta(\mathcal{L}_T(z))\right) \in \mathrm{Fil}^0 \mathbb{D}_K(T)$$

by [LLZ11, Proposition 4.8]. Therefore, as in the proof of Proposition 2.7, the last $r(d-d_0)$ entries of

$$(C_\varphi)^{-1}\eta \begin{pmatrix} \mathcal{L}_{T,1}(z) \\ \vdots \\ \mathcal{L}_{T,rd}(z) \end{pmatrix}$$

are zero. Therefore, the last $r(d-d_0)$-entries of

$$(C_\varphi)^{-1}\eta \begin{pmatrix} \mathcal{L}_{T,1}(z) \\ \vdots \\ \mathcal{L}_{T,rd}(z) \end{pmatrix} = \eta(\mathrm{Col}_T^K(z))$$

are zero when evaluated at $X = 0$.

Otherwise, if η is the trivial character,

$$(1-\varphi)^{-1}(1-p^{-1}\varphi^{-1})\,(\eta(\mathcal{L}(z))) \in \mathrm{Fil}^0\,\mathbb{D}_K(T).$$

The last $r(d-d_0)$-entries of

$$(1-C_\varphi)^{-1}(C_\varphi - p^{-1})\eta(\mathrm{Col}_T^K(z))$$

are zeros by (7). □

Corollary 2.14. *If η is non-trivial, then* $\mathrm{Im}\left(\mathrm{Col}_T^K\right)^\eta$ *is contained in*

$$\mathbb{Z}_p[[X]]^{\oplus rd_0} \oplus X\mathbb{Z}_p[[X]]^{\oplus r(d-d_0)}.$$

If η is trivial, then $\mathrm{Im}\left(\mathrm{Col}_T^K\right)^\eta$ *is contained in*

$$\left\{F \in \mathbb{Z}_p[[X]]^{\oplus rd} : \text{the last } r(d-d_0)\text{entries of } (1-C_\varphi)^{-1}(C_\varphi - p^{-1})F \text{ are divisible by } X\right\}.$$

Proposition 2.15. *The containments in Corollary 2.14 have finite index.*

Proof. By the Colmez-Perrin-Riou reciprocity law, with respect to a Λ-basis of $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T_p(A))$ and a $\mathbb{Z}_p$-basis of $\mathbb{D}_K(T)$, the determinant of $\mathcal{L}_T$ is, up to a unit in Λ, $(\log(1+X)/p)^{r(d-d_0)}$. By Proposition 2.4, the determinant of M_T is, up to a constant in $\mathbb{Z}_p^\times$, $(\log(1+X)/pX)^{r(d-d_0)}$. Therefore,

$$\det{}_\Lambda\left(\mathrm{Im}\left(\mathrm{Col}_T^K\right)\right) = X^{r(d-d_0)}\Lambda.$$

by Corollary 2.12. Since the modules described in Corollary 2.14 have determinant $X^{r(d-d_0)}$, the quotients of the containments have trivial determinant. □

Corollary 2.16. *For any η,* $\mathrm{Im}\left(\mathrm{Col}_{T,i}^K\right)^\eta$ *is pseudo-isomorphic to either $\mathbb{Z}_p[[X]]$ or $X\mathbb{Z}_p[[X]]$.*

3. Conjectures

Let F be a number field of degree r where the prime p is unramified. We assume that F is either a totally real field or a CM field. We fix a rank d continuous $\mathbb{Z}_p$-representation T of G_F such that T verifies the hypotheses (H.F.-L.), (H.S.), (H.Leop) and (H.nA) introduced above.

Furthermore, in order to simplify notation, we set $g = [F:\mathbb{Q}] \times d$ and define $g_+ := \dim\left(\mathrm{Ind}_{F/\mathbb{Q}}T \otimes \mathbb{Q}_p\right)^+$ as above. Set $g_- = g - g_+$ and suppose throughout that $g_- > 0$. Let $\mathbb{D}_p(T)$ be the direct sum $\oplus_{\mathfrak{p}|p}\mathbb{D}_{F_\mathfrak{p}}(T)$. We assume until the end that the following form of the *Panchishkin condition* holds true:

(H.P.) $\dim\left(\mathrm{Fil}^0\mathbb{D}_p(T)\otimes\mathbb{Q}_p\right) = g_-$.

Let S be the set of primes of F where T is ramified and those that divide p. If L is an extension of F, we write $G_{L,S}$ for the Galois group of the maximal extension of L unramified outside S. Fix until the end an even Dirichlet character η of $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$.

For $i = 1, 2$, we define

$$H^i_{\mathrm{Iw},S}(F,T) = \varprojlim H^i(G_{F(\mu_{p^n}),S}, T).$$

By [PR95, Proposition 1.3.2], our assumptions on T imply that at each isotypic component, $H^2_{\mathrm{Iw},S}(F,T)$ is $\mathbb{Z}_p[[X]]$-torsion and $H^1_{\mathrm{Iw},S}(F,T)_\pm$ is of rank $g_\mp$ over $\Lambda_\pm$. Let $\mathfrak{f}_2 \in \Lambda$ be the characteristic ideal of $H^2_{\mathrm{Iw},S}(F,T)$. We write loc for the localization map

$$\mathrm{loc} : H^1_{\mathrm{Iw},S}(F,T) \longrightarrow H^1_{\mathrm{Iw}}(F_p,T) := \bigoplus_{\mathfrak{p}|p} H^1_{\mathrm{Iw}}(F_\mathfrak{p},T),$$

and also for the map induced on the η-isotypic submodule.

3.1. **Semi-local decomposition.** Consider the map

$$\mathcal{L}^F_T = \oplus_{\mathfrak{p}|p}\mathcal{L}^{F_\mathfrak{p}}_T : H^1_{\mathrm{Iw}}(F_p,T) \longrightarrow \mathcal{H} \otimes_{\mathbb{Z}_p} \mathbb{D}_p(T).$$

We fix a basis $v_1, \dots, v_g$ for $\mathbb{D}_p(T)$ consisting of bases for each $\mathbb{D}_{F_\mathfrak{p}}(T)$ that admit the construction of the logarithmic matrix $M_{T|G_{F_\mathfrak{p}}}$ from Section 2.2. In particular, it consists of sub-bases $\{v_{\mathfrak{p},i}\}$ of $\mathbb{D}_{F_\mathfrak{p}}(T)$ for each $\mathfrak{p}|p$.

Let M_T be the $g\times g$ block diagonal matrix where the entries are given by $M_{T|G_{F_\mathfrak{p}}}$ for $\mathfrak{p}|p$. We write $(\mathrm{Col}_{T,i})_{i=1}^g$ for the column vector given by $\left(\mathrm{Col}^{F_\mathfrak{p}}_T\right)_{\mathfrak{p}|p}$. Then, Corollary 2.12 gives us the decomposition of Λ-homomorphism

$$\mathcal{L}^F_T = \begin{pmatrix} v_1 & \cdots & v_g \end{pmatrix} \cdot M_T \cdot \begin{pmatrix} \mathrm{Col}_{T,1} \\ \vdots \\ \mathrm{Col}_{T,g} \end{pmatrix} \tag{8}$$

for some block diagonal matrix $M_T \in M_{g\times g}(\mathcal{H})$, whose entries are all $o(\log)$.

Let loc_p be the localization from $H^1_{\mathrm{Iw},S}(F,T)$ to $H^1_{\mathrm{Iw}}(F_p,T)$. We write $\mathcal{L}_{\mathrm{loc}}$ for the composition $\mathcal{L}^F_T \circ \mathrm{loc}$.

Definition 3.1. *We write $\mathfrak{I}_p$ for the set of tuples $\underline{I} = (I_\mathfrak{p})_{\mathfrak{p}|p}$ where each $I_\mathfrak{p}$ is a subset of of $\{1, \dots, [F_\mathfrak{p} : \mathbb{Q}_p]\}$ such that $\sum \#I_\mathfrak{p} = g_-$. This can be equally regarded as the set of subsets of $\{1, \dots, g\}$ of size g_-. We shall construct a Selmer group for each $\underline{I} \in \mathfrak{I}_p$, which we conjecture to be Λ-cotorsion.*

3.2. **Perrin-Riou's main conjecture.**

Definition 3.2. *Let $\mathfrak{B} = \{v_1, \cdots, v_g\}$ be a $\mathbb{Z}_p$-basis of $\mathbb{D}_p(T)$ such that a sub-basis $\{v_{i_1}, \cdots, v_{i_{g_-}}\}$ generating $\mathrm{Fil}^0\,\mathbb{D}_p(T)$. Let $\mathfrak{B}' = \{v'_1, \cdots, v'_g\} \subset \mathbb{D}_p(T^*(1))$ be its dual basis. The basis $\mathfrak{B}$ is called admissible if for any $\underline{I} \in \mathfrak{I}_p$, we have*

$$\mathrm{span}\,(v'_i : i \in \underline{I}) \cap \mathrm{Fil}^0\,\mathbb{D}_p(T^*(1)) = 0.$$

Proposition 3.3. *An admissible basis exists.*

The proof Proposition 3.3 will be given in Appendix B. We henceforth assume that the basis we have chosen in (8) is an admissible basis.

Recall the hypothesis (H.M.) that $T \otimes \mathbb{Q}_p$ is the p-adic realization of the motive $\mathcal{M}$. Let $\mathcal{M}^*(1)$ denote the dual motive.

Conjecture 3.4. *There exists an analytic p-adic L-function*

$$L_p(\mathcal{M}^*(1)) \in \mathcal{H}_+ \otimes \wedge^{g_-} \mathbb{D}_p(T)$$

such that for all even Dirichlet characters θ of conductor $p^n > 1$, we have

$$\theta\left(L_p(\mathcal{M}^*(1))\right) = \sum_{\underline{I} \in \mathfrak{I}_p} \left(\frac{p^n}{\tau(\theta^{-1})}\right)^{g_-} L(\mathcal{M}^*(1), \theta^{-1}, 1) \frac{\Omega_{\mathcal{M}(\theta)^*(1),p}(\underline{I})}{\Omega_{\mathcal{M}(\theta)^*(1)}(\underline{I})} \cdot \varphi^n \left(\wedge_{i \in \underline{I}} v_i\right) .$$

When θ is the trivial character,

$$\theta\left(L_p(\mathcal{M}^*(1))\right) = \sum_{\underline{I} \in \mathfrak{I}_p} (1-\varphi)(1-p^{-1}\varphi^{-1})^{-1} L(\mathcal{M}^*(1), 1) \frac{\Omega_{\mathcal{M}^*(1),p}(\underline{I})}{\Omega_{\mathcal{M}^*(1)}(\underline{I})} \cdot \left(\wedge_{i \in \underline{I}} v_i\right) .$$

Here $\Omega_{\mathcal{M}(\theta)^*(1)}(\underline{I})$ is some element in $\mathbb{C}^\times$ such that $\frac{L(\mathcal{M}^*(1),\theta^{-1},1)}{\Omega_{\mathcal{M}(\theta)^*(1)}(\underline{I})} \in \overline{\mathbb{Q}}$, which we regard as an element of $\overline{\mathbb{Q}}_p$ and $\Omega_{\mathcal{M}(\theta)^*(1),p}(\underline{I})$ is some p-adic period.

Remark 3.5. *Our interpolation formulae are not quite the ones stated in* [PR95, §4.2] *that predict a relation between the leading term of the p-adic L-function and complex L-values. Rather, we opt for a formulation that is closer to the existing one for elliptic curves and the one stated in* [CPR89]. *We also implicitly assume that the p-adic period $\Omega_{\mathcal{M}(\theta)^*(1),p}(\underline{I})$ is non-zero.*

The main conjecture of Perrin-Riou relates this conjectural p-adic L-function to the following module.

Definition 3.6. *Perrin-Riou's module of p-adic L-function is defined to be*

$$\mathbb{I}_{\mathrm{arith}}(T) = \det{}_\Lambda\left(\mathrm{Im}(\mathcal{L}_{\mathrm{loc}})\right) \otimes \det{}_\Lambda\left(H^2_{\mathrm{Iw},S}(F,T)\right)^{-1} .$$

Conjecture 3.7 (Perrin Riou's Main Conjecture)**.** *As Λ_+-modules, we have*

$$L_p(\mathcal{M}^*(1))\Lambda_+ = \mathbb{I}_{\mathrm{arith}}(T)_+ .$$

Lemma 3.8. *Let R be a commutative ring. Let M and M' be two R-modules, with a homomorphism $F : M \to M'$ of Λ-modules. Let $m \leq n$ be integers. Fix $a_1, \ldots, a_m \in M$ and $b_1, \ldots, b_n \in M'$ with*

$$F(a_i) = \sum_{j=1}^{n} r_{i,j} b_j$$

for $i = 1, \ldots, m$. Then

$$F(a_1 \wedge \ldots \wedge a_m) = \sum_{j_1 < \cdots < j_m} \det(r_{j_1,\ldots,j_m})\, b_{j_1} \wedge \cdots \wedge b_{j_m}$$

where $r_{j_1,\ldots,j_m}$ is the $m \times m$ matrix whose (k,l)-entry is given by r_{k,j_l}.

Proof. This is standard multi-linear algebra. □

We now study the conjectural $L_p(\mathcal{M}^*(1))$ further and relate it to the regulator map of Perrin-Riou.

Proposition 3.9. *Let $\mathfrak{c} = \mathfrak{c}_1 \wedge \cdots \wedge \mathfrak{c}_{g_-} \in \wedge^{g_-} H^1_{\mathrm{Iw},S}(F,T)_+$, θ an even Dirichlet character of conductor p^n. For $\underline{I} = (I_\mathfrak{p})_{\mathfrak{p}|p} \in \mathfrak{I}_p$, we write $\mathfrak{M}^{\underline{I}}_\theta(\mathfrak{c})$ for the $g_- \times g_-$ matrix whose entries are given by $\left[\sum_{\sigma\in G_n} \theta(\sigma)\exp^*_n\left(\mathrm{loc}_\mathfrak{p}(\mathfrak{c}_i)^\sigma\right), v'_{\mathfrak{p},j}\right]$ for $1 \le i \le g_-$ and $j \in I_\mathfrak{p}$. If for all $\underline{I}$ and θ,*

$$\det\left(\mathfrak{M}^{\underline{I}}_\theta(\mathfrak{c})\right) = L(\mathcal{M}^*(1),\theta^{-1},1)\frac{\Omega_{\mathcal{M}(\theta)^*(1),p}(\underline{I})}{\Omega_{\mathcal{M}(\theta)^*(1)}(\underline{I})},$$

then $\mathcal{L}_{\mathrm{loc}}(\mathfrak{c})$ satisfies the interpolation properties given in Conjecture 3.4.

Proof. This follows from Lemmas 2.6 and 3.8. □

Remark 3.10. *Note that if we had $v'_j \in \mathrm{Fil}^0\,\mathbb{D}_{F_\mathfrak{p}}(T^*(1))$ for some $\mathfrak{p}|p$ and $j \in I_\mathfrak{p}$, then we would have $\det\left(\mathfrak{M}^{\underline{I}}_\theta(\mathfrak{c})\right) = 0$ for every Dirichlet character θ as above. We have fixed an admissible basis to avoid this situation.*

Remark 3.11. *Note that we have only considered the interpolation problem for the twists of the motive $\mathcal{M}^*(1)$ by even characters θ of Γ. One can also formulate a conjecture for* odd *characters, for which one needs to replace everywhere g_- by g_+ (and vice-versa). Note also that upon studying the motive $\mathcal{M}\otimes\omega$ (where ω is the Teichmüller character) in place of $\mathcal{M}$, one may reduce the consideration for odd characters to the case of even characters.*

Perrin-Riou's special element conjecture can be interpreted as follows.

Conjecture 3.12. *There exists a non-zero element $\mathfrak{c} \in \wedge^{g_-} H^1_{\mathrm{Iw},S}(F,T)_+$ satisfying the properties described in Proposition 3.9.*

If M is a Λ-module such that M^η is $\mathbb{Z}_p[[X]]$-torsion for all even characters of η, we define the characteristic ideal

$$\mathrm{char}_{\Lambda_+} M_+ := \sum_\eta e_\eta \cdot \mathrm{char}_{\mathbb{Z}_p[[X]]} M^\eta$$

where the sum runs over all even characters of Δ.

Proposition 3.13. *If Conjecture 3.12 holds, then Conjecture 3.7 is equivalent to the assertion that*

$$\mathrm{char}_{\Lambda_+}\left(H^2_{\mathrm{Iw},S}(F,T)_+\right) = \mathrm{char}_{\Lambda_+}\left(H^1_{\mathrm{Iw},S}(F,T)_+/(\mathfrak{c}_1,\ldots,\mathfrak{c}_{g_-})\right). \tag{9}$$

Proof. For any non-zero element $\mathfrak{c} = \mathfrak{c}_1 \wedge \cdots \wedge \mathfrak{c}_{g_-} \in \wedge^{g_-} H^1_{\mathrm{Iw},S}(F,T)_+$, we write $\mathfrak{f}_\mathfrak{c}$ for a generator of $\mathrm{char}_{\Lambda_+} H^1_{\mathrm{Iw},S}(F,T)_+/(\mathfrak{c}_1,\ldots,\mathfrak{c}_{g_-})$. Therefore, we have

$$e_+ \cdot \mathbb{I}_{\mathrm{arith}}(A) = \mathfrak{f}_2\mathfrak{f}_\mathfrak{c}^{-1} \cdot \mathcal{L}_{\mathrm{loc}}(\mathfrak{c}) \cdot \Lambda_+$$

for any non-trivial $\mathfrak{c}$. If furthermore

$$\mathcal{L}_{\mathrm{loc}}(\mathfrak{c}) = L_p(\mathcal{M}^*(1)),$$

the result follows immediately. □

3.3. **Bounded p-adic L-functions.** Throughout, we assume that Conjecture 3.12 holds. Let $\mathfrak{c} = \mathfrak{c}_1 \wedge \cdots \wedge \mathfrak{c}_{g_-}$ be the element given the conjecture.

Lemma 3.14. *For $\underline{I} \in \mathfrak{I}_p$ and a character η modulo p, there exists an integer $n(\underline{I}, \eta) \geq 0$ such that*

$$\det\left(\mathrm{Im}\left(\mathrm{Col}_T^{\underline{I}}\right)^{\eta}\right) = X^{n(\underline{I},\eta)}\mathbb{Z}_p[[X]].$$

Proof. This follows from Proposition 2.15. □

To simplify notation, if we write $\mathrm{Col}_T^{\underline{I}}(\mathfrak{c}_i)$ for $\mathrm{Col}_T^{\underline{I}}(\mathrm{loc}(\mathfrak{c}_i))$, $1 \leq i \leq g_-$.

Definition 3.15. *For each $\underline{I} \in \mathfrak{I}_p$, we define the p-adic L-function $L_{\underline{I}}(\mathcal{M}^*(1))$ to be* $\det\left(\mathrm{Col}_{\underline{I}}(\mathfrak{c}_i)\right)$.

Lemma 3.16. *We have*

$$\det\left(\mathrm{Im}\left(\mathrm{Col}_T^{\underline{I}}\right)\Big/\mathrm{span}_\Lambda\left\{\mathrm{Col}_{\underline{I}}(\mathfrak{c}_i)\right\}_{i=1}^{g_-}\right)^{\eta} = \left(L_{\underline{I}}(\mathcal{M}^*(1))^{\eta}/X^{n(\underline{I},\eta)}\right)\mathbb{Z}_p[[X]].$$

Proof. This follows from Lemma 3.14 and the fact that taking det is compatible with exact sequences. □

Theorem 3.17. *For $\underline{I} = (I_{\mathfrak{p}}), \underline{J} = (J_{\mathfrak{p}}) \in \mathfrak{I}_p$, let $M_T^{\underline{I},\underline{J}}$ be the $g_- \times g_-$ the submatrix of M_T whose entries correspond to the elements of $I_{\mathfrak{p}}$ and $J_{\mathfrak{p}}$. Then there is a decomposition*

$$L_p(\mathcal{M}^*(1)) = \sum_{\underline{I},\underline{J} \in \mathfrak{I}_p} \wedge_{i \in \underline{I}} v_i \det(M_T^{\underline{I},\underline{J}}) L_{\underline{J}}(\mathcal{M}^*(1)).$$

Proof. Let the (j,k)-entry of M_T be $m_{j,k}$. Recall that (8) says that

$$\mathcal{L}_{\mathrm{loc}}(\mathfrak{c}_i) = \sum_{1 \leq j,k \leq g} v_j m_{j,k} \mathrm{Col}_{T,k}(\mathrm{loc}(\mathfrak{c}_i))$$

for $1 \leq i \leq g_-$. Hence by Lemma 3.8, we have

$$\begin{aligned}\wedge_{i=1}^{g_-}\mathcal{L}_{\mathrm{loc}}(\mathfrak{c}_i) &= \sum_{\underline{I} \in \mathfrak{I}_p} \det\left(\sum_{k=1}^{g} m_{j,k}\mathrm{Col}_{T,k}(\mathrm{loc}(\mathfrak{c}_i))\right)_{j \in \underline{I}, 1 \leq i \leq g_-} \cdot \wedge_{i \in \underline{I}} v_i \\ &= \sum_{\underline{I} \in \mathfrak{I}_p} \wedge_{i \in \underline{I}} v_i \sum_{\underline{J} \in \mathfrak{I}_p} \det(m_{j,k})_{j \in \underline{I}, k \in \underline{J}} \cdot \det(\mathrm{Col}_{T,k}(\mathrm{loc}(\mathfrak{c}_i))_{k \in \underline{J}, 1 \leq i \leq g_-}\end{aligned}$$

as required. □

3.4. **Special elements for ray class fields and connections with Euler systems of rank g_-.** For a finite abelian extension L/F which is unramified at all primes of F above p, we define the relative (semi-local) Dieudonné module of T by setting

$$\mathbb{D}_L(T) := \mathbb{D}_p(\mathrm{Ind}_{L/F} T).$$

For $L = F$, we will continue to denote this module by $\mathbb{D}_p(T)$ instead of writing $\mathbb{D}_F(T)$.

Definition 3.18. *For a finite extension $E/\mathbb{Q}_p$ and a character*

$$\chi : \mathrm{Gal}(L/F) \longrightarrow E^\times,$$

let $\epsilon_\chi = \dfrac{1}{[L:F]} \displaystyle\sum_{g\in \mathrm{Gal}(L/F)} \chi(g) g^{-1}$ *be the associated idempotent. We denote by* Π_χ *the compositum of the maps*

$$\Pi_\chi : H^1_{\mathrm{Iw},S}(L,T)\otimes\mathbb{Q}_p \xrightarrow{\sim} H^1_{\mathrm{Iw},S}(F, \mathrm{Ind}_{L/F}\, T)\otimes\mathbb{Q}_p \longrightarrow H^1_{\mathrm{Iw},S}(F, T\otimes\chi)\otimes\mathbb{Q}_p$$

where the first isomorphism follows from Shapiro's Lemma and the second map is the projection on the χ^{-1}*-isotypic component.*

Note that Π_χ factors as

$$\begin{array}{ccc} H^1_{\mathrm{Iw},S}(L,T)\otimes\mathbb{Q}_p & \xrightarrow{\Pi_\chi} & H^1_{\mathrm{Iw},S}(F,T\otimes\chi)\otimes\mathbb{Q}_p \\ {\scriptstyle \epsilon_{\chi^{-1}}}\downarrow & \nearrow_{\sim} & \\ \epsilon_{\chi^{-1}}\left(H^1_{\mathrm{Iw},S}(L,T)\otimes\mathbb{Q}_p\right) & & \end{array}$$

Lemma 3.19. (i) *There is a natural identification*

$$\mathbb{D}_L(T) \cong \mathcal{O}_L \otimes_{\mathcal{O}_F} \mathbb{D}_p(T)\,.$$

(ii) *For every finite extension E of $\mathbb{Q}_p$ and non-trivial character*

$$\chi : \mathrm{Gal}(L/F) \longrightarrow E^\times,$$

every choice of an embedding $L \hookrightarrow B_{\mathrm{cris}}$ induces an isomorphism

$$E \otimes_{\mathcal{O}_E} \mathbb{D}_p(T\otimes\chi) \cong \epsilon_{\chi^{-1}}\left(E\otimes_{\mathbb{Q}_p}\mathbb{D}_L(T)\right).$$

Proof. Both assertions are standard and follow from the fact that the G_F-representation $\mathrm{Ind}_{L/F}\, T$ is crystalline at all primes above p, as the G_F-representation T is and L/F is unramified above p. □

For every prime $\mathfrak{q} \nmid S$ of F, let $F(\mathfrak{q})$ denote the maximal pro-p-extension contained in the ray class field of F modulo $\mathfrak{q}$. Let $\mathfrak{N}$ denote the square-free products of primes of F that are not in S. For $\tau = \mathfrak{q}_1\cdots\mathfrak{q}_k \in \mathfrak{N}$, let $F(\tau)$ denote the compositum $F(\mathfrak{q}_1)\cdots F(\mathfrak{q}_k)$. Set $\Delta_\tau = \mathrm{Gal}(F(\tau)/F)$.

Remark 3.20. *Recall that we have assumed F is either a CM field or a totally real field. If F is a CM field, then $F(\tau)$ is totally complex. If F is totally real, then so is $F(\tau)$. Hence, for*

$$\begin{aligned} g_-(F(\tau)) &:= \mathrm{rank}_{\mathbb{Q}_p[\Delta_\tau]}\left(\mathrm{Ind}_{F(\tau)/\mathbb{Q}}\, T\right)^- \\ &= \mathrm{rank}_{\mathbb{Q}_p[\Delta_\tau]}\left(\mathbb{Q}_p[\Delta_\tau]\otimes \mathrm{Ind}_{F/\mathbb{Q}}\, T\right)^- \end{aligned}$$

(where complex conjugation acts on the factor $\mathbb{Q}_p[\Delta_\tau]$ by conjugation), we have $g_-(F(\tau)) = g_-$ for every $\tau \in \mathfrak{N}$ in either case.

Fix once and for all an embedding

$$\iota : \varinjlim_{\tau \in \mathfrak{N}} F(\tau) \hookrightarrow B_{\mathrm{cris}} \ .$$

Let $\mathfrak{B} = \{v_1, \cdots, v_g\}$ be an admissible $\mathbb{Z}_p$-basis (in the sense of Definition 3.2) of $\mathbb{D}_p(T)$. By, Lemma 3.19 (ii), ι induces an admissible $\mathcal{O}_E$-basis $\mathfrak{B}^\chi = \{v_1^\chi, \cdots, v_g^\chi\}$ of $\mathbb{D}_p(T \otimes \chi)$.

Definition 3.21. *Given an element*

$$\boldsymbol{c}^{(\tau)} = c_1^{(\tau)} \wedge \cdots \wedge c_{g_-}^{(\tau)} \in \wedge^{g_-}_{\Lambda_+[\Delta_\tau]} H^1_{\mathrm{Iw},S}(F(\tau), T)_+,$$

an even Dirichlet character θ of conductor p^n, a character $\chi : \Delta_\tau \to E^\times$ and for $\underline{I} = \{i_1, \ldots, i_{g_-}\} \in \mathfrak{I}_p$ with $i_1 < \cdots < i_{g_-}$, let $\mathfrak{M}^{\underline{I}}_{\theta,\chi}\left(\mathfrak{c}^{(\tau)}\right)$ be the $g_- \times g_-$ matrix whose (k,l)-entry is given by

$$\left[\sum_{\sigma \in G_n} \theta(\sigma) \exp_n^* \left(\mathrm{loc}\left(\Pi_\chi \left(c_k^{(\tau)} \right) \right)^\sigma \right), (v_{i_l}^\chi)' \right].$$

In the spirit of [Rub00, §VIII], we propose the following extension of Conjecture 3.12 by essentially introducing the conjectural p-adic L-functions over $F(\tau)$ for $\tau \in \mathfrak{N}$.

Conjecture 3.22. *For every finite extension E of $\mathbb{Q}_p$, every non-trivial character $\chi : \Delta_\tau \to E^\times$ and every even Dirichlet character θ of conductor p^n, there is a non-zero element*

$$\boldsymbol{\zeta}^{(\tau)} = \boldsymbol{\zeta}_1^{(\tau)} \wedge \cdots \wedge \boldsymbol{\zeta}_{g_-}^{(\tau)} \in \wedge^{g_-}_{\Lambda_+[\Delta_\tau]} H^1_{\mathrm{Iw},S}(F(\tau), T)_+$$

such that

$$\det\left(\mathfrak{M}^{\underline{I}}_{\theta,\chi}(\boldsymbol{\zeta}^{(\tau)}) \right) = L_\tau(\mathcal{M}^*(1), \chi^{-1}\theta^{-1}, 1) \frac{\Omega_{\mathcal{M}(\chi\theta)^*(1),p}(\underline{I})}{\Omega_{\mathcal{M}(\chi\theta)^*(1)}(\underline{I})} \ ,$$

where $L_\tau(\mathcal{M}^*(1), \chi^{-1}\theta^{-1}, s)$ is the complex valued (twisted) L-function with the Euler factors at dividing τ removed.

Proposition 3.23. *Assume that Conjecture 3.22 holds true. Then the collection $\{\boldsymbol{\zeta}^{(\tau)}\}_{\tau \in \mathfrak{N}}$ is an Euler system of rank g_- in the sense of* [PR98, Definition 1.2.2] *and* [Büy10, Definition 3.1].

Proof. Since we have assumed (H.nA), this follows as in the proof of [Rub00, Lemma VIII.5.1] using Propisition 3.9. □

3.5. **Modified Selmer groups.**

Definition 3.24. *For $\underline{I} \in \mathfrak{I}_p$, we define*

$$\begin{aligned} \mathrm{Col}^{\underline{I}}_T : H^1_{\mathrm{Iw}}(F_p, T) &\to \Lambda^{\oplus g_-} \\ z &\mapsto \oplus_{i \in \underline{I}} \mathrm{Col}_{T,i}(z) \end{aligned}$$

and $H^1_{\underline{I}}(F_p, T)$ is defined to be the kernel of $\mathrm{Col}^{\underline{I}}_T$.

Lemma 3.25. *For any subset $\{i_1, \ldots, i_k\}$ of the set $\{1, \ldots, g\}$, the Λ-module $\bigcap_{j=1}^k \ker \mathrm{Col}_{i_j}$ is torsion-free of rank $g - k$.*

Proof. Recall that the Λ-torsion submodule of $H^1_{\mathrm{Iw}}(F_p,T)$ is isomorphic to $H^0(F(\mu_{p^\infty})_p,T)$ trivial since we assumed (H.nA). it follows that the Λ-module $H^1_{\mathrm{Iw}}(T_p(A))$ is torsion-free.

By Proposition 2.15, $\mathrm{Im}\left(\oplus_{j=1}^k \mathrm{Col}_{i_j}\right)$ has rank k over Λ. But $H^1_{\mathrm{Iw}}(F_p,T)$ is of rank g over Λ thus $\ker\left(\oplus_{j=1}^k \mathrm{Col}_{i_j}\right)=\bigcap_{j=1}^k \ker \mathrm{Col}_{i_j}$ has rank $g-k$ over Λ. □

Corollary 3.26. (a) *For each $\underline{I}\in\mathfrak{I}_p$, the torsion-free Λ-module $H^1_{\underline{I}}(F_p,T)$ has rank g_+.*

(b) $\displaystyle\bigcap_{i=1}^{g}\ker \mathrm{Col}_i=0.$

Lemma 3.27. *Let W be (a torsion-free) Λ-submodule of $H^1_{\mathrm{Iw}}(F_p,T)$ generated by at most g_- elements. Then there is an $\underline{I}\in\mathfrak{I}_p$ such that*

$$W\cap H^1_{\underline{I}}(F_p,T)=0\,.$$

Proof. Assume contrary that

$$W\cap H^1_{\underline{I}}(F_p,T)\neq 0$$

for any $\underline{I}\in\mathfrak{I}_p$. We prove by induction on $0\le k\le g_+$ that for every subset J of $\{1,\cdots,g\}$ of size g_-+k, there is an non-zero element

$$0\neq w_J\in W\cap\left(\bigcap_{i\in J}\ker \mathrm{Col}_i\right).$$

When $k=0$, this is the hypothesis of the lemma. Assume its truth for $k=n<g_+$ and consider $J=\{i_1,\cdots,i_{g_-+n+1}\}\subset\{1,\cdots,g\}$. Set $J_s=J\backslash\{i_s\}$ for $s=1,\cdots,g_-+n+1$ and choose using the induction hypothesis a non-zero element $z_s\in W\cap\big(\bigcap_{i\in J_s}\ker \mathrm{Col}_i\big)$. As the Λ-module W is generated by at most g_- elements, it follows that $\{z_s\}_{s=1}^{g_-+n+1}$ verifies a non-trivial relation

$$b_1z_1+b_2z_2+\cdots+b_{g_-+n+1}z_{g_-+n+1}=0,$$

where $b_i\in\Lambda$. Let $s_0\in\{1,\cdots,g_-+n+1\}$ be the smallest index such that $b_{s_0}\neq 0$. Then observe that $b_{s_0}z_{s_0}$ is non-zero since W is torsion free and $b_{s_0}z_{s_0}\in \mathrm{span}\{z_i\}_{i\neq s_0}\subset\ker \mathrm{Col}_{i_{s_0}}$, where the latter containment is due to our choice of the elements z_j's. On the other hand, $b_{s_0}z_{s_0}\in\bigcap_{s\neq s_0}\ker \mathrm{Col}_{i_s}$ by the choice of z_{s_0}, hence

$$0\neq b_{s_0}z_{s_0}\in\ker \mathrm{Col}_{s_0}\cap\left(\bigcap_{s\neq s_0}\ker \mathrm{Col}_{i_s}\right)=\bigcap_{i\in J}\ker \mathrm{Col}_i\,,$$

as desired. Now this shows (for $k=g_+$) that

$$W\cap\left(\bigcap_{i=1}^{g}\ker \mathrm{Col}_i\right)\neq 0\,,$$

contradicting Corollary 3.26(b). □

Proposition 3.28. *Assume the truth of Conjecture 3.12. For some $\underline{I}\in\mathfrak{I}_p$,*

$$\mathrm{span}\,\{\mathrm{loc}(c_i)\}_{i=1}^{g_-}\cap H^1_{\underline{I}}(F_p,T)=\{0\}.$$

Proof. This is immediate from Lemma 3.27 by setting $W = \operatorname{span}\{\log(c_i)\}_{i=1}^{g_-}$.

□

Let $T^\vee = T^* \otimes \mu_{p^\infty}$. The standard Selmer group $\mathrm{Sel}(T^\vee/F(\mu_{p^\infty}))$ is defined to be

$$\mathrm{Sel}(T^\vee/F(\mu_{p^\infty})) := \ker\left(H^1(F(\mu_{p^\infty}),T^\vee) \to \bigoplus_v \frac{H^1(F(\mu_{p^\infty})_v,T^\vee)}{H^1_f(F(\mu_{p^\infty})_v,T^\vee)}\right).$$

We shall modify the conditions at primes above p using our Coleman maps.

Fix $\underline{I} \in \mathfrak{I}_p$. By local Tate duality, there is a pairing

$$H^1_{\mathrm{Iw}}(F_p,T) \times H^1(F(\mu_{p^\infty})_p,T^\vee) \to \mathbb{Q}_p/\mathbb{Z}_p \tag{10}$$

where $H^1(F(\mu_{p^\infty})_p,T^\vee)$ denotes $\bigoplus_{\mathfrak{p}|p} H^1(F(\mu_{p^\infty})_\mathfrak{p},T^\vee)$.

Define $H^1_{\underline{I}}(F(\mu_{p^\infty})_p,T^\vee)$ to be the orthogonal complement of $H^1_{\underline{I}}(F_p,T)$ under the pairing (10).

Definition 3.29. *We define the $\underline{I}$-Selmer group* $\mathrm{Sel}_{\underline{I}}(T^\vee/F(\mu_{p^\infty}))$ *to be*

$$\ker\left(H^1(F(\mu_{p^\infty}),T^\vee) \longrightarrow \bigoplus_{v\nmid p} \frac{H^1(F(\mu_{p^\infty})_v,T^\vee)}{H^1_f(F(\mu_{p^\infty})_v,T^\vee)} \oplus \frac{H^1(F(\mu_{p^\infty})_p,T^\vee)}{H^1_{\underline{I}}(F(\mu_{p^\infty})_p,T^\vee)}\right).$$

Remark 3.30. *Let $A/\mathbb{Q}$ be an abelian variety of dimension g and $A^\vee$ denote its dual abelian variety. Throughout this remark we set $T = T_p(A)$, the p-adic Tate module of A. In this case, we have for the local conditions that determine the standard Selmer group that*

$$H^1_f(\mathbb{Q}_p(\mu_{p^\infty}),T^\vee) = A^\vee\left(\mathbb{Q}_p(\mu_{p^\infty})\right).$$

When A has good ordinary reduction at p, the Λ-module $A^\vee\left(\mathbb{Q}_p(\mu_{p^\infty})\right)$ has corank g by the main result of [Sch87] *and $\mathrm{Sel}(A^\vee/\mathbb{Q}(\mu_{p^\infty}))$ is predicted to be Λ-cotorsion. In the supersingular case, however, the module $A^\vee\left(\mathbb{Q}_p(\mu_{p^\infty})\right)$ has Λ-corank $2g$, thus $\mathrm{Sel}(A^\vee/\mathbb{Q}(\mu_{p^\infty}))$ has corank at least g. In the definition above we replace the local conditions $A^\vee\left(\mathbb{Q}_p(\mu_{p^\infty})\right)$ that appear in the definition of the standard Selmer group by a corank-g submodule and conjecture that the resulting Selmer groups are Λ-cotorsion.*

Conjecture 3.31. *For any $\underline{I} \in \mathfrak{I}_p$, the Λ_+-module $\mathrm{Sel}_{\underline{I}}(T^\vee/F(\mu_{p^\infty}))_+$ is cotorsion at each isotypic component.*

The following statement will be referred as the *$\underline{I}$-main conjecture.* We shall verify that its truth for a single $\underline{I} \in \mathfrak{I}_p$ is equivalent to the η-isotypical part of Perrin-Riou's main Conjecture 3.7.

Conjecture 3.32. *Assume that Conjecture 3.31 holds. Let $\underline{I} \in \mathfrak{I}_p$ and η an even Dirichlet character of conductor p, then*

$$\mathrm{char}_{\mathbb{Z}_p[[X]]}\mathrm{Sel}_{\underline{I}}(T^\vee/F(\mu_{p^\infty}))^{\vee,\eta} = \left(L_{\underline{I}}(\mathcal{M}^*(1))^\eta/X^{n(\underline{I},\eta)}\right)\mathbb{Z}_p[[X]].$$

Proposition 3.33. *Assume the truth of Conjecture 3.12 and suppose that $\underline{I} \in \mathfrak{I}_p$ is as in the conclusion of Proposition 3.28. Then*

$$\log\left(H^1_{\mathrm{Iw},S}(F,T)^\eta\right) \cap H^1_{\underline{I}}(F_p,T)^\eta = 0$$

Proof. For $\underline{I} \in \mathfrak{I}_p$ as in the statement of the proposition, let $\mathcal{F}_I$ be the *Selmer structure* on $T \otimes \Lambda$ (in the sense of [MR04]) given by local condition determined by the submodule $H^1_{\underline{I}}(F_p, T)$ at p and no conditions imposed at primes $\ell \neq p$. Let $H^1_{\mathcal{F}_{\underline{I}}}(F, T \otimes \Lambda)$ denote the Selmer group associated to the Selmer structure $\mathcal{F}_{\underline{I}}$. By Proposition 3.28,

$$\begin{aligned}\operatorname{rank}_{\mathbb{Z}_p[[X]]} \operatorname{loc}\left(H^1_{\mathrm{Iw},S}(F,T)^\eta\right) &\geq \operatorname{rank}_{\mathbb{Z}_p[[X]]} \operatorname{loc}\left(H^1_{\mathcal{F}_{\underline{I}}}(F, T\otimes\Lambda)^\eta\right) \\ &\quad + \operatorname{rank}_{\mathbb{Z}_p[[X]]} \left(\operatorname{span}\left\{\operatorname{loc}(c_i)\right\}_{i=1}^{g_-}\right)^\eta \\ &= \operatorname{rank}_{\mathbb{Z}_p[[X]]} \operatorname{loc}\left(H^1_{\mathcal{F}_{\underline{I}}}(F, T\otimes\Lambda)^\eta\right) + g_-\end{aligned}$$

By the weak Leopoldt conjecture (that we have assumed)

$$\operatorname{rank}_{\mathbb{Z}_p[[X]]} H^1_{\mathrm{Iw},S}(F,T)^\eta = g_- \,.$$

This in return implies that (note that the map loc is injective also by the weak Leopoldt conjecture) $H^1_{\mathcal{F}_{\underline{I}}}(F, T\otimes\Lambda)^\eta$ is $\mathbb{Z}_p[[X]]$-torsion. However, the module $H^1_{\mathrm{Iw},S}(F,T)^\eta \supset H^1_{\mathcal{F}_{\underline{I}}}(F, T\otimes\Lambda)^\eta$ is $\mathbb{Z}_p[[X]]$-torsion free (since we have assumed (H.nA)) hence it is trivial. Thus

$$\ker\left(H^1_{\mathrm{Iw},S}(F,T)^\eta \xrightarrow{\mathrm{loc}} \frac{H^1_{\mathrm{Iw}}(F_p,T)^\eta}{H^1_{\underline{I}}(F_p,T)^\eta}\right) =: H^1_{\mathcal{F}_{\underline{I}}}(F, T\otimes\Lambda)^\eta = 0, \tag{11}$$

as desired. □

Theorem 3.34. *Assume that Conjectures 3.12 and 3.31, then for every even Dirichlet character η of Δ, the η-part of Conjecture 3.7 is equivalent to Conjecture 3.32 for every $\underline{I} \in \mathfrak{I}_p$ verifying the conclusion of Proposition 3.28.*

Proof. The Poitou-Tate exact sequence (as studied in [PR95, §A.3]) implies that we have an exact sequence

$$0 \to H^1_{\mathrm{Iw},S}(F,T)^\eta \to \frac{H^1_{\mathrm{Iw}}(F_p,T)^\eta}{H^1_{\underline{I}}(F_p,T)^\eta} \to \mathrm{Sel}_{\underline{I}}(T^\vee/F(\mu_{p^\infty}))^{\vee,\eta} \to H^2_{\mathrm{Iw},S}(F,T)^\eta \to 0. \tag{12}$$

Note that the left-most injection follows from the choice of $\underline{I}$ and Proposition 3.33. The second term in (12) is isomorphic to $\operatorname{Im}\left(\mathrm{Col}^{\underline{I}}_T\right)^\eta$, which is described by Proposition 2.15.

Let $\mathfrak{c} = \mathfrak{c}_1 \wedge \cdots \wedge \mathfrak{c}_{g_-}$ be the element given by Conjecture 3.12. The exact sequence (12) then yields the following exact sequence:

$$\begin{aligned}0 \longrightarrow H^1_{\mathrm{Iw},S}(F,T)^\eta / \left(\operatorname{span}_\Lambda\{c_i\}_{i=1}^{g_-}\right)^\eta \longrightarrow \operatorname{Im}\left(\mathrm{Col}^{\underline{I}}_T\right)^\eta \Big/ \left(\operatorname{span}_\Lambda\left\{\mathrm{Col}_{\underline{I}}(\mathfrak{c}_i)\right\}_{i=1}^{g_-}\right)^\eta \\ \longrightarrow \mathrm{Sel}_{\underline{I}}(T^\vee/F(\mu_{p^\infty}))^{\vee,\eta} \longrightarrow H^2_{\mathrm{Iw},S}(F,T)^\eta \longrightarrow 0.\end{aligned}$$

Therefore, we have

$$\begin{aligned}\det\left(H^1_{\mathrm{Iw},S}(F,T)^\eta / \left(\operatorname{span}_\Lambda\{c_i\}_{i=1}^{g_-}\right)^\eta\right) \otimes \det\left(\mathrm{Sel}_{\underline{I}}(T^\vee/F(\mu_{p^\infty}))^{\vee,\eta}\right) = \\ \det\left(\operatorname{Im}\left(\mathrm{Col}^{\underline{I}}_T\right)^\eta \Big/ \left(\operatorname{span}_\Lambda\left\{\mathrm{Col}_{\underline{I}}(\mathfrak{c}_i)\right\}_{i=1}^{g_-}\right)^\eta\right) \otimes \det\left(H^2_{\mathrm{Iw},S}(F,T)^\eta\right),\end{aligned}$$

which can be rewritten as

$$e_\eta \cdot \mathfrak{f}_{\mathfrak{c}}^{-1} \det\left(\mathrm{Sel}_{\underline{I}}(T^\vee/F(\mu_{p^\infty}))^\vee\right) = e_\eta \cdot \det\left(\mathrm{Im}\left(\mathrm{Col}_T^{\underline{I}}\right)\Big/\mathrm{span}_\Lambda\left\{\mathrm{Col}_{\underline{I}}(\mathfrak{c}_i)\right\}_{i=1}^{g_-}\right)\mathfrak{f}_2^{-1}.$$

By Proposition 3.13, it follows that Conjecture 3.7 is equivalent to

$$\det\left(\mathrm{Sel}_{\underline{I}}(T^\vee/F(\mu_{p^\infty}))^{\vee,\eta}\right) = \det\left(\mathrm{Im}\left(\mathrm{Col}_T^{\underline{I}}\right)^\eta\Big/\left(\mathrm{span}_\Lambda\left\{\mathrm{Col}_{\underline{I}}(\mathfrak{c}_i)\right\}_{i=1}^{g_-}\right)^\eta\right).$$

Hence we are done by Lemma 3.16. □

Theorem 3.35. *Suppose that the representation T verifies the hypotheses* **(H1)-(H4)** *of* [MR04, §3.5]. *If Conjecture 3.22 holds true, then so does Conjecture 3.31 for some $\underline{I} \in \mathfrak{I}_p$ and for every character η.*

Proof. The proof of Theorem 3.35 follows using the rank-g_- Euler system $\{\boldsymbol{\zeta}^{(\tau)}\}_{\tau\in\mathfrak{N}}$ along with the methods developed in our companion article [BL14], more particularly by the first part of Theorem A.3.1 of loc.cit. The key points are as follows. The hypotheses (H.wL) in loc.cit. holds true thanks to Conjecture 3.12 and the weak Leopoldt conjecture, both of which we assume. We take the map Ψ in loc.cit. to be $e_\eta \cdot \mathrm{Col}_T^{\underline{I}}$ where $\underline{I} \in \mathfrak{I}_p$ is chosen so that the conclusion of Proposition 3.28 holds true. The hypotheses (H.V) in [BL14, Appendix A.3] is satisfied for the Selmer structure $\mathcal{F}_{\underline{I}}$ thanks to (11). Therefore Theorem A.3.1 of loc.cit. indeed applies and the proof follows. □

Corollary 3.36. *Suppose that the hypotheses* **(H1)-(H4)** *of* [MR04, §3.5] *on T hold true. The truth of Conjecture 3.22 implies the containment* **??**

$$L_p(\mathcal{M}^*(1))\Lambda_+ = \mathbb{I}_{\mathrm{arith}}(T)_+.$$

in the statement of Perrin-Riou's Main Conjecture 3.7.

Proof. By Theorem 3.35, Conjecture 3.31 holds true under our running hypotheses. Let η be an even Dirichlet character on Δ. The containment

$$\left(L_{\underline{I}}(\mathcal{M}^*(1))^\eta/X^{n(\underline{I},\eta)}\right)\cdot\mathbb{Z}_p[[X]] \subset \mathrm{char}_{\mathbb{Z}_p[[X]]}\mathrm{Sel}_{\underline{I}}(T^\vee/F(\mu_{p^\infty}))^{\vee,\eta}$$

in the statement of Conjecture 3.32 now follows from the second part of Theorem A.3.1 of [BL14], applied as in the proof of Theorem 3.35 above. This containment combined with the proof of Theorem 3.34 yields the Corollary. □

Remark 3.37. *See* [BL14] *for an example where we deduce an explicit version of Corollary 3.36. In loc.cit., we study more closely the motive attached to the Hecke character associated to a CM abelian variety that has supersingular reduction at all primes above p. In this particular case, the hypotheses* **(H1)-(H4)** *of* [MR04, §3.5], (H.F.-L.), (H.S.), (H.P.) *and* (H.nA) *hold true.*

Appendix A. An alternative approach using Wach modules

In [LLZ10] and [LLZ11], we showed that the theory of Wach module can be used to study the Iwasawa theory of p-adic representations. The key is to find an explicit basis for the Wach module. In this appendix, we show that the construction of the logarithmic matrix M_T in §2.2 can be modified to construct an explicit basis for the Wach module $\mathbb{N}(T)$ of T. Here, T is as defined in §2.2, satisfying (H.F.-L.) and (H.S.).

Let $\mathbb{A}_K^+ = \mathcal{O}_K[[\pi]]$, which is equipped with the usual semi-linear actions by Γ and φ (see for example [Ber04]). We write $q = \varphi(\pi)/\pi$.

Definition A.1. *A Wach module with weights in $[a;b]$ is a finitely generated free $\mathbb{A}_K^+$-module M such that*

(1) *It is equipped with a semi-linear action by Γ that is trivial modulo π;*
(2) *There is a semi-linear map $\varphi : M[\pi^{-1}] \to M[\varphi(\pi)^{-1}]$ such that $\varphi(\pi^b M) \subset \pi^b M$ and $q^{b-a}\varphi(\pi^b M) \subset \pi^b M$;*
(3) *The actions of Γ and φ commute.*

A Wach module N is equipped with a filtration

$$\mathrm{Fil}^i N = \{x \in N : \varphi(x) \in q^i N\}.$$

Let $v_1, \dots, v_d$ be $\mathcal{O}_K$-basis of $\mathbb{D}_K(T)$ such that $v_1, \dots, v_{d_0}$ generate $\mathrm{Fil}^0 \mathbb{D}_K(T)$. Let C_φ be the matrix of φ with respect to this basis. As in §2.2,

$$C_\varphi = \left(\begin{array}{c|c} I_{r_0} & 0 \\ \hline 0 & \frac{1}{p} I_{r-r_0} \end{array}\right) C$$

for some $C \in \mathrm{GL}_d(\mathcal{O}_K)$.

Definition A.2. *For $n \geq 1$, we define*

$$P_n = \left(\begin{array}{c|c} I_{r_0} & 0 \\ \hline 0 & \frac{1}{\varphi^{n-1}(q)} I_{r-r_0} \end{array}\right) C \quad \text{and} \quad M_n' = (C_\varphi)^n P_n^{-1} \cdots P_1^{-1}.$$

Proposition A.3. *The sequence of matrices $\{M_n'\}_{n\geq 1}$ converges entry-wise with respect to the sup-norm topology on $\mathbb{B}^+_{\mathrm{rig},K}$. If M_T' denotes the limit of the sequence, each entry of M_T' are $o(\log)$. Moreover, $\det(M_T')$ is, up to a constant in $\mathcal{O}_K^\times$, equal to $\left(\frac{\log(1+\pi)}{\pi}\right)^g$.*

Proof. The proof is the same as that for Proposition 2.4. □

Definition A.4. *For each $\gamma \in \Gamma$, define a matrix $G_\gamma = (M_T')^{-1} \cdot \gamma(M_T')$.*

We shall show that G_γ is a matrix defined over $\mathbb{A}_K^+$. Let us first prove the following lemma.

Lemma A.5. *Let $M_{r\times r}(\mathbb{A}_K^+)$ be the set of $r \times r$ matrices that are defined over $\mathbb{A}_K^+$.*

(a) *$P_1 \cdot \gamma\left(P_1^{-1}\right) \in I + \pi M_{r\times r}(\mathbb{A}_K^+)$;*
(b) *If $M \in I + \pi M_{r\times r}(\mathbb{A}_K^+)$, then $P_1 \cdot \varphi(M) \cdot \gamma(P_1^{-1}) \in I + \pi M_{r\times r}(\mathbb{A}_K^+)$.*

Proof. For (a), we have $P_1 \cdot \gamma(P_1^{-1}) = \left(\begin{array}{c|c} I_{r_0} & 0 \\ \hline 0 & \frac{\gamma\cdot q}{q} I_{r-r_0} \end{array}\right)$ and $\frac{\gamma\cdot q}{q} \in 1 + \pi\mathbb{A}_K^+$, hence the result.

Let $M = I + \pi N$, then

$$P_1 \cdot \varphi(M) \cdot \gamma(P_1^{-1}) = P_1 \gamma\left(P_1^{-1}\right) + \pi\left(qP_1 \cdot \varphi(N) \cdot \gamma\left(P_1^{-1}\right)\right)$$

since $\varphi(\pi) = \pi q$. Both qP_1 and P_1^{-1} are defined over $\mathbb{A}_K^+$, so (b) follows from (a). □

Proposition A.6. *For all γ, the matrix G_γ is an element of $I + \pi M_{r\times r}(\mathbb{A}_K^+)$.*

Proof. Since $G_\gamma = \lim_{n\to\infty} (M_n')^{-1} \cdot \gamma(M_n')$, it is enough to show that $(M_n')^{-1} \cdot \gamma(M_n')$ is in $I + \pi M_{r\times r}(\mathbb{A}_K^+)$ for all n. Let us show this by induction.

We have for all n

$$(M_n')^{-1} \cdot \gamma(M_n') = P_1 \cdots P_n \gamma(P_n^{-1}) \cdots \gamma(P_1^{-1}). \tag{13}$$

Hence, the claim for $n = 1$ is Lemma A.5(a).

By definition, $P_n = \varphi^{n-1}(P_1)$, so we have for $n \geq 2$

$$(M_n')^{-1} \cdot \gamma(M_n') = P_1 \cdot \varphi\left((M_n')^{-1} \cdot \gamma(M_n')\right) \cdot \gamma(P_1^{-1}).$$

Hence, the inductive step is simply Lemma A.5(b). □

Lemma A.7. *For all γ, we have the matrix identity*

$$P_1 \cdot \varphi(G_\gamma) = G_\gamma \cdot \gamma(P_1).$$

Proof. By (13) and the fact that $P_n = \varphi^{n-1}(P_1)$, we have

$$P_1 \cdot \varphi\left((M_n')^{-1} \cdot \gamma(M_n')\right) = P_1 \cdots P_{n+1} \gamma(P_{n+1}^{-1} \cdots P_2^{-1})$$

and

$$\left((M_n')^{-1} \cdot \gamma(M_n')\right) \cdot \gamma(P_1) = P_1 \cdots P_n \gamma(P_n^{-1} \cdots P_2^{-1}).$$

In other words,

$$P_1 \cdot \varphi\left((M_n')^{-1} \cdot \gamma(M_n')\right) = \left(\left(M_{n+1}'\right)^{-1} \cdot \gamma\left(M_{n+1}'\right)\right) \cdot \gamma(P_1)$$

Hence the result follows on taking $n \to \infty$. □

Definition A.8. *We define a free $\mathbb{A}_K^+$-module N_{C_φ} of rank r, with basis $n_1, \ldots, n_r$. With respect to this basis, we equip N_{C_φ} with a semi-linear action by Γ, which is given by the matrix G_γ (well-defined by Proposition A.6) and a semi-linear map $\varphi : N_{C_\varphi}[\pi^{-1}] \to N_{C_\varphi}[\varphi(\pi)^{-1}]$, which is given by the matrix P_1.*

Proposition A.9. *The module N_{C_φ} is a Wach module with weights in $[0; 1]$.*

Proof. By Proposition A.6, the action of Γ on N_{C_φ} is trivial modulo π.

Since $P_1 \in 1/qM_{r\times r}(\mathbb{A}_K^+)$, we have

$$\varphi\left(\pi N_{C_\varphi}\right) \in \pi N_{C_\varphi} \quad \text{and} \quad q\varphi\left(N_{C_\varphi}\right) \subset \pi^b N_{C_\varphi}.$$

Finally, by Lemma A.7, the actions of Γ and φ commute, so we are done. □

Theorem A.10. *As Wach modules, N_{C_φ} is isomorphic to $\mathbb{N}(T)$. Furthermore,*

$$\begin{pmatrix} v_1 & \cdots & v_r \end{pmatrix} M_T' = \begin{pmatrix} n_1 & \cdots & n_r \end{pmatrix}.$$

Proof. In order to show that $N_{C_\varphi} \cong \mathbb{N}(T)$, it is enough to show that

$$\mathbb{D}_K(T) \cong N_{C_\varphi} \mod \pi \tag{14}$$

as filtered φ-module by [Ber04, Théorme III.4.4].

By definition $P_1 \equiv C_\varphi \mod \pi$, so the actions of φ agree on the two sides of (14). For the filtration, we have

$$\mathrm{Fil}^i N_{C_\varphi} = \begin{cases} N_{C_\varphi} & i \leq -1 \\ \left(\bigoplus_{1\leq j\leq r_0} \mathbb{A}_K^+ \cdot n_j\right) \oplus \left(\bigoplus_{r_0+1\leq j\leq r} \mathbb{A}_K^+ \cdot \pi n_j\right) & i = 0 \\ \left(\bigoplus_{1\leq j\leq r_0} \mathbb{A}_K^+ \cdot \pi^i n_j\right) \oplus \left(\bigoplus_{r_0+1\leq j\leq r} \mathbb{A}_K^+ \cdot \pi^{i+1} n_j\right) & i \geq 1 \end{cases}.$$

Since $\mathrm{Fil}^0 \mathbb{D}(T_p(A))$ is generated by $v_1, \ldots, v_{r_0}$, we see that the filtraions on the two sides of (14) as well.

By [Ber04, §II.3],

$$\begin{pmatrix} v_1 & \cdots & v_r \end{pmatrix} M = \begin{pmatrix} n_1 & \cdots & n_r \end{pmatrix}.$$

for some matrix $M \in I + \pi M_{r\times r}(\mathbb{B}^+_{\mathrm{rig},K})$. For any $\gamma \in \Gamma$,

$$\begin{pmatrix} v_1 & \cdots & v_r \end{pmatrix} \gamma(M) = \begin{pmatrix} n_1 & \cdots & n_r \end{pmatrix} G_\gamma.$$

Therefore, $G_\gamma = M \cdot \gamma(M^{-1}) = M'_T \cdot \gamma\left(M'_T\right)^{-1}$. But $M'_T \in I + \pi M_{r\times r}(\mathbb{B}^+_{\mathrm{rig},K})$ also. Hence,

$$M \cdot \left(M'_T\right)^{-1} \in \left(I + \pi M_{r\times r}(\mathbb{B}^+_{\mathrm{rig},K})\right)^\Gamma.$$

This implies that $M = M'_T$ as required. □

Appendix B. Linear Algebra: Proof of Proposition 3.3

The goal of this appendix is to provide a proof of Proposition 3.3.

Lemma B.1. *Let W be a free $\mathbb{Z}_p$-module of rank $\mathfrak{d}$ and let W' be a free, rank $\mathfrak{d}-1$ direct summand of W. Then the collection $\{W' + \mathbb{Z}_p \cdot v : v \in W\}$ of submodules of W is totally ordered (with respect to inclusion).*

Proof. This follows from the fact that the quotient W/W' is a free $\mathbb{Z}_p$-module of rank one. □

Lemma B.2. *Let W be as in the previous lemma. Let $\mathfrak{D}$ be a finite collection of rank $\mathfrak{d}-1$ direct summands of W and let $W_0 = \cup_{\mathfrak{D}} W'$ be their union. For any $k \in \mathbb{Z}^+$ we have,*

$$p^k W \cup W_0 \neq W.$$

Proof. Choose any element $w = w_0 \in W - W_0$ (such an element clearly exists). If $w_0 \notin p^k W$, we are done, otherwise write $w_0 = p^k w_1$. Observe that $w_1 \notin W_0$ (as otherwise, w_0 would be an element of W_0 as well). Now if $w_1 \notin p^k W$, we are done again. Otherwise we may continue with this process, which eventually has to terminate. □

Lemma B.3. *For $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p)$, the set $\left\{\frac{ax+by}{cx+dy} : x, y \in \mathbb{Z}_p^\times\right\}$ has infinite cardinality.*

Proof. Since $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p)$, either $c \neq 0$ or $d \neq 0$; say the first holds true. Note that $\dfrac{ax+by}{cx+dy} = \dfrac{a}{c} - \dfrac{(ad-bc)/c}{cx+dy}$, and $ad-bc \neq 0$ and that $cx+dy$ takes on infinitely many values as $x, y \in \mathbb{Z}_p^\times$ vary. □

Lemma B.4. *Let W, $\mathfrak{D}$ and W_0 be as in Lemma B.2. Let $W_1, W_2 \in \mathfrak{D}$ and suppose $v_1, v_2 \in W - W_0$ verify*

$$W_1 \oplus \mathbb{Z}_p \cdot v_1 = W = W_2 \oplus \mathbb{Z}_p \cdot v_2 \,.$$

There one can choose $\alpha, \beta \in \mathbb{Z}_p$ so that

(a) $v = \alpha v_1 + \beta v_2 \in W - W_0$,
(b) $W_1 \oplus \mathbb{Z}_p \cdot v = W_2 \oplus \mathbb{Z}_p \cdot v = W$.

Proof. Fix a basis $\mathfrak{B}_1$ of W_1 and $\mathfrak{B}_2$ of W_2. Let x_1 be the v_2-coordinate of v_1 with respect to the basis $\mathfrak{B}_2 \cup \{v_2\}$ and x_2 be the v_1-coordinate of v_2 with respect to the basis $\mathfrak{B}_1 \cup \{v_1\}$. We may assume without loss of generality that $v_p(x_i) > 0$ for $i = 1, 2$, as otherwise, say in case $v_p(x_1) = 0$, it would follow that $\mathrm{span}\,(\mathfrak{B}_2, v_1) = \mathrm{span}\,(\mathfrak{B}_2, x_1 \cdot v_2) = W$ and thus the choice $\alpha = 1$ and $\beta = 0$ (thus $v = v_1$) would work. Let $X = \begin{pmatrix} x_1 & 1 \\ 1 & x_2 \end{pmatrix}$ and let $Y = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p)$ be such that $YX = 1$ (such Y exists since $\det(X) \in \mathbb{Z}_p^\times$ thanks to our running hypothesis).

Consider $W_0 \cap \mathrm{span}\,(v_1, v_2)$. Since $v_1 \notin W_0$, it follows that this intersection is a finite union of $\mathbb{Z}_p$-lines, say spanned by $\{\alpha_i v_1 + \beta_i v_2\}_{i=1}^d$ (with $\alpha_i, \beta_i \in \mathbb{Z}_p$). Let $\mathfrak{X} = \{\alpha_i/\beta_i : \beta_i \neq 0\}$, note that it is a finite subset of $\mathbb{Q}_p$. Use Lemma B.3 to choose $x, y \in \mathbb{Z}_p^\times$ such that $\frac{ax+by}{cx+dy} \notin \mathfrak{X}$. Set $\alpha = ax + by$ and $\beta = cx + dy$. Note that we have by definitions

$$Y \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

or equivalently that

$$\begin{pmatrix} x_1 & 1 \\ 1 & x_2 \end{pmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}. \tag{15}$$

Observe that $v := \alpha v_1 + \beta v_2 \notin W_0$ (as $\alpha/\beta \notin \mathfrak{X}$), so v satisfies (a). Furthermore,

$$v = \alpha v_1 + \beta v_2 \equiv (\alpha x_1 + \beta) \cdot v_2 = x \cdot v_2 \mod W_2$$

and

$$v \equiv (\alpha + \beta x_2) \cdot v_1 = y \cdot v_1 \mod W_1$$

We therefore conclude (using the fact $x, y \in \mathbb{Z}_p^\times$) that

$$\mathrm{span}\,(W_1, v) = \mathrm{span}\,(W_1, y \cdot v_1) = \mathrm{span}\,(W_1, v_1) = W\,,$$

and

$$\mathrm{span}\,(W_2, v) = \mathrm{span}\,(W_2, x \cdot v_2) = \mathrm{span}\,(W_1, v_2) = W\,,$$

which proves that v verifies (b) as well. □

Lemma B.5. *Let W be as in the previous lemma and let $\{w_1, \ldots, w_{\mathfrak{d}}\}$ be a given basis of W. For any non-negative integer k, one can find elements $\{w_{\mathfrak{d}+1}, \ldots, w_{\mathfrak{d}+k}\} \subset W$ so that for any $I \subset \{1, \ldots, \mathfrak{d}+k\}$ of size $\mathfrak{d}$, the set $\{w_j\}_{j \in \mathfrak{I}_p}$ spans W.*

Proof. We prove the lemma by induction on k. When $k=0$, the assertion is clear and suppose that $k \geq 1$ we have found a set $\{w_{\mathfrak{d}+1}, \dots, w_{\mathfrak{d}+k-1}\}$. Let $\mathfrak{S}$ denote the collection of subsets of $1, \dots, \mathfrak{d}+k-1$ of size $\mathfrak{d}-1$ and let $\mathfrak{D} = \{\mathrm{span}\,(\{w_i\}_{i\in S}) : S \in \mathfrak{S}\}$ be a set of free, rank $\mathfrak{d}-1$ direct summands of W. Set $W_0 = \cup_{\mathfrak{D}} W'$, observe that W_0 is a proper subset of W. For any $w \in W - W_0$ and $S \in \mathfrak{S}$, the submodule $\mathrm{span}\,(\{w\} \cup \{w_i\}_{i\in S})$ of W is of finite index. Fix $S \in \mathfrak{S}$ and define $W_S := \mathrm{span}\,(w_i : i \in S)$.

We first prove that there is an element $v_S \in W - W_0$ such that

$$W_S + \mathbb{Z}_p \cdot v_S = W. \tag{16}$$

Indeed, pick any $w \in W - W_0$. If $W_S + \mathbb{Z}_p \cdot w = W$, we are done. Otherwise we may use Lemma B.2 to choose $w_1 \in W - (W_S + \mathbb{Z}_p \cdot v \cup W_0)$, for which we have

$$W_S + \mathbb{Z}_p \cdot w_1 \supsetneq W_S + \mathbb{Z}_p \cdot w\,.$$

This process has to terminate and when it does, we have found the desired v_S satisfying (16).

Using Lemma B.4 iteratively, one obtains an element $v \in W - W_0$ such that

$$W_S + \mathbb{Z}_p \cdot v = W$$

for every $S \in \mathfrak{S}$. We set $w_{\mathfrak{d}+k} := v$. □

Proof of Proposition 3.3. Let $\mathfrak{B} = \{v_1, \cdots, v_{g_-}, w_{g_-+1}, \dots, w_g\}$ be any $\mathbb{Z}_p$-basis of $\mathbb{D}_p(T)$ such that $\{v_1, \cdots, v_{g_-}\}$ forms a basis of $\mathrm{Fil}^0 \mathbb{D}_p(T)$. Form the dual basis

$$\mathfrak{B}' = \{v_1', \cdots, v_{g_-}', w_{g_-+1}', \cdots, w_g'\} \subset \mathbb{D}_p(T^*(1)).$$

Consider the free $\mathbb{Z}_p$-module $W := \mathbb{D}_p(T^*(1))/\,\mathrm{Fil}^0 \mathbb{D}_p(T^*(1))$ of rank g_- and for an element $v \in \mathbb{D}_p(T^*(1))$, let $\bar{v}$ denote its image in W. It is easy to see that $\{\bar{v}_1', \cdots, \bar{v}_{g_-}'\}$ forms a basis of W. Use Lemma B.5 (with $\mathfrak{d} = g_-$ and $k = g_+$) to obtain a set $\{\bar{v}_1', \cdots, \bar{v}_g'\}$ such that for any $\underline{I} \in \mathfrak{I}_p$,

$$\mathrm{span}\,(\bar{v}_i' : i \in \underline{I}) = W.$$

One can lift the set $\{\bar{v}_1', \cdots, \bar{v}_g'\}$ to a basis $\mathfrak{B}'_{\mathrm{ad}} = \{v_1', \cdots, v_g'\}$ of $\mathbb{D}_p(T^*(1))$ and the the basis $\mathfrak{B}_{\mathrm{ad}}$ dual to $\mathfrak{B}'_{\mathrm{ad}}$ gives us as an admissible basis. □

References

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

[BL14] Kâzım Büyükboduk and Antonio Lei, *Rubin-Stark elements and the supersingular iwasawa theory of CM abelian varieties*, 2014, in preparation, draft available upon request.

[Büy10] Kâzim Büyükboduk, *On Euler systems of rank r and their Kolyvagin systems*, Indiana Univ. Math. J. **59** (2010), no. 4, 1277–1332.

[Büy13] Kâzım Büyükboduk, *On the Iwasawa theory of CM fields for supersingular primes*, 2013, submitted.

[Col98] Pierre Colmez, *Théorie d'Iwasawa des représentations de de Rham d'un corps local*, Ann. of Math. (2) **148** (1998), no. 2, 485–571.

[CPR89] John Coates and Bernadette Perrin-Riou, *On p-adic L-functions attached to motives over* **Q**, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 23–54.

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

[Lei11] Antonio Lei, *Iwasawa theory for modular forms at supersingular primes*, Compositio Math. **147** (2011), no. 03, 803–838.

[LLZ10] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Wach modules and Iwasawa theory for modular forms*, Asian J. Math. **14** (2010), no. 4, 475–528.

[LLZ11] ———, *Coleman maps and the p-adic regulator*, Algebra Number Theory **5** (2011), no. 8, 1095–1131.

[MR04] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96.

[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.

[PR94] Bernadette Perrin-Riou, *Théorie d'Iwasawa des représentations p-adiques sur un corps local*, Invent. Math. **115** (1994), no. 1, 81–161.

[PR95] ———, *Fonctions L p-adiques des représentations p-adiques*, Astérisque (1995), no. 229, 198.

[PR98] ———, *Systèmes d'Euler p-adiques et théorie d'Iwasawa*, Ann. Inst. Fourier (Grenoble) **48** (1998), no. 5, 1231–1307.

[PR04] 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.

[Rub00] Karl Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study.

[Sch87] Peter Schneider, *Arithmetic of formal groups and applications I: Universal norm subgroups*, Invent. Math. **87** (1987), no. 3, 587–602.

[Spr12] Florian E. Ito Sprung, *Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures*, J. Number Theory **132** (2012), no. 7, 1483–1506.

Kâzim Büyükboduk
Max Planck Institut Für Mathematik, Vivatsgasse 7, 53111, Bonn, Deutschland
and
Koç University, Mathematics, Rumeli Feneri Yolu, 34450 Sariyer, Istanbul, Turkey

E-mail address: kazim@math.stanford.edu

Antonio Lei
Department of Mathematics and Statistics, Burnside Hall, McGill University, Montreal, QC, Canada H3A 0B9

E-mail address: antonio.lei@mcgill.ca