Λ-ADIC KOLYVAGIN SYSTEMS

KÂZIM BÜYÜKBODUK

ABSTRACT. In this paper we study Kolyvagin Systems, as defined by Mazur and Rubin, over the cyclotomic $\mathbb{Z}_p$-tower for a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representation T. We prove, under certain hypotheses, that the module of Λ-adic Kolyvagin Systems for the *cyclotomic deformation* $T \otimes \Lambda$ is free of rank one over the cyclotomic Iwasawa algebra. We link our result with a web of conjectures due to Perrin-Riou and Rubin; and we relate the Λ-adic Kolyvagin Systems we prove to exist to (conjectural) p-adic L-functions. We also study the Iwasawa theory of Rubin-Stark elements via the perspective offered by our main theorem, and outline a strategy to deduce the main conjectures of Iwasawa theory for totally real number fields assuming the Rubin-Stark conjecture.

CONTENTS

1. INTRODUCTION

Kolyvagin's machinery of Euler Systems is a powerful tool to bound the order of Selmer groups. It takes an Euler System (which is a collection of cohomology classes with certain coherence relations) as an input, and produces, using a descent argument, the so called derivative classes. These classes give the bounds we seek for.

There is of course a considerable cost for such a useful tool: Finding an Euler System is an extremely difficult task. There are only a few Euler systems known to exist, all of which with great importance, and yet we fail to know if there should be Euler Systems in any other setting than these few number of instances.

However, one may answer an existence problem for the derivative classes. In [MR04], Mazur and Rubin isolate the notion of a *Kolyvagin system*, which has the same formal properties that Kolyvagin's derivative classes have, except that the Kolyvagin Systems enjoy some other local conditions than utilized before. This new property adds to the level of rigidity, and one gains control over the size of the module of Kolyvagin Systems.

Fix a finite extension Φ of $\mathbb{Q}_p$, and let $\mathcal{O}$ be its ring of integers, with $\mathfrak{m}$ its maximal ideal, ϖ its uniformizer, and $\mathbb{F} = \mathcal{O}/\mathfrak{m}$ its residue field. For any field K with a fixed separable closure $\overline{K}$, write $G_K = \mathrm{Gal}(\overline{K}/K)$. Let T be a free $\mathcal{O}$-module of finite rank, endowed with a continuous $G_{\mathbb{Q}}$-action which is unramified outside finitely many primes. Let $\mathcal{F}$ denote a Selmer structure on T and $\Sigma(\mathcal{F})$ a finite set of places of $\mathbb{Q}$ that contains the infinite place, the prime p and all primes where T is ramified (see Definition 2.1.1 of [MR04] for a definition of a *Selmer structure*) and let $\mathcal{P}$ denote a set of rational primes disjoint from $\Sigma(\mathcal{F})$ which we will occasionally refer to as *Kolyvagin primes*. Let also $\chi(T, \mathcal{F})$ denote the core Selmer rank of the Selmer structure $\mathcal{F}$ on T, as in [MR04, Definition 4.1.11].

The following result is proved in [MR04] (Corollary 4.5.1 and Corollary 4.5.2) under suitable hypotheses:

Theorem (Howard, Mazur, Rubin). *Let* $\mathbf{KS}(T/\mathfrak{m}^k T, \mathcal{F}, \mathcal{P})$ *be the module of Kolyvagin Systems over* $\mathcal{O}/\mathfrak{m}^k$, *with* $k \in \mathbb{Z}^+$. *Then*

(i) *If* $\chi(T, \mathcal{F}) = 0$, *then* $\mathbf{KS}(T/\mathfrak{m}^k T, \mathcal{F}, \mathcal{P}) = 0$.
(ii) *If* $\chi(T, \mathcal{F}) = 1$, *then* $\mathbf{KS}(T/\mathfrak{m}^k T, \mathcal{F}, \mathcal{P})$ *is free of rank one as an* $\mathcal{O}/\mathfrak{m}^k$-*module*.
(iii) *If* $\chi(T, \mathcal{F}) > 1$, *then for every* r, *the* $\mathcal{O}/\mathfrak{m}^k$-*module* $\mathbf{KS}(T/\mathfrak{m}^k T, \mathcal{F}, \mathcal{P})$ *contains a free submodule of rank* r.

Therefore, we have an answer for when one could hope to apply Kolyvagin's machinery, at least for the residual representations $T/\mathfrak{m}^k T$. Furthermore, when $\chi(T, \mathcal{F}) = 1$, one may go further and use the result above to obtain Kolyvagin systems for the representation T itself (and not only for its quotients $T/\mathfrak{m}^k T$). These Kolyvagin systems proved to exist essentially have the same use as the derivative classes obtained from an Euler System.

Mazur and Rubin also show (c.f., [MR04, Theorem 5.3.3]) how to obtain Kolyvagin Systems over the cyclotomic Iwasawa algebra starting from an Euler System (in the sense of [Rub00]). Using these Kolyvagin systems over the cyclotomic tower, one *expects* to prove one divisibility in main conjectures of Iwasawa Theory[1]. Once again, one may wonder if there should exist Kolyvagin Systems over an Iwasawa algebra in general. This is what we answer in this paper. Before we describe our main results, we introduce some more notation.

Let $T^* = \mathrm{Hom}(T, \Phi/\mathcal{O}(1))$ be the Cartier dual of T and let $A = T \otimes_{\mathcal{O}} \Phi/\mathcal{O}$. Let also $\mathcal{I}_\ell$ denote a fixed inertia subgroup of $G_{\mathbb{Q}}$ at ℓ. Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ be its Galois group. As usual, $\Lambda := \mathcal{O}[[\Gamma]]$ is the cyclotomic Iwasawa algebra.

Let $\mathcal{F}_{\mathrm{can}}$ denote the canonical Selmer structure on $T \otimes \Lambda$ (see Section 2.1 below), and let $\chi(T) = \chi(T, \mathcal{F}_{\mathrm{can}})$ denote the core Selmer rank of the canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ on T (see [MR04,

---

[1]These Kolyvagin system which we also prove to exist in this article without assuming the existence of Euler systems, have a priori no relation with the L-values. Conjecturally, the classes that we prove to exist here should be related to the relevant p-adic L-function via an independent recipe due in full generality to Perrin-Riou [PR94b]. See Section 4 below for further details.

Definition 4.1.11 and Theorem 5.2.15] for a definition). Let $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ denote the Λ-module of Kolyvagin systems for $\mathcal{F}_{\mathrm{can}}$ on $T \otimes \Lambda$ (defined as in §3.2; see also Remark 3.24 for a comparison of this definition to [MR04, Definitions 3.1.3 and 3.1.6]). Define also $\overline{\mathbf{KS}}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ to be the $\mathcal{O}$-module of Kolyvagin systems for $\mathcal{F}_{\mathrm{can}}$ on T (which has been extensively studied in [MR04, §5.2], see particularly [MR04, Theorem 5.2.12]).

The main technical result of this paper (Theorem 3.23) shows that the Kolyvagin Systems exist over the cyclotomic Iwasawa algebra under certain technical hypotheses:

Theorem A. *Assume the hypotheses in §2.2 and that $\chi(T) = 1$. Then:*

   (i) *The Λ-module $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ is free of rank one.*
   (ii) *The specialization map*

$$\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P}) \longrightarrow \overline{\mathbf{KS}}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$$

   is surjective.

Any element of the module $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ will be called a Λ-*adic Kolyvagin system*.

Before we explain our strategy to prove the theorem above, we first discuss its consequences in several aspects. When $T = \mathcal{O}(1) \otimes \rho^{-1}$, where ρ is an even Dirichlet character, the Kolyvagin system that Theorem A proves to exist comes from the cyclotomic unit Euler system (via the Euler systems to Kolyvagin systems map of Mazur and Rubin, c.f., [MR04, Theorem 5.3.3]). Our theorem further shows that the Kolyvagin system which arises from the cyclotomic unit Euler system is the "best possible" in this setting. See Proposition 4.1 below for more details.

Consider now an elliptic curve $E_{/\mathbb{Q}}$ without CM such that

   (E1) p is coprime to all its Tamagawa factors,
   (E2) p is not anomalous for E (in the sense of Mazur [Maz72]),

and let $T = T_p(E)$ be the p-adic Tate module. In this case, the Λ-adic Kolyvagin system Theorem A proves to exist comes from Kato's [Kat04] Euler system (again via the Euler systems to Kolyvagin systems map of Mazur and Rubin). And again our theorem shows (assuming the Birch and Swinnerton-Dyer conjecture) that the Kolyvagin system which arises from Kato's Euler system is the "best possible" in this setting. See Proposition 4.2 below for further details.

Besides these now-classical examples mentioned above, we also discuss several other arithmetic applications of Theorem A. As the first application, we study in §4.2 the relation of Λ-adic Kolyvagin systems with p-adic L-functions, using the rigidity offered by our main result. Rubin [Rub00, §8] (see also §4.2 below) constructs an Euler system starting from Perrin-Riou's [PR95] conjectural p-adic L-functions. This conjectural Euler system gives rise to a Λ-adic Kolyvagin system using the Euler system to Kolyvagin system map of Mazur and Rubin [MR04, Theorem 5.3.3] and the first part of Theorem A implies that the cohomology classes that we prove to exist in this article should be related (up to multiplication by an element of Λ) to the cohomology classes that Perrin-Riou [PR95, §4.4] and Rubin [Rub00, Conjecture 8.2.6] predict to exist. Thus, Λ-adic Kolyvagin systems we construct here relate to Perrin-Riou's conjectural p-adic L-functions. On the other hand, one may also think of Theorem A as an evidence (albeit quite weak) for the conjectures of Perrin-Riou and Rubin; as it proves a consequence of these conjectures, namely the existence of Λ-adic Kolyvagin systems.

As a further application, we study in §4.3 the Iwasawa theory of Rubin-Stark elements from the perspective offered by Theorem A. Let F be a totally real number field, and $r = [F : \mathbb{Q}]$. Let ρ be a totally even character of G_F (i.e., it is trivial on all complex conjugations inside G_F) into $\mathcal{O}^\times$ that has finite prime-to-p order, and let f_ρ be its conductor. We assume that $(p, f_\rho) = 1$ and $\rho(\wp) \neq 1$ for any prime $\wp$ of F lying over p. Assume also for notational simplicity that p is unramified in $F/\mathbb{Q}$. Let $T = \mathcal{O}(1) \otimes \rho^{-1}$, but now considered as a G_F-representation. The main difficulty in

this setting is that the core Selmer rank of the canonical Selmer structure is greater than one. We show first how to overcome this difficulty by constructing an auxiliary Selmer structure (denoted by $\mathcal{F}_{\mathbb{L}_\infty}$ in §4.3.1), by modifying the local conditions at p. For the construction of $\mathcal{F}_{\mathbb{L}_\infty}$, we utilize a structure theorem for the semi-local cohomology group $H^1(F_p, T \otimes \Lambda)$ due to Perrin-Riou (see Appendix A). Once the auxiliary Selmer structure is constructed, we apply Theorem A to show the existence of Λ-adic Kolyvagin systems for these modified Selmer structures. On the other hand, Rubin [Rub96, §6] shows that the Rubin-Stark elements give rise to an Euler system in this setting. If we apply Mazur and Rubin's Euler systems to Kolyvagin systems map, we *only* obtain a Λ-adic Kolyvagin system for the canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ on $T \otimes \Lambda$, which is coarser than our modified Selmer structure $\mathcal{F}_{\mathbb{L}_\infty}$; and the techniques of [MR04] do not apply. We discuss how to obtain a Λ-adic Kolyvagin system for the modified Selmer structure $\mathcal{F}_{\mathbb{L}_\infty}$ starting with the Rubin-Stark elements, based on the methods of [Büy09a], and how to deduce the main conjectures using these Λ-adic Kolyvagin systems. In a forthcoming work [Büy09b], we extend the methods of [Büy09a] to verify all the speculative claims in §4.3.

In a forthcoming work [Büy08], the author gives another important arithmetic application of the first part of Theorem A (i.e., the rigidity of Λ-adic Kolyvagin systems) which we do not present here: He describes a relation between the Stickelberger elements and the Rubin-Stark elements for totally real fields. The existence of the Rubin-Stark elements is conjectural, whereas the existence of the Euler system of Stickelberger elements constructed in [Büy08] (see also [Kur03] for a construction of an Euler system using Stickelberger elements in a different way) rely only on a special case of Brumer's conjecture, which is proved in a variety of cases (c.f., [Wil90a, Kur03, Gre04]) from Wiles' proof[2] of the main conjectures [Wil90b].

We would also like to point out that the rigidity phenomenon for Kolyvagin systems plays a central role in a recent work of Mazur and Rubin [MR09], where they prove an important portion of Darmon's conjecture [Dar95].

There are three main steps in proving Theorem A. Let us give a brief outline of these in this paragraph. Let γ be a topological generator of Γ and let $R_{k,m}$ be the artinian ring $\Lambda/(\mathfrak{m}^k, (\gamma-1)^k)$ with $k, m \in \mathbb{Z}^+$. The main idea of the current article is to consider "non-arithmetic specializations" (as Ochiai [Och05] also calls them) $T_{k,m} := T \otimes R_{k,m}$ of the *big* Galois representation $T \otimes \Lambda$. The first step is to choose (see §2.4) a collection of *Kolyvagin primes* $\mathcal{P}_{k,m}$ for each $G_\mathbb{Q}$-representation $T_{k,m}$. The second step is the construction (see §2.7) of what Mazur and Rubin call the *core vertices* for the canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ on $T_{k,m}$. This construction builds on the ideas developed in [MR04, §4.1], however, the situation in this paper is technically more involved as one has to deal with two-dimensional artinian coefficient rings $R_{k,m}$, whereas Mazur and Rubin give a construction of core vertices for principal artinian coefficient rings. To achieve this, we use an Iwasawa theoretic control mechanism in order to give an upper bound on the size of certain Selmer groups (see Lemma 2.28 and Proposition 2.30) and an argument based on global duality to give a lower bound on the size of these Selmer groups (see Proposition 2.31). In the final step, we prove (see §3.1) mostly following Howard's arguments in [MR04, Appendix B] that there is a canonical isomorphism from the $R_{k,m}$-module $\mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k,m})$ onto the module $H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{k,m})$, for any core vertex n. Furthermore, these isomorphisms are compatible with the base change maps $T_{k,m} \to T_{k',m'}$, which allows us to patch them together and construct (in §3.2) the sought after classes inside $H^1(\mathbb{Q}, T \otimes \Lambda)$.

---

[2]The author has been warned that there might be a gap in Wiles' proof of Brumer's conjecture and his proof of the main conjecture for totally real fields in [Wil90b]. He was also told that Buzzard and Taylor are able to mend this problem by making use of the recent developments in the theory of p-adic Hilbert modular forms.

Theorem A, particularly the second part, can be interpreted as a deformation theoretical result: We prove that a Kolyvagin system for the $\mathcal{O}$-representation T can be deformed to a Λ-adic Kolyvagin system for the *cyclotomic deformation* $T \otimes \Lambda$ of T. Although we restrict our attention to the case of cyclotomic deformations of Galois representations in this paper, one hopes that our formalism would apply in a similar way for other deformations of T. For example, consider an elliptic curve E defined over $\mathbb{Q}$ and let $T = T_p(E)$ be its p-adic Tate module. In this setting, Kato has constructed an Euler system, which gives rise to a Kolyvagin system for the cyclotomic deformation of T. Ochiai [Och05] proved that this Euler system may be further deformed to a *big* Euler system for the nearly ordinary deformation of T under certain technical hypotheses (most notable of which is the assumption that the deformation ring in question is a power series ring). An appropriate generalization of Theorem A (and the work of Ochiai) should say similarly that for a general Galois representation T, the Kolyvagin systems which Mazur and Rubin [MR04] prove to exist may be deformed to Kolyvagin systems for various types of deformations of T.

2. CORE VERTICES OVER Λ

2.1. **Preliminaries.** Let T be a free $\mathcal{O}$-module of finite rank, on which the absolute Galois group $G_{\mathbb{Q}}$ acts continuously, and let $V = T \otimes \Phi$, and $A = V/T$. We will denote $G_{\mathbb{Q}_\ell}$ by $\mathcal{D}_\ell$ whenever we wish to identify this group with a closed subgroup of $G_{\mathbb{Q}}$; namely with a particular decomposition group at ℓ. We further define $\mathcal{I}_\ell \subset \mathcal{D}_\ell$ to be the inertia group and $\mathrm{Fr}_\ell \in \mathcal{D}_\ell/\mathcal{I}_\ell$ to be the arithmetic Frobenius element at ℓ. We also write $\mathbb{Q}_\ell^{\mathrm{unr}} \subset \overline{\mathbb{Q}}_\ell$ for the maximal unramified subfield of $\overline{\mathbb{Q}}_\ell$.

Let $\boldsymbol{\mu}_{p^n} \subset \overline{\mathbb{Q}}$ be the p^n-th roots of unity and $\boldsymbol{\mu}_{p^\infty} = \varinjlim_n \boldsymbol{\mu}_{p^n}$. For any ring R, an ideal $\mathfrak{a} \subset R$ and any R-module M, write $M[\mathfrak{a}]$ for the submodule killed by the elements of $\mathfrak{a}$.

Let $\Lambda := \mathcal{O}[[\Gamma]]$, with $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ and $\mathbb{Q}_\infty$ the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Fixing a topological generator γ of Γ, we may identify Λ with the power series ring $\mathcal{O}[[\gamma - 1]]$ in one variable over $\mathcal{O}$, and we will occasionally do so, denoting $\gamma - 1$ by $\mathbf{X}$. We will consider modules $T_f := T \otimes \Lambda/(f)$ and $T_{k,f} := T \otimes \Lambda/(\mathfrak{m}^k, f)$, where k is a positive integer and f is an element of Λ such that the quotient $\Lambda/(f)$ is free of non-zero finite rank over $\mathcal{O}$. Such an element $f \in \Lambda$ will be called a *distinguished power series*. We will let $G_{\mathbb{Q}}$ act on the tensor products above via acting on both factors. For $\ell \neq p$, the inertia subgroup $\mathcal{I}_\ell$ acts trivially on Λ, hence T_f (resp., $T_{k,f}$) is ramified at ℓ if and only if T (resp., $T/\mathfrak{m}^k T$) is ramified at ℓ.

We recall a definition from [MR04, §2].

Definition 2.1. Let M be any $\mathcal{O}[[G_{\mathbb{Q}}]]$-module. A *Selmer structure* $\mathcal{F}$ on M is a collection of the following data:

- A finite set $\Sigma(\mathcal{F})$ of places of $\mathbb{Q}$, including ∞, p, and all primes where M is ramified.
- For every $\ell \in \Sigma(\mathcal{F})$, a local condition on M (which we now view as a $\mathbb{Z}_p[[\mathcal{D}_\ell]]$-module), i.e., a choice of an $\mathcal{O}$-submodule $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, M) \subset H^1(\mathbb{Q}_\ell, M)$.

Definition 2.2. A *Selmer triple* is a triple $(T, \mathcal{F}, \mathcal{P})$ where $\mathcal{F}$ is a Selmer structure on T and $\mathcal{P}$ is a set of rational primes, disjoint from $\Sigma(\mathcal{F})$.

Define $\mathcal{F}_{\mathrm{can}}$, the *canonical Selmer structure*, on $T \otimes \Lambda/(f)$ as follows:

- $\Sigma(\mathcal{F}_{\mathrm{can}}) = \{\ell : T \text{ is ramified at } \ell\} \cup \{p, \infty\}$.
-
$$H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, T_f) := \begin{cases} H^1(\mathbb{Q}_p, T_f) & , \text{ if } \ell = p, \\ H^1_f(\mathbb{Q}_\ell, T_f) & , \text{ if } \ell \in \Sigma(\mathcal{F}_{\mathrm{can}}) - \{p, \infty\}. \end{cases}$$

Here $H^1_f(\mathbb{Q}_\ell, T_f) := \ker\{H^1(\mathbb{Q}_\ell, T_f) \longrightarrow H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, T_f \otimes \Phi)\}$, where, for any $\mathcal{O}[[G_{\mathbb{Q}_\ell}]]$-module M, we define

$$H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, M) := \ker\{H^1(\mathbb{Q}_\ell, M) \longrightarrow H^1(\mathbb{Q}_\ell^{\mathrm{unr}}, M)) = H^1(\mathbb{Q}_\ell^{\mathrm{unr}}/\mathbb{Q}_\ell, M^{\mathcal{I}_\ell})\}$$

as in [MR04, Definitions 1.1.6 and 3.2.1].

We denote the Selmer structure on the quotients $T_{k,f}$ obtained by *propagating* the local conditions given by $\mathcal{F}_{\mathrm{can}}$ on T_f to $T_{k,f}$ also by $\mathcal{F}_{\mathrm{can}}$. See [MR04, Example 1.1.2] for a definition of the *propagation* of local conditions.

The main objective of this Section is to prove, under the assumptions listed below, the existence of *core vertices* for the Selmer structure $\mathcal{F}_{\mathrm{can}}$ on $T_{k,m} := T_{k,\mathbf{X}^m}$ (see Theorem 2.27).

Definition 2.3. Let $\boldsymbol{\mu}_\ell$ denote group ℓ-th roots of unity inside $\overline{\mathbb{Q}}_\ell$. For a $\mathcal{O}[[\mathcal{D}_\ell]]$-module M which is finite over $\mathcal{O}$, the submodule

$$H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, M) := H^1\left(\mathbb{Q}_\ell(\boldsymbol{\mu}_\ell)/\mathbb{Q}_\ell, H^0(\mathbb{Q}(\boldsymbol{\mu}_\ell), M)\right) \subset H^1(\mathbb{Q}_\ell, M)$$

chosen as the local condition is called the *transverse condition* on M at ℓ.

We will often make use of the following notation from [MR04]:

Definition 2.4. Let $a, b, c \in \mathbb{Z}^+$ be pairwise coprime, and assume that c is not divisible by any prime in $\Sigma(\mathcal{F})$. Then we write $\mathcal{F}^a_b(c)$ for the Selmer structure on a $\mathcal{O}[[G_\mathbb{Q}]]$-module M given by

- $\Sigma(\mathcal{F}^a_b(c)) = \Sigma(\mathcal{F}) \cup \{\ell : \ell \mid abc\}$
- $H^1_{\mathcal{F}^a_b(c)}(\mathbb{Q}_\ell, M) = \begin{cases} H^1_{\mathcal{F}}(\mathbb{Q}_\ell, M) & , \text{ if } \ell \in \Sigma(\mathcal{F}) \text{ and } \ell \nmid ab \\ H^1(\mathbb{Q}_\ell, M) & , \text{ if } \ell \mid a \\ 0 & , \text{ if } \ell \mid b \\ H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, M) & , \text{ if } \ell \mid c \end{cases}$

Whenever any of a, b, c equals 1, we will suppress it from the notation.

2.2. **Hypotheses on T.**

We will be assuming all the hypotheses introduced in [MR04, §3.5], except for **H**.**5** and **H**.**6**:

(**H**.1) $T/\mathfrak{m}T$ is an absolutely irreducible $\mathbb{F}[[G_\mathbb{Q}]]$-representation.

(**H**.2) There is a $\tau \in G_\mathbb{Q}$ such that $\tau = 1$ on $\boldsymbol{\mu}_{p^\infty}$ and the $\mathcal{O}$-module $T/(\tau - 1)T$ is free of rank one.

(**H**.3) $H^1(\mathbb{Q}(T, \boldsymbol{\mu}_{p^\infty})/\mathbb{Q}, T/\mathfrak{m}T) = H^1(\mathbb{Q}(T, \boldsymbol{\mu}_{p^\infty})/\mathbb{Q}, T^*[\mathfrak{m}]) = 0$.
    Here, $\mathbb{Q}(T)$ is the smallest extension of $\mathbb{Q}$ such that the $G_\mathbb{Q}$-action on T factors through $\mathrm{Gal}(\mathbb{Q}(T)/\mathbb{Q})$ and $\mathbb{Q}(T, \boldsymbol{\mu}_{p^\infty}) = \mathbb{Q}(T)(\boldsymbol{\mu}_{p^\infty})$.

(**H**.4) Either $\mathrm{Hom}_{\mathbb{F}[[G_\mathbb{Q}]]}(T/\mathfrak{m}T, T^*[\mathfrak{m}]) = 0$, or $p > 4$.

In addition to the hypothesis **H**.1-**H**.4, we will need the following assumptions for the main results of this paper:

(ℍ.**T**) *Tamagawa Condition*: The $\mathcal{O}$-module $A^{\mathcal{I}_\ell}$ is divisible for every $\ell \neq p$.

(ℍ.**sEZ**) *Strong Exceptional Zero-like Condition*: $H^0(\mathbb{Q}_p, T^*) = 0$.

We will also consider the following weaker version of ℍ.**sEZ**:

(ℍ.**EZ**) *Exceptional Zero-like Condition*: $H^0(\mathbb{Q}_p, T^*)$ is finite.

We will later choose a set of rational primes $\mathcal{P}_{k,m}$ (in §2.4 below) and verify that the analogues of hypotheses **H**.5 and **H**.6 of [MR04, §3.5] hold for the collection $\{\mathcal{P}_{k,m}\}$ and for the Selmer structures $\mathcal{F}_{\mathrm{can}}(n)$, for every $n \in \mathcal{N}_{k,m} := \{\text{square free products of primes in } \mathcal{P}_{k,m}\}$.

2.3. **Cartesian Property for $\mathcal{F}_{\mathbf{can}}$ on $T \otimes \Lambda$.**

Recall that an element $f \in \Lambda$ is called a *distinguished power series* if $\Lambda/(f)$ is a free $\mathcal{O}$-module of finite non-zero rank. Let $\mathcal{T} = \{T_{k,f}\}$ denote the collection of quotients of $T \otimes \Lambda$, where f ranges over distinguished power series and $k \in \mathbb{Z}^+ \cup \{+\infty\}$ (with the convention that $T_{k,f} = T_f$ when $k = +\infty$).

The main theorems of this paper will only concern the sub-collection

$$\mathcal{T}_0 = \{T_{k,\mathbf{X}^m} : k \in \mathbb{Z}^+ \cup \{\infty\}, m \in \mathbb{Z}^+\} \subset \mathcal{T},$$

yet we still give the proofs of certain auxiliary facts in greater generality for the sake of clarity.

Definition 2.5. A local condition $\mathcal{F}$ is *cartesian* on $\mathcal{T}$ if it satisfies the following conditions for every prime:

(**C1**) (Functoriality) If f and g are distinguished polynomials and $k \le k'$ are positive integers then

  (**C1.a**) $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k,f})$ is the image of $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k',f})$ under the canonical map

$$H^1(\mathbb{Q}_\ell, T_{k',f}) \longrightarrow H^1(\mathbb{Q}_\ell, T_{k,f}), \text{ and}$$

  (**C1.b**) $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k,f})$ is the image of $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k,fg})$ under the canonical map

$$H^1(\mathbb{Q}_\ell, T_{k,fg}) \longrightarrow H^1(\mathbb{Q}_\ell, T_{k,f}).$$

(**C2**) (Cartesian condition over power series) If f and g are distinguished power series and $k \in \mathbb{Z}^+$, then $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k,f})$ is the inverse image of $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k,fg})$ under the natural map

$$H^1(\mathbb{Q}_\ell, T_{k,f}) \longrightarrow H^1(\mathbb{Q}_\ell, T_{k,fg}),$$

  which is induced from the injection $T_{k,f} \xrightarrow{[g]} T_{k,fg}$, where $[g]$ stands for multiplication by g.

(**C3**) (Cartesian condition over powers of p) If f is a distinguished power series and $k \le k'$ are positive integers, then $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k,f})$ is the inverse image of $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k',f})$ under the natural map $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k,f}) \longrightarrow H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k',f})$, which is induced from the injection $T_{k,f} \xrightarrow{[p^{k'-k}]} T_{k',f}$, where $[p^{k'-k}]$ is the multiplication by $p^{k'-k}$.

Condition **C1** may sometimes be replaced by the weaker:

(**C1′**) (weak Functoriality) If f and g are distinguished power series and $k \le k'$ are positive integers then

  (**C1′.a**) $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k,f})$ lies inside the image of $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k',f})$ under the canonical map

$$H^1(\mathbb{Q}_\ell, T_{k',f}) \longrightarrow H^1(\mathbb{Q}_\ell, T_{k,f}),$$

  (**C1′.b**) $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k,f})$ lies inside the image of $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T_{k,fg})$ under the canonical map

$$H^1(\mathbb{Q}_\ell, T_{k,fg}) \longrightarrow H^1(\mathbb{Q}_\ell, T_{k,f}).$$

which is sufficient for most of our purposes. When a Selmer structure $\mathcal{F}$ satisfies **C1′**, **C2** and **C3** we still say $\mathcal{F}$ is *weakly cartesian* on $\mathcal{T}$.

In this section, we will check the cartesian properties for $\mathcal{F}_{\mathrm{can}}$ and for $\mathcal{F}_{\mathrm{can}}(n)$ on certain sub-collections of $\mathcal{T}$. We remark that the local condition $\mathcal{F}_{\mathrm{can}}$ on $T_{k,f}$ is obtained by propagating $\mathcal{F}_{\mathrm{can}}$ defined on T_f. Hence the condition **C1.a** of Definition 2.5 is automatically satisfied for $\mathcal{F}_{\mathrm{can}}$.

Since we assume $p > 2$, we have $H^1(\mathbb{R}, T) = 0$, hence the local conditions at the infinite place will be forced to be *zero*. We therefore trivially have the cartesian property at ∞, regardless of the choice of a Selmer structure.

2.3.1. *Cartesian property at $\ell \ne p$.* Throughout this section, ℓ denotes a rational prime other than p and we assume $\mathbb{H}.\mathbf{T}$. Note that if $\ell \notin \Sigma(\mathcal{F}_{\mathrm{can}})$, then $A^{\mathcal{I}_\ell} = A$ and therefore $A^{\mathcal{I}_\ell}$ is divisible. Hence, $\mathbb{H}.\mathbf{T}$ is satisfied for primes $\ell \notin \Sigma(\mathcal{F}_{\mathrm{can}})$.

Lemma 2.6. *For any distinguished power series $f \in \Lambda$, the $\mathcal{O}$-module $A_f^{\mathcal{I}_\ell}$ is divisible.*

Proof. Since $\ell \ne p$, the inertia group $\mathcal{I}_\ell$ acts trivially on $\Lambda/(f)$, hence $A_f^{\mathcal{I}_\ell} = A^{\mathcal{I}_\ell} \otimes \Lambda/(f)$. $\qquad\square$

Let V_f denote the Φ-vector space $T_f \otimes \Phi$, and A_f denote V_f/T_f. Note that there is a natural injection $T_{k,f} \hookrightarrow A_f$; in fact, we may identify the image of $T_{k,f}$ under this injection with the $\mathfrak{m}^k$-torsion subgroup $A_f[\mathfrak{m}^k] \subset A_f$.

Recall the definition of the unramified local cohomology group

$$H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, V_f) := \ker\{H^1(\mathbb{Q}_\ell, V_f) \longrightarrow H^1(\mathcal{I}_\ell, V_f)\} \cong H^1(\mathbb{Q}_\ell^{\mathrm{unr}}/\mathbb{Q}_\ell, V_f^{\mathcal{I}_\ell}).$$

We define $H^1_f(\mathbb{Q}_\ell, A_f)$ as the image of $H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, V_f)$ under the natural map

$$H^1(\mathbb{Q}_\ell, V_f) \longrightarrow H^1(\mathbb{Q}_\ell, A_f).$$

We also define $H^1_f(\mathbb{Q}_\ell, T_{k,f})$ as the inverse image of $H^1_f(\mathbb{Q}_\ell, A_f)$ under the map $H^1(\mathbb{Q}_\ell, T_{k,f}) \to H^1(\mathbb{Q}_\ell, A_f)$, which is induced from the injection $T_{k,f} \hookrightarrow A_f$.

Lemma 2.7. [Rub00, Lemma 1.3.8(i)] $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, T_{k,f}) = H^1_f(\mathbb{Q}_\ell, T_{k,f})$.

Lemma 2.8. [Rub00, Lemma 1.3.5] *For every $\ell \neq p$, the following sequences are exact:*
  (i) $0 \longrightarrow H^1_f(\mathbb{Q}_\ell, A_f) \longrightarrow H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, A_f) \longrightarrow \mathcal{W}_f/(\mathrm{Fr}_\ell - 1)\mathcal{W}_f \longrightarrow 0,$
  (ii) $0 \longrightarrow H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, T_f) \longrightarrow H^1_f(\mathbb{Q}_\ell, T_f) \longrightarrow \mathcal{W}_f^{\mathrm{Fr}_\ell = 1} \longrightarrow 0.$

with $\mathcal{W}_f = A_f^{\mathcal{I}_\ell}/(A_f^{\mathcal{I}_\ell})_{\mathrm{div}}$ and M_{div} stands for the maximal divisible submodule of an $\mathcal{O}$-module M.

As an immediate consequence of Lemma 2.8, we obtain:

Corollary 2.9. *If $\mathbb{H}.\mathbf{T}$ holds, then $H^1_f(\mathbb{Q}_\ell, A_f) = H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, A_f)$ and $H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, T_f) = H^1_f(\mathbb{Q}_\ell, T_f)$ for every $\ell \neq p$.*

Corollary 2.10. *Assume $\mathbb{H}.\mathbf{T}$ holds. Then $H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, T_{k,f})$ is the image of $H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, T_f)$ under the map $H^1(\mathbb{Q}_\ell, T_f) \to H^1(\mathbb{Q}_\ell, T_{k,f})$ restricted to $H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, T_f)$.*

Proof. By Lemma 2.7, Lemma 2.8 and Corollary 2.9 we have the following diagram:

$$
\begin{array}{ccccccc}
H^1_f(\mathbb{Q}_\ell, T_{k,f}) & = & \mathrm{image}(H^1_f(\mathbb{Q}_\ell, T_f)) & = & \mathrm{image}(H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, T_f)) & \subset & H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, T_{k,f}) \\
\| & & & & & & \\
H^1_f(\mathbb{Q}_\ell, T_{k,f}) & = & \iota_{k,f}^{-1}(H^1_f(\mathbb{Q}_\ell, A_f)) & = & \iota_{k,f}^{-1}(H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, A_f)) & \supset & H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, T_{k,f})
\end{array}
$$

which shows that all the containments above are in fact equalities. This completes the proof. $\square$

Proposition 2.11. *Assuming $\mathbb{H}.\mathbf{T}$, the canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ is cartesian on $\mathcal{T}$ at $\ell \neq p$.*

Proof. As we have remarked earlier, **C1.a** is satisfied by the definition of $\mathcal{F}_{\mathrm{can}}$ on $\mathcal{T}$.

C1.b also follows from Lemma 2.7, Lemma 2.9 and Corollary 2.10.

We next check **C2**. Suppose f and g are any distinguished power series. Let V_f and A_f be as above. Then we have the following commutative diagram with exact rows:

(1)
$$
\begin{array}{ccccccc}
0 & \longrightarrow & H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, T_{k,f}) & \longrightarrow & H^1(\mathbb{Q}_\ell, T_{k,f}) & \longrightarrow & \dfrac{H^1(\mathbb{Q}_\ell, A_f)}{H^1_f(\mathbb{Q}_\ell, A_f)} \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, T_{k,fg}) & \longrightarrow & H^1(\mathbb{Q}_\ell, T_{k,fg}) & \longrightarrow & \dfrac{H^1(\mathbb{Q}_\ell, A_{fg})}{H^1_f(\mathbb{Q}_\ell, A_{fg})}
\end{array}
$$

The rows are exact by Lemma 2.7 and the vertical maps are all induced from the multiplication by g map $[g] : \Lambda/(f) \to \Lambda/(fg)$.

Using the Hochschild-Serre spectral sequence and the fact that the cohomological dimension of $\mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{unr}}/\mathbb{Q}_\ell) \cong \hat{\mathbb{Z}}$ is one, we obtain the following diagram:

(2)
$$
\begin{array}{ccccc}
\dfrac{H^1(\mathbb{Q}_\ell, A_f)}{H^1(\mathbb{Q}_\ell^{\mathrm{unr}}/\mathbb{Q}_\ell, A_f(\mathcal{I}_\ell))} & \xrightarrow{\ \sim\ } & H^1(\mathbb{Q}_\ell^{\mathrm{unr}}, A_f)^{\mathrm{Fr}_\ell=1} & = & H^1(\mathcal{I}_\ell, A_f)^{\mathrm{Fr}_\ell=1} \\
\downarrow & & \downarrow & & \downarrow \\
\dfrac{H^1(\mathbb{Q}_\ell, A_{fg})}{H^1(\mathbb{Q}_\ell^{\mathrm{unr}}/\mathbb{Q}_\ell, A_{fg}(\mathcal{I}_\ell))} & \xrightarrow{\ \sim\ } & H^1(\mathbb{Q}_\ell^{\mathrm{unr}}, A_{fg})^{\mathrm{Fr}_\ell=1} & = & H^1(\mathcal{I}_\ell, A_{fg})^{\mathrm{Fr}_\ell=1}
\end{array}
$$

where $A_f(\mathcal{I}_\ell) := A_f^{\mathcal{I}_\ell}$. Further, the $\mathcal{I}_\ell$-cohomology of the exact sequence

(3)
$$
\begin{array}{ccccc}
A_f & & A_{fg} & & A_g \\
\| & & \| & & \| \\
0 \longrightarrow A \otimes \Lambda/(f) & \xrightarrow{[g]} & A \otimes \Lambda/(fg) \longrightarrow & A \otimes \Lambda/(g) & \longrightarrow 0
\end{array}
$$

(which exists because of the division algorithm for distinguished polynomials, see [Was82, §7]) gives, using the proof of Lemma 2.6,

$$
0 \longrightarrow A^{\mathcal{I}_\ell} \otimes \Lambda/(f) \xrightarrow{[g]} A^{\mathcal{I}_\ell} \otimes \Lambda/(fg) \longrightarrow A^{\mathcal{I}_\ell} \otimes \Lambda/(g).
$$

Since tensoring with $A^{\mathcal{I}_\ell}$ is right exact, the very right map in the exact sequence above is in fact surjective, thus the following sequence is exact:

(4)
$$
0 \longrightarrow A^{\mathcal{I}_\ell} \otimes \Lambda/(f) \xrightarrow{[g]} A^{\mathcal{I}_\ell} \otimes \Lambda/(fg) \longrightarrow A^{\mathcal{I}_\ell} \otimes \Lambda/(g) \longrightarrow 0
$$

Furthermore, the $\mathcal{I}_\ell$-cohomology of the exact sequence (3) and the exact sequence (4) give rise to the following diagram with exact rows:

$$
\begin{array}{ccccccc}
H^0(\mathcal{I}_\ell, A_{fg}) & \longrightarrow & H^0(\mathcal{I}_\ell, A_g) & \longrightarrow & H^1(\mathcal{I}_\ell, A_f) & \longrightarrow & H^1(\mathcal{I}_\ell, A_{fg}) \\
\| & & \| & & & & \\
A^{\mathcal{I}_\ell} \otimes \Lambda/(fg) & \longrightarrow & A^{\mathcal{I}_\ell} \otimes \Lambda/(g) & \longrightarrow & 0 & &
\end{array}
$$

This shows that the map $H^1(\mathcal{I}_\ell, A_f) \to H^1(\mathcal{I}_\ell, A_{fg})$ is injective and therefore the map on the right hand side in (2) is also injective (as well as the map on the left hand side), hence

(5)
$$
H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, A_f) = \ker\left(H^1(\mathbb{Q}_\ell, A_f) \longrightarrow \frac{H^1(\mathbb{Q}_\ell, A_{fg})}{H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, A_{fg})} \right).
$$

Since we assumed $\mathbb{H}.\mathbf{T}$, it follows by Corollary 2.9 that $H^1_f(\mathbb{Q}_\ell, A_f) = H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, A_f)$ for every distinguished power series f. This in turn implies, using (5),

$$
H^1_f(\mathbb{Q}_\ell, A_f) = \ker\left(H^1(\mathbb{Q}_\ell, A_f) \longrightarrow \frac{H^1(\mathbb{Q}_\ell, A_{fg})}{H^1_f(\mathbb{Q}_\ell, A_{fg})} \right).
$$

But this means that the rightmost map in (1) is injective, therefore

$$
H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, T_{k,f}) = \ker\left(H^1(\mathbb{Q}_\ell, T_{k,f}) \longrightarrow \frac{H^1(\mathbb{Q}_\ell, T_{k,fg})}{H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, T_{k,fg})} \right)
$$

which is the property $\mathbf{C2}$ in Definition 2.5.

To verify the property $\mathbf{C3}$ in Definition 2.5, note that by the definition of $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, T_f)$, we have an injection

$$
H^1(\mathbb{Q}_\ell, T_f)/H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, T_f) \hookrightarrow H^1(\mathbb{Q}_\ell, V_f)/H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, V_f),
$$

which shows that $H^1(\mathbb{Q}_\ell, T_f)/H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, T_f)$ is $\mathcal{O}$-torsion free. Property $\mathbf{C3}$ now follows from [MR04, Lemma 3.7.1(i)]. $\qquad\square$

2.3.2. *Cartesian property at p.* In this section we verify that $\mathcal{F}_{\mathrm{can}}$ is cartesian on the collection

$$\mathcal{T}_0 = \{T_{k,\mathbf{X}^m} : k, m \in \mathbb{Z}^+\} \subset \mathcal{T}.$$

We will write $T_{k,m}$ instead of $T_{k,\mathbf{X}^m}$, and T_m instead of $T_{\mathbf{X}^m}$ for notational convenience. Define also $R_{k,m} := \Lambda/(\mathfrak{m}^k, \mathbf{X}^m)$ for every $k, m \in \mathbb{Z}^+$.

Throughout this section we assume that $\mathbb{H}.\mathbf{sEZ}$ holds.

Lemma 2.12. $H^2(\mathbb{Q}_p, T \otimes \Lambda) = 0.$

Proof. By local duality, $H^0(\mathbb{Q}_p, T^*) = 0$ if and only if $H^2(\mathbb{Q}_p, T) = 0$. Since the cohomological dimension of $G_{\mathbb{Q}_p}$ is 2 and since we assumed $\mathbb{H}.\mathbf{sEZ}$, it follows that

$$H^2(\mathbb{Q}_p, T \otimes \Lambda)/(\gamma - 1) \cong H^2(\mathbb{Q}_p, T) = 0.$$

Proof of Lemma now follows by Nakayama's lemma. $\qquad\square$

Proposition 2.13. *The canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ is cartesian on $\mathcal{T}_0$ (in the sense of Definition 2.5; but $\mathcal{T}$ replaced by $\mathcal{T}_0$) at the prime p.*

Proof. **C1.a** is satisfied by the definition of $\mathcal{F}_{\mathrm{can}}$ on $\mathcal{T}_0$.

The exact sequence

$$H^1(\mathbb{Q}_p, T \otimes \Lambda) \longrightarrow H^1(\mathbb{Q}_p, T_m) \longrightarrow H^2(\mathbb{Q}_p, T \otimes \Lambda)[(\gamma - 1)^m]$$

shows, by Lemma 2.12, that $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_p, T_m) = H^1(\mathbb{Q}_p, T_m) = \mathrm{image}(H^1(\mathbb{Q}_p, T \otimes \Lambda))$. Furthermore, the $G_{\mathbb{Q}_p}$-cohomology of the exact sequence

$$0 \longrightarrow T_m \xrightarrow{[\varpi^k]} T_m \longrightarrow T_{k,m} \longrightarrow 0$$

implies that $\mathrm{coker}\{H^1(\mathbb{Q}_p, T_m) \to H^1(\mathbb{Q}_p, T_{k,m})\} = H^2(\mathbb{Q}_p, T_m)[\mathfrak{m}^k]$. Since the cohomological dimension of $G_{\mathbb{Q}_p}$ is 2, it follows that

$$H^2(\mathbb{Q}_p, T_m) \cong H^2(\mathbb{Q}_p, T \otimes \Lambda)/(\gamma - 1)^m H^2(\mathbb{Q}_p, T \otimes \Lambda),$$

and this is *zero* by Lemma 2.12. We therefore see that

(6) $\qquad H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_p, T_{k,m}) := \mathrm{im}\{H^1(\mathbb{Q}_p, T \otimes \Lambda) \to H^1(\mathbb{Q}_p, T_{k,m})\} = H^1(\mathbb{Q}_p, T_{k,m}).$

It now follows from (6) that $\mathcal{F}_{\mathrm{can}}$ satisfies **C1.b**, **C2** and **C3**.

$\qquad\square$

Remark 2.14. For $\mathcal{F}_{\mathrm{can}}$ on $\mathcal{T}_0$ to satisfy condition **C2**, $\mathbb{H}.\mathbf{EZ}$ alone is not sufficient; we indeed need to assume $\mathbb{H}.\mathbf{sEZ}$. This is what we explain in this paragraph: We prove that $\mathbb{H}.\mathbf{EZ}$ together with **C2** for $\mathcal{F}_{\mathrm{can}}$ imply $\mathbb{H}.\mathbf{sEZ}$.

We have the following diagram with exact rows:

$$
\begin{array}{ccccccc}
H^1(\mathbb{Q}_p, T_1) & \longrightarrow & H^1(\mathbb{Q}_p, T_{k,1}) & \longrightarrow & H^2(\mathbb{Q}_p, T_1)[\mathfrak{m}^k] & \longrightarrow & 0 \\
\downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\theta} & & \\
H^1(\mathbb{Q}_p, T_{m+1}) & \longrightarrow & H^1(\mathbb{Q}_p, T_{k,m+1}) & \longrightarrow & H^2(\mathbb{Q}_p, T_{m+1})[\mathfrak{m}^k] & \longrightarrow & 0
\end{array}
$$

where α, β and θ are all induced from multiplication by $\mathbf{X}^m$. If **C2** is true, then this means θ is injective. Set $M = H^2(\mathbb{Q}_p, T \otimes \Lambda)$. It is well known that M is a finitely generated torsion Λ-module (c.f., [PR94b, Proposition 3.2.1]). Let $\mathrm{char}(M)$ denote the characteristic ideal of M. Then $\mathbb{H}.\mathbf{EZ}$ is equivalent to saying that $\mathbf{X} \nmid \mathrm{char}(M)$; which in return implies that $M/\mathbf{X}^r M$ is finite for all $r \in \mathbb{Z}^+$.

On the other hand, since the cohomological dimension of $G_{\mathbb{Q}_p}$ is 2,

$$H^2(\mathbb{Q}_p, T_1) \cong M/\mathbf{X}M, \text{ and } H^2(\mathbb{Q}_p, T_{m+1}) \cong M/\mathbf{X}^{m+1}M,$$

hence θ is given by

$$\theta : \{M/\mathbf{X}M\}[\mathfrak{m}^k] \longrightarrow \{M/\mathbf{X}^{m+1}M\}[\mathfrak{m}^k].$$

Further, since $M/\mathbf{X}M$ is finite, one can choose k large enough so that

$$\{M/\mathbf{X}M\}[\mathfrak{m}^k] = M/\mathbf{X}M, \text{ and } \{M/\mathbf{X}^{m+1}M\}[p^k] = M/\mathbf{X}^{m+1}M.$$

For such k, the kernel of θ is $(M[\mathbf{X}^m] + \mathbf{X}M)/\mathbf{X}M$, which is trivial since θ is injective. This means $M[\mathbf{X}^m] \subset \mathbf{X}M$ for all m. Let $M[\mathbf{X}^\infty] := \cup_{m \in \mathbb{Z}^+} M[\mathbf{X}^m]$. Then $M[\mathbf{X}^\infty] \subset \mathbf{X}M$; which shows that $M[\mathbf{X}^\infty]$ is in fact $\mathbf{X}$-divisible. But since M is finitely generated, this is impossible unless $M = 0$. As in the proof of Lemma 2.12, this is equivalent to $\mathbb{H}.\mathbf{sEZ}$.

2.4. Choosing a set of Kolyvagin primes.
In this section, we choose the set of primes $\mathcal{P}_{k,m}$ that were mentioned in §2.2. Let τ be as in $\mathbf{H}.\mathbf{2}$. Given $k, m \in \mathbb{Z}^+$, we define

$$\mathcal{P}_{k,m} := \{\ell : \mathrm{Fr}_\ell \text{ is conjugate to } \tau \text{ in } \mathrm{Gal}(\mathbb{Q}(T/\mathfrak{m}^{k+m}T, \boldsymbol{\mu}_{p^{k+m+1}})/\mathbb{Q})\},$$

where $\mathbb{Q}(T/\mathfrak{m}^{k+m}T, \boldsymbol{\mu}_{p^{k+m+1}})$ is the fixed field in $\overline{\mathbb{Q}}$ of the kernel of the map

$$G_\mathbb{Q} \longrightarrow \mathrm{Aut}(T/\mathfrak{m}^{k+m}T) \oplus \mathrm{Aut}(\boldsymbol{\mu}_{p^{k+m+1}}).$$

Note that $\mathcal{P}_{k,m}$ depends only on $k + m$; we may therefore define $\mathcal{P}_{k+m} := \mathcal{P}_{k,m}$. We set $\mathcal{P} := \mathcal{P}_2 = \mathcal{P}_{1,1}$. Note also that $\mathcal{P}_j \subset \mathcal{P}_i$ for all $j > i$.

Remark 2.15. If $\ell \in \mathcal{P}_{k,m}$, then by our definition Fr_ℓ is conjugate to τ in $\mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_{p^{k+m+1}})/\mathbb{Q})$, hence we have $\ell \equiv 1 \pmod{\mathfrak{m}^{k+m+1}}$, since $\tau = 1$ on $\boldsymbol{\mu}_{p^\infty}$.

Lemma 2.16. *For $\ell \in \mathcal{P}_{k,m}$, the Frobenius Fr_ℓ acts trivially on $\Lambda/(\mathfrak{m}^k, \mathbf{X}^m)$.*

Proof. Let γ be the fixed topological generator of Γ, such that $\gamma - 1$ corresponds to $\mathbf{X}$ under the identification of Λ with $\mathcal{O}[[\mathbf{X}]]$. The Frobenius Fr_ℓ acts on Λ through the natural surjection $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \Gamma$. Let $\overline{\mathrm{Fr}}_\ell$ be the image of Fr_ℓ under this map. Since Fr_ℓ and τ are conjugate in the group $\mathrm{Gal}(\mathbb{Q}(T/\mathfrak{m}^kT, \boldsymbol{\mu}_{p^{k+m+1}})/\mathbb{Q})$ (so also in $\mathrm{Gal}(\mathbb{Q}_{k+m}/\mathbb{Q})$, where $\mathbb{Q}_{k+m}$ is the $(k+m)$-layer of $\mathbb{Q}_\infty$), it follows from our assumption that $\tau = 1$ on $\boldsymbol{\mu}_{p^\infty}$ that $\overline{\mathrm{Fr}}_\ell = \gamma^\alpha$, with $\alpha \in \mathbb{Z}_p$ and has p-adic valuation at least $k + m$. Note that

$$\gamma^\alpha = (\gamma - 1 + 1)^\alpha \equiv (\gamma - 1)^\alpha + 1 \equiv 1 \bmod (\mathfrak{m}^k, (\gamma - 1)^m),$$

which completes the proof of Lemma. $\qquad\square$

Recall that $R_{k,m} := \Lambda/(\mathfrak{m}^k, \mathbf{X}^m)$ for $k, m \in \mathbb{Z}^+$.

Lemma 2.17. *For any $\ell \in \mathcal{P}_{k,m}$, the $R_{k,m}$-module $T_{k,m}/(\mathrm{Fr}_\ell - 1)T_{k,m}$ is free of rank one.*

Proof. By Lemma 2.16, $(\mathrm{Fr}_\ell - 1)T_{k,m} = \left[(\mathrm{Fr}_\ell - 1)(T/\mathfrak{m}^kT)\right] \otimes \Lambda/(\mathbf{X}^m)$. Since $(\mathrm{Fr}_\ell - 1)(T/\mathfrak{m}^kT) = (\mathfrak{m}^kT + (\mathrm{Fr}_\ell - 1)T)/\mathfrak{m}^kT$, it follows that

$$(7) \qquad\qquad (\mathrm{Fr}_\ell - 1)T_{k,m} = (\mathfrak{m}^kT + (\mathrm{Fr}_\ell - 1)T)/\mathfrak{m}^kT \otimes \Lambda/(\mathbf{X}^m)$$

Since $\Lambda/(\mathbf{X}^m)$ is a free $\mathcal{O}$-module, the functor $[- \otimes_\mathcal{O} \Lambda/\mathbf{X}^m]$ is exact. It therefore follows from (7) that

$$(8) \qquad\qquad T_{k,m}/(\mathrm{Fr}_\ell - 1)T_{k,m} = T/(\mathfrak{m}^kT + (\mathrm{Fr}_\ell - 1)T) \otimes \Lambda/(\mathbf{X}^m).$$

Since $\ell \in \mathcal{P}_{k,m}$, the $\mathcal{O}/\mathfrak{m}^k$-module $T/(\mathfrak{m}^k T + (\mathrm{Fr}_\ell - 1)T)$ is free of rank one. Now using (8), the proof of Lemma follows.

$\square$

Note that, by Remark 2.15 it follows that $|\mathbb{F}_\ell^\times| \cdot T_{k,m} = (\ell - 1) \cdot T_{k,m} = 0$, hence all the results proved in [MR04, §1.2] hold with the choice $R = R_{k,m}$ and the free $R_{k,m}$-module $T_{k,m}$. We record these results for future reference:

Lemma 2.18. [MR04, Lemma 1.2.1] *For $\ell \in \mathcal{P}_{k,m}$, there are canonical functorial isomorphisms*

  (i) $H_f^1(\mathbb{Q}_\ell, T_{k,m}) \cong T_{k,m}/(\mathrm{Fr}_\ell - 1)T_{k,m}$,
  (ii) $H_s^1(\mathbb{Q}_\ell, T_{k,m}) \otimes \mathbb{F}_\ell^\times \cong T_{k,m}^{\mathrm{Fr}_\ell = 1}$

Lemma 2.19. [MR04, Lemma 1.2.3] *For $\ell \in \mathcal{P}_{k,m}$, the finite-singular comparison map*

$$\phi_\ell^{\mathrm{fs}} : H_f^1(\mathbb{Q}_\ell, T_{k,m}) \longrightarrow H_s^1(\mathbb{Q}_\ell, T_{k,m}) \otimes \mathbb{F}_\ell^\times$$

(see [MR04] Definition 1.2.2) is an isomorphism. In particular, both $H_f^1(\mathbb{Q}_\ell, T_{k,m})$ and $H_s^1(\mathbb{Q}_\ell, T_{k,m})$ are free of rank one over $R_{k,m}$.

2.5. **The Transverse Condition.** In this section we study the properties of the *transverse condition* (recall Definition 2.3 above) at primes $\ell \in \mathcal{P}_{k,m}$. Compare the facts we record in this section to Definition 1.1.6(iv), §1.2 and Lemma 3.7.4 of [MR04].

As remarked earlier, if $\ell \in \mathcal{P}_{k,m}$, then the results from [MR04, §1.2] still apply. In particular:

Lemma 2.20. *The transverse subgroup $H_{\mathrm{tr}}^1(\mathbb{Q}_\ell, T_{k,m}) \subset H^1(\mathbb{Q}_\ell, T_{k,m})$ projects isomorphically onto $H_s^1(\mathbb{Q}_\ell, T_{k,m})$ in the exact sequence*

$$0 \longrightarrow H_f^1(\mathbb{Q}_\ell, T_{k,m}) \longrightarrow H^1(\mathbb{Q}_\ell, T_{k,m}) \longrightarrow H_s^1(\mathbb{Q}_\ell, T_{k,m}) \longrightarrow 0$$

In other words, the sequence above has a functorial splitting

$$H^1(\mathbb{Q}_\ell, T_{k,m}) = H_f^1(\mathbb{Q}_\ell, T_{k,m}) \oplus H_{\mathrm{tr}}^1(\mathbb{Q}_\ell, T_{k,m}).$$

2.6. **Cartesian Property of $\mathcal{F}_{\mathbf{can}}(n)$.** Recall $\mathcal{N}_{k,m} = \{$square free products of primes in $\mathcal{P}_{k,m}\}$. In this section, we verify that the modified Selmer structure $\mathcal{F}_{\mathrm{can}}(n)$ (given as in Definition 2.4) is cartesian on the collection of Λ-modules $\mathcal{T}_{k,m} := \{T_{\alpha,\beta}\}_{\substack{\alpha \leq k \\ \beta \leq m}}$, for every $n \in \mathcal{N}_{k,m}$.

Proposition 2.21. (Compare to [MR04] Lemma 3.7.4) *For every $\ell \in \mathcal{P}_{k,m}$, the transverse condition at ℓ is cartesian on the collection of quotients $\mathcal{T}_{k,m}$.*

Proof. Let $n \leq N \leq m$ and $l \leq L \leq k$ be positive integers. For $\ell \in \mathcal{P}_{k,m}$, we have the following commutative diagram by Lemma 2.20:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & H_{\mathrm{tr}}^1(\mathbb{Q}_\ell, T_{L,N}) & \longrightarrow & H^1(\mathbb{Q}_\ell, T_{L,N}) & \longrightarrow & H_f^1(\mathbb{Q}_\ell, T_{L,N}) & \longrightarrow & 0 \\
& & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H_{\mathrm{tr}}^1(\mathbb{Q}_\ell, T_{l,n}) & \longrightarrow & H^1(\mathbb{Q}_\ell, T_{l,n}) & \longrightarrow & H_f^1(\mathbb{Q}_\ell, T_{l,n}) & \longrightarrow & 0
\end{array}
$$

where the vertical maps are induced by canonical surjection $T_{L,N} \twoheadrightarrow T_{l,n}$. This diagram shows that $H_{\mathrm{tr}}^1(\mathbb{Q}_\ell, T_{L,N}) = \ker\{H^1(\mathbb{Q}_\ell, T_{L,N}) \to H_f^1(\mathbb{Q}_\ell, T_{L,N})\}$ is mapped into

$$H_{\mathrm{tr}}^1(\mathbb{Q}_\ell, T_{l,n}) = \ker\{H^1(\mathbb{Q}_\ell, T_{l,n}) \longrightarrow H_f^1(\mathbb{Q}_\ell, T_{l,n})\}$$

under the map $H^1(\mathbb{Q}_\ell, T_{L,N}) \to H^1(\mathbb{Q}_\ell, T_{l,n})$. This shows that the transverse condition satisfies **C1'**. By Lemma 2.18 and 2.19, we have that $T_{L,N}^{\mathrm{Fr}_\ell=1}$ (resp., $T_{l,n}^{\mathrm{Fr}_\ell=1}$) is a free $R_{L,N}$-module (resp., $R_{l,n}$-module) of rank one. Hence the functorial map below induced from $T_{L,N} \twoheadrightarrow T_{l,n}$ is surjective:

$$T_{L,N}^{\mathrm{Fr}_\ell=1} \cong H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_{L,N}) \otimes \mathbb{F}_\ell^\times \longrightarrow H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_{l,n}) \otimes \mathbb{F}_\ell^\times \cong T_{l,n}^{\mathrm{Fr}_\ell=1}.$$

This shows that **C1** holds as well.

By Lemma 2.20, we have the following commutative diagram, where the isomorphisms on the right come from Lemma 2.18:

$$
(9) \quad
\begin{array}{ccccc}
H^1(\mathbb{Q}_\ell, T_{k,n}) & \twoheadrightarrow & H^1_f(\mathbb{Q}_\ell, T_{k,n}) & \overset{\sim}{\longrightarrow} & T_{k,n}/(\mathrm{Fr}_\ell - 1)T_{k,n} \\
\downarrow {\scriptstyle [\mathbf{X}^{N-n}]} & & \downarrow {\scriptstyle [\mathbf{X}^{N-n}]} & & \downarrow {\scriptstyle [\mathbf{X}^{N-n}]} \\
H^1(\mathbb{Q}_\ell, T_{k,N}) & \twoheadrightarrow & H^1_f(\mathbb{Q}_\ell, T_{k,N}) & \overset{\sim}{\longrightarrow} & T_{k,N}/(\mathrm{Fr}_\ell - 1)T_{k,N}
\end{array}
$$

Since $T_{k,n}/(\mathrm{Fr}_\ell - 1)T_{k,n}$ (resp., $T_{k,N}/(\mathrm{Fr}_\ell - 1)T_{k,N}$) is a free $R_{k,n}$-module (resp., $R_{k,N}$-module) of rank one by Lemma 2.19, and since the map $[\mathbf{X}^{N-n}] : R_{k,n} \to R_{k,N}$ is injective, it follows that the the vertical map on the right is injective. So, if $c \in H^1(\mathbb{Q}_\ell, T_{k,n})$ and $[\mathbf{X}^{N-n}]c$ projects to *zero* in $H^1_f(\mathbb{Q}_\ell, T_{k,N})$, then c projects to *zero* in $H^1_f(\mathbb{Q}_\ell, T_{k,n})$, i.e.,

$$c \in \ker\{H^1(\mathbb{Q}_\ell, T_{k,n}) \longrightarrow H^1_f(\mathbb{Q}_\ell, T_{k,n})\} = H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_{k,n})$$

provided $[\mathbf{X}^{N-n}]c \in \ker\{H^1(\mathbb{Q}_\ell, T_{k,N}) \to H^1_f(\mathbb{Q}_\ell, T_{k,N})\} = H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_{k,N})$. This shows that

$$H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_{k,n}) = \ker\{H^1(\mathbb{Q}_\ell, T_{k,n}) \overset{[\mathbf{X}^{N-n}]}{\longrightarrow} H^1(\mathbb{Q}_\ell, T_{k,N})/H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_{k,N})\},$$

which is the property **C2** for the transverse condition on $\mathcal{T}_{k,m}$.

One can similarly prove, for positive integers $l \leq L \leq k$, that

$$H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_{l,n}) = \ker\{H^1(\mathbb{Q}_\ell, T_{l,n}) \overset{[\varpi^{L-l}]}{\longrightarrow} H^1(\mathbb{Q}_\ell, T_{L,n})/H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_{L,n})\}$$

for all $n \leq m$, which is the property **C3** for the transverse condition on $\mathcal{T}_{k,m}$. $\qquad\square$

Using Propositions 2.11, 2.13 and 2.21 we obtain the following:

Corollary 2.22. *For every $n \in \mathcal{N}_{k,m}$, the Selmer structure $\mathcal{F}_{\mathrm{can}}(n)$ is cartesian on $\mathcal{T}_{k,m}$.*

Remark 2.23. Corollary 2.22 has the following consequences for the Selmer modules:
Suppose $k \geq L \geq l$ and $m \geq S \geq s$ are positive integers, and $n \in \mathcal{N}_{k,m}$. Then:

(i) The image of $H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{L,S})$ lies in $H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{l,s})$ under the natural map

$$H^1(\mathbb{Q}, T_{L,S}) \longrightarrow H^1(\mathbb{Q}, T_{l,s}).$$

(ii) $H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{L,s})$ is the pre-image of $H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{L,S})$ under the map

$$H^1(\mathbb{Q}, T_{L,s}) \overset{[\mathbf{X}^{S-s}]}{\longrightarrow} H^1(\mathbb{Q}, T_{L,S}) \quad \text{and}$$

$H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{l,S})$ is the pre-image of $H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{L,S})$ under the map

$$H^1(\mathbb{Q}, T_{l,S}) \overset{[\varpi^{L-l}]}{\longrightarrow} H^1(\mathbb{Q}, T_{L,S}).$$

2.7. **Core Vertices for** $(T_{k,m}, \mathcal{F}_{\mathbf{can}}, \mathcal{P}_{k,m})$**.** Throughout this section we assume **H**.**1**-**H**.**4** as well as $\mathbb{H}.\mathbf{T}$ and $\mathbb{H}.\mathbf{sEZ}$. Let $\overline{T} := T/\mathfrak{m}T \cong T_{k,m}/(\mathfrak{m}, \mathbf{X})T_{k,m} = T_{1,1}$ be the residual representation. Fix a pair $k, m \in \mathbb{Z}^+$ until the end of §2.7.

Definition 2.24. Suppose M is an $\mathcal{O}[[G_{\mathbb{Q}}]]$-module which is finite over $\mathcal{O}$. If $\mathcal{F}$ is a Selmer structure on M, we define the Selmer group $H^1_{\mathcal{F}}(\mathbb{Q}, M) \subset H^1(\mathbb{Q}, M)$ to be the kernel of the sum of restriction maps

$$H^1(\mathbb{Q}_{\Sigma(\mathcal{F})}/\mathbb{Q}, M) \longrightarrow \bigoplus_{\ell \in \Sigma(\mathcal{F})} H^1(\mathbb{Q}_\ell, M)/H^1_{\mathcal{F}}(\mathbb{Q}_\ell, M)$$

where $\mathbb{Q}_{\Sigma(\mathcal{F})}$ denotes the maximal extension of $\mathbb{Q}$ which is unramified outside $\Sigma(\mathcal{F})$.

See [MR04, §2.3] for a definition of the dual Selmer structure $\mathcal{F}^*$ on M^* and the dual Selmer group $H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)$.

Definition 2.25. We say that $n \in \mathcal{N}_{k,m}$ is a *core vertex* for the triple $(T_{k,m}, \mathcal{F}_{\mathbf{can}}, \mathcal{P}_{k,m})$ if

- $H^1_{\mathcal{F}_{\mathbf{can}}(n)^*}(\mathbb{Q}, T^*_{k,m}) = 0$,
- $H^1_{\mathcal{F}_{\mathbf{can}}(n)}(\mathbb{Q}, T_{k,m})$ is a free $R_{k,m}$-module.

Thanks to [MR04, Corollary 4.1.9], there exists core vertices $n \in \mathcal{N}_{k,m}$ for the Selmer triple $(\overline{T} = T_{1,1}, \mathcal{F}_{\mathbf{can}}, \mathcal{P}_{k,m})$.

Definition 2.26. The *core Selmer rank* of the Selmer structure $\mathcal{F}_{\mathbf{can}}$ on $T_{1,1}$ is the dimension of the $\mathbb{F}$-vector space $H^1_{\mathcal{F}_{\mathbf{can}}(n)}(\mathbb{Q}, \overline{T})$ for any core vertex $n \in \mathcal{N}_{k,m}$. By [MR04, Theorem 4.1.10] this definition makes sense. We denote the core Selmer rank for $\mathcal{F}_{\mathbf{can}}$ on T by $\chi(\overline{T}) = \chi(\overline{T}, \mathcal{F}_{\mathbf{can}})$.

We note that the results from [MR04] we quote above rely on the hypotheses **H1**-**H6** of [MR04, §3.5]. These hypotheses are satisfied for the triple $(\overline{T}, \mathcal{F}_{\mathbf{can}}, \mathcal{P}_{k,m})$ under our running assumptions and thanks to Propositions 2.11 and 2.13.

We assume until the end of this paper that $\chi(\overline{T}) = 1$ (except in §4.3, where we construct another Selmer structure with core Selmer rank one). Making use of [MR04, Corollary 4.1.9], we construct below *core vertices* for the Selmer triple $(T_{k,m}, \mathcal{F}_{\mathbf{can}}, \mathcal{P}_{k,m})$:

Theorem 2.27. *Suppose* $\chi(\overline{T}) = 1$ *and* n *is a core vertex for the triple* $(\overline{T}, \mathcal{F}_{\mathbf{can}}, \mathcal{P}_{k,m})$. *Then:*

(i) *The* $R_{k,m}$-*module* $H^1_{\mathcal{F}_{\mathbf{can}}(n)}(\mathbb{Q}, T_{k,m})$ *is free of rank one.*

(ii) $H^1_{\mathcal{F}_{\mathbf{can}}(n)^*}(\mathbb{Q}, T^*_{k,m}) = 0$.

We say that n *is a core vertex for the triple* $(T_{k,m}, \mathcal{F}_{\mathbf{can}}, \mathcal{P}_{k,m})$.

Theorem 2.27 is an extension of [MR04, Theorem 4.1.10] to cover $G_{\mathbb{Q}}$-representations over the coefficient rings $R_{k,m}$. We note that Mazur and Rubin prove their assertion [MR04, Theorem 4.1.10] only for one-dimensional artinian coefficient rings.

Before proving Theorem 2.27, we need several preliminary results. Recall that hypotheses **H**.**1**-**H**.**4** along with $\mathbb{H}.\mathbf{T}$ and $\mathbb{H}.\mathbf{sEZ}$ are in effect throughout this section, as well as the assumption that $\chi(\overline{T}) = 1$.

Lemma 2.28. *Suppose* $n \in \mathcal{N}_{k,m}$. *Then the injection*

$$[\varpi^{k-1}] : T_{1,m} = T \otimes R_{1,m} \longrightarrow T \otimes R_{k,m} = T_{k,m}$$

induces isomorphisms

(i) $[\varpi^{k-1}] : H^1(\mathbb{Q}, T_{1,m}) \xrightarrow{\sim} H^1(\mathbb{Q}, T_{k,m})[\mathfrak{m}]$,

(ii) $[\varpi^{k-1}] : H^1_{\mathcal{F}_{\mathbf{can}}(n)}(\mathbb{Q}, T_{1,m}) \xrightarrow{\sim} H^1_{\mathcal{F}_{\mathbf{can}}(n)}(\mathbb{Q}, T_{k,m})[\mathfrak{m}]$.

Proof. Set $\mathbb{T} := T \otimes \Lambda$ and let $\mathcal{M} := (\mathfrak{m}, \mathbf{X})$ be the maximal ideal of Λ. Then, $\mathbb{T}/\mathcal{M}\mathbb{T} = T/\mathfrak{m}T$, and since we assumed **H**.**3**, it follows that $(\mathbb{T}/\mathcal{M}\mathbb{T})^{G_\mathbb{Q}} = 0$. By [MR04, Lemma 2.1.4], we have $S^{G_\mathbb{Q}} = 0$ for every subquotient S of $\mathbb{T}$ as well. In particular, $T_{k,m}^{G_\mathbb{Q}} = 0$ for every $k, m \in \mathbb{Z}^+$.

Now the $G_\mathbb{Q}$-cohomology of the exact sequences

$$0 \longrightarrow T_{1,m} \xrightarrow{\varpi^{k-1}} T_{k,m} \longrightarrow T_{k-1,m} \longrightarrow 0$$

$$0 \longrightarrow T_{k-1,m} \xrightarrow{\varpi} T_{k,m}$$

gives (together with the vanishing of $S^{G_\mathbb{Q}}$ for the relevant quotients S of $\mathbb{T}$)

(10)
$$0 \longrightarrow H^1(\mathbb{Q}, T_{1,m}) \xrightarrow{[\varpi^{k-1}]} H^1(\mathbb{Q}, T_{k,m}) \xrightarrow{\mathfrak{R}} H^1(\mathbb{Q}, T_{k-1,m})$$

$$0 \longrightarrow H^1(\mathbb{Q}, T_{k-1,m}) \xrightarrow{[\varpi]} H^1(\mathbb{Q}, T_{k,m})$$

This shows

$$\begin{aligned} H^1(\mathbb{Q}, T_{1,m}) &= \ker(\mathfrak{R}) \\ &= \ker([\varpi] \circ \mathfrak{R}) \\ &= H^1(\mathbb{Q}, T_{k,m})[\mathfrak{m}]. \end{aligned}$$

The second equality is because $[\varpi]$ is injective on $H^1(\mathbb{Q}, T_{k-1,m})$ thanks to the second exact sequence in (10), and the last equality is because $[\varpi] \circ \mathfrak{R}$ on $H^1(\mathbb{Q}, T_{k,m})$ is multiplication by ϖ).

This proves (i). To finish the proof of Lemma, we need to show that $H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{1,m})$ maps isomorphically onto $H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{k,m})[\mathfrak{m}]$ under the isomorphism of (i). This follows at once from Remark 2.23. □

Remark 2.29. Starting from the exact sequences

$$0 \longrightarrow T_{k,1} \xrightarrow{\mathbf{X}^{m-1}} T_{k,m} \longrightarrow T_{k,m-1} \longrightarrow 0$$

$$0 \longrightarrow T_{k,m-1} \xrightarrow{\mathbf{X}} T_{k,m}$$

one may similarly prove that

$$[\mathbf{X}^{m-1}] : H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{k,1}) \xrightarrow{\sim} H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{k,m})[\mathbf{X}]$$

for every $k, m \in \mathbb{Z}^+$.

Write $\mathcal{M}_{k,m} = (\mathfrak{m}, \mathbf{X})$ for the maximal ideal of $R_{k,m}$. Since

$$H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{k,m})[\mathcal{M}] = \{H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{k,m})[\mathfrak{m}]\}[\mathbf{X}],$$

it follows from Lemma 2.28 and Remark 2.29 that

(11)
$$H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{k,m})[\mathcal{M}] \cong H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, \overline{T}).$$

Proposition 2.30. *Suppose $n \in \mathcal{N}_{k,m}$ is a core vertex for $(\overline{T}, \mathcal{F}_{\text{can}}, \mathcal{P}_{k,m})$ and $\chi(\overline{T}, \mathcal{F}_{\text{can}}) = 1$. Then the $R_{k,m}$-module $\text{Hom}\left(H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{k,m}), \Phi/\mathcal{O}\right)$ is cyclic.*

Proof. By the assumption on n, it follows that the $\mathbb{F}$-vector space $H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{1,1}) = H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, \overline{T})$ is one-dimensional. Furthermore, by Remark 2.29 applied with $k = 1$ and using the fact that $R_{1,m}$ is a principal ideal ring, it follows that $H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{1,m})$ is a cyclic $R_{1,m}$-module:

$$H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{1,m}) \cong \mathbb{F}[[\mathbf{X}]]/\mathbf{X}^\alpha, \text{ for some } \alpha \leq m \text{ (as an } R_{1,m}\text{-module)}.$$

By Lemma 2.28(ii), we have

(12) $$H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{k,m})[\mathfrak{m}] \cong H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{1,m}).$$

Taking the Pontryagin duals of both sides in (12), we obtain

$$\begin{aligned}
\mathrm{Hom}\left(H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{k,m}), \Phi/\mathcal{O}\right) \otimes \mathcal{O}/\mathfrak{m} \ &\cong \mathrm{Hom}\left(H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{1,m}), \mathbb{F}\right) \\
&\cong \mathrm{Hom}\left(\mathbb{F}[[\mathbf{X}]]/\mathbf{X}^\alpha, \mathbb{F}\right) \\
&\cong \mathbb{F}[[\mathbf{X}]]/\mathbf{X}^\alpha
\end{aligned}$$

which shows that $\mathrm{Hom}\left(H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{k,m}), \Phi/\mathcal{O}\right)/\mathfrak{m}\cdot\mathrm{Hom}\left(H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{k,m}), \Phi/\mathcal{O}\right)$ is generated by one element as an $R_{1,m}$-module. By Nakayama's lemma, it now follows that the $R_{k,m}$-module $\mathrm{Hom}\left(H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{k,m}), \Phi/\mathcal{O}\right)$ is generated by one element. $\qquad\square$

Proposition 2.31. *Under the hypotheses and the notation of Proposition 2.30,*

$$\mathrm{length}_{\mathcal{O}}\, H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{k,m}) - \mathrm{length}_{\mathcal{O}}\, H^1_{\mathcal{F}_{\mathrm{can}}(n)^*}(\mathbb{Q}, T^*_{k,m}) = k \cdot m.$$

Proof. (All the *length*s in this proof are measured over $\mathcal{O}$.)

Fix m, and let R_k denote the ring $\mathcal{O}/\mathfrak{m}^k$. Using [MR04, Corollary 2.3.6], it suffices to prove Lemma only for $n = 1$, i.e., for $\mathcal{F}_{\mathrm{can}}(n) = \mathcal{F}_{\mathrm{can}}$. By [MR04, Theorem 4.1.5], there are integers r_k, s_k, one of which can be taken to be zero, such that, there is an isomorphism

$$H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) \oplus R_k^{r_k} \cong H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}, T^*_{k,m}) \oplus R_k^{s_k}.$$

Here we regard $T_{k,m}$ as an R_k-representation. We note that proof of [MR04, Theorem 4.1.5] still holds true in our case by Proposition 2.11 and Lemma 2.28. The proof of the same theorem in fact shows that r_k, s_k do not depend on k, we denote this common value by $\chi(T^*_m)$, $\chi(T_m)$, respectively. Hence, there is an isomorphism

(13) $$H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) \oplus R_k^{\chi(T^*_m)} \cong H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}, T^*_{k,m}) \oplus R_k^{\chi(T_m)}.$$

Passing to inverse limit in (13) (by making use of Remark 2.23), we see that

$$\chi(T_m) - \chi(T^*_m) = \mathrm{rank}_{\mathcal{O}}\, H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}, T_m) - \mathrm{corank}_{\mathcal{O}}\, H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}, T^*_m).$$

On the other hand, by [MR04, Lemma 5.2.15], it follows that

(14)
$$\begin{aligned}
\mathrm{rank}_{\mathcal{O}}\, H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}, T_m) - \mathrm{corank}_{\mathcal{O}}\, H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}, T^*_m) \ &= \ \mathrm{rank}_{\mathcal{O}}\, T^-_m + \mathrm{corank}_{\mathcal{O}}\, H^0(\mathbb{Q}_p, T^*_m) \\
&= \ m \cdot \mathrm{rank}_{\mathcal{O}}\, T^- + \mathrm{corank}_{\mathcal{O}}\, H^0(\mathbb{Q}_p, T^*_m),
\end{aligned}$$

where for a $G_{\mathbb{Q}}$-module M, we write M^- for the (-1)-eigenspace for an arbitrary complex conjugation $\mathfrak{c} \in G_{\mathbb{Q}}$. The second equality in (14) is because the complex conjugation acts trivially on $\Lambda/\mathbf{X}^m$. Hence,

$$\begin{aligned}
\mathrm{length}_{\mathcal{O}}\, H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) - \mathrm{length}_{\mathcal{O}}\, H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}, T^*_{k,m}) &= k\left(\chi(T_m) - \chi(T^*_m)\right) \\
&= k \cdot m \cdot \mathrm{rank}_{\mathbb{Z}_p}\, T^- + k \cdot \mathrm{corank}_{\mathbb{Z}_p}\, H^0(\mathbb{Q}_p, T^*_m)
\end{aligned}$$

By local Tate duality, $H^0(\mathbb{Q}_p, T^*_m)$ is dual to $H^2(\mathbb{Q}_p, T_m)$, and

$$H^2(\mathbb{Q}_p, T_m) = H^2(\mathbb{Q}_p, T \otimes \Lambda/\mathbf{X}^m) \cong H^2(\mathbb{Q}_p, T \otimes \Lambda)/\mathbf{X}^m H^2(\mathbb{Q}_p, T \otimes \Lambda)$$

because $G_{\mathbb{Q}_p}$ has cohomological dimension 2. However, $H^2(\mathbb{Q}_p, T \otimes \Lambda) = 0$ by Lemma 2.12, which in turn shows that $\mathrm{corank}_{\mathcal{O}}\, H^0(\mathbb{Q}_p, T^*_m) = 0$ for all m. We therefore conclude that

(15) $$\mathrm{length}_{\mathcal{O}}\, H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) - \mathrm{length}_{\mathcal{O}}\, H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}, T^*_{k,m}) = k \cdot m \cdot \mathrm{rank}_{\mathcal{O}}\, T^-.$$

The equation (15) for $m = 1$, together with our assumption that $\chi(\overline{T}) = 1$ imply that $\mathrm{rank}_{\mathcal{O}} T^- = 1$. Proof of Lemma follows. $\qquad\square$

Remark 2.32. For any height one prime $\wp$ of Λ which is not exceptional in the sense of [MR04, Definition 5.3.12], one may prove that the core Selmer rank $\mathcal{X}(T \otimes S_\wp, \mathcal{F}_{\mathrm{can}})$ for the canonical Selmer structure on $T \otimes S_\wp$ does not depend on $\wp$ (see [MR04, Lemma 5.3.16]). Here, $S_\wp$ is the integral closure of $\Lambda/\wp$ inside its field of fractions $\mathrm{Frac}(\Lambda/\wp)$. This common value is called the *generic core Selmer rank* of the canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ on $T \otimes \Lambda$. In particular, our assumption that the core Selmer rank $\mathcal{X}(\overline{T}, \mathcal{F}_{\mathrm{can}}) = 1$, together with the hypothesis $\mathbb{H}.\mathbf{EZ}$ is equivalent to the assumption that the generic core Selmer rank equals *one*.

Proof of Theorem 2.27. Immediate from Propositions 2.30 and 2.31. $\qquad\square$

3. Λ-ADIC KOLYVAGIN SYSTEMS

Many of the arguments in this section are essentially present in [MR04, §4.3 and Appendix B]. We still include every detail for completeness.

3.1. **Kolyvagin Systems over $R_{k,m}$.**

3.1.1. *Generalities.* Let R be a local artinian ring with finite residue field. If M is an R-module and $\psi \in \mathrm{Hom}(M, R)$, we define for any integer r a map $\overset{r}{\bigwedge} M \to \overset{r-1}{\bigwedge} M$, also denoted by ψ, by setting

$$\psi : m_1 \wedge \cdots \wedge m_r \mapsto \sum_{i=1}^{r} (-1)^{i+1} \psi(m_i) m_1 \wedge \ldots m_{i-1} \wedge m_{i+1} \wedge \cdots \wedge m_r.$$

We also define a map $\overset{s}{\bigwedge} \mathrm{Hom}(M, R) \to \mathrm{Hom}(\overset{r}{\bigwedge} M, \overset{r-s}{\bigwedge} M)$ for $s \leq r$, by iterating the construction above: $\psi_1 \wedge \cdots \wedge \psi_s := \psi_s \circ \cdots \circ \psi_1$.

Lemma 3.1 below is one of the main technical tools we utilize in this section. It generalizes [MR04, Lemma B.1] to apply with coefficient rings which are artinian (and not necessarily principal artinian, as assumed in loc.cit.). However, Lemma 3.1 claims less than [MR04, Lemma B.1], e.g., Lemma 3.1 does not determine the exact image of the map Ψ below unless the map ψ defined below is surjective.

Lemma 3.1. *Suppose M is a free R-module of rank at least $r + 1$ and $\psi_1, \ldots, \psi_r \in \mathrm{Hom}(M, R)$. Define:*

$$\begin{aligned} \psi &= \psi_1 \oplus \cdots \oplus \psi_r : M \longrightarrow R^r \\ \Psi &= \psi_1 \wedge \cdots \wedge \psi_r : \overset{r+1}{\bigwedge} M \longrightarrow M \end{aligned}$$

Then

$$\begin{aligned} \Psi\left(\overset{r+1}{\bigwedge} M\right) &\subset \ker(\psi), \text{ and,} \\ &= \ker(\psi) \text{ if } \psi \text{ is surjective.} \end{aligned}$$

Proof. Suppose first that ψ is surjective with kernel $A \subset M$. Then the image of ψ is R^r, which is a projective R-module, hence the exact sequence

$$0 \longrightarrow A \longrightarrow M \overset{\psi}{\longrightarrow} R^r \longrightarrow 0$$

splits. Therefore, there is a submodule B of M which complements A, i.e., $M = A \oplus B$ and ψ maps B isomorphically onto R^r. We have a functorial isomorphism

$$\tag{16} \bigwedge^{r+1} M \cong \bigoplus_{p+q=r+1} \left(\bigwedge^p A \otimes \bigwedge^q B \right).$$

The map Ψ, after the identification (16), takes the factor $A \otimes \bigwedge^r B$ isomorphically onto A and kills the other summands. This proves the equality when ψ is surjective.

To prove the containment in general, we need to check that the map

$$\psi_s \circ \Psi : \bigwedge^{r+1} M \longrightarrow R$$

is identically *zero* for all $s = 1, \ldots, r$. We will only check this when $s = 1$, and the other cases follow in an identical fashion.

A simple combinatorial argument shows that

$$\Psi(m_1 \wedge \cdots \wedge m_{r+1}) = (\psi_1 \wedge \cdots \wedge \psi_r)(m_1 \wedge \cdots \wedge m_{r+1}) =$$

$$\sum_{i=1}^{r+1} \sum_{\sigma} (-1)^i \mathrm{sign}(\sigma) \cdot \psi_1(m_{\sigma(1)}) \ldots \psi_{i-1}(m_{\sigma(i-1)}) \cdot \psi_i(m_{\sigma(i+1)}) \ldots \psi_r(m_{\sigma(r+1)}) \cdot m_i$$

where the second sum is over all permutations σ of $\{1, \ldots, i-1, i, i+1, \ldots, r+1\}$ such that $\sigma(i) = i$. Then

$$\psi_1 \circ \Psi(m_1 \wedge \cdots \wedge m_{r+1}) =$$

$$\sum_{i=1}^{r+1} \sum_{\sigma} (-1)^i \mathrm{sign}(\sigma) \cdot \psi_1(m_{\sigma(1)}) \ldots \psi_{i-1}(m_{\sigma(i-1)}) \cdot \psi_i(m_{\sigma(i+1)}) \ldots \psi_r(m_{\sigma(r+1)}) \cdot \psi_1(m_i).$$

We fix i. Then the expression $\psi_1(m_{\sigma(1)}) \cdots \psi_{i-1}(m_{\sigma(i-1)}) \cdot \psi_i(m_{\sigma(i+1)}) \cdots \psi_r(m_{\sigma(r+1)}) \cdot \psi_1(m_i)$ appears exactly twice in the final displayed equality above. We now identify these terms and show that they will have opposite signs. This will conclude that $\psi_1 \circ \Psi(m_1 \wedge \cdots \wedge m_{r+1}) = 0$.

Let $\sigma(1) = j$, and let

$$\alpha = \begin{cases} (1, i, i+1, \ldots, j) & , \text{ if } j > i \\ (1, i, i-1, \ldots, j) & , \text{ if } j < i \end{cases}$$

be a cycle in the symmetric group $\mathfrak{S}_{r+1}$. Set $\tau = \sigma \circ \alpha$. Then the term

$$\psi_1(m_{\sigma(1)}) \ldots \psi_{i-1}(m_{\sigma(i-1)}) \cdot \psi_i(m_{\sigma(i+1)}) \ldots \psi_r(m_{\sigma(r+1)}) \cdot \psi_1(m_i)$$

appears once for the permutation σ itself (with the sign $(-1)^i \mathrm{sign}(\sigma)$) and for the permutation τ (with the sign $(-1)^j \mathrm{sign}(\tau)$). Since $\mathrm{sign}(\tau) = \mathrm{sign}(\sigma)\mathrm{sign}(\alpha) = \mathrm{sign}(\sigma)(-1)^{i-j+1}$, it follows that $(-1)^j \mathrm{sign}(\tau) = (-1)^{i+1}\mathrm{sign}(\sigma)$. This shows that

$$\psi_1 \circ \Psi(m_1 \wedge \cdots \wedge m_{r+1}) = 0.$$

$\square$

3.1.2. *The lower bound.* We keep the notation above. Let $\nu(n)$ be the number of prime divisors of n. In this section, we obtain (Theorem 3.11) a lower bound on the size of the $R_{k,m}$-module of Kolyvagin Systems.

Definition 3.2. If X is a graph and $\mathrm{Mod}_{R_{k,m}}$ is the category of $R_{k,m}$-modules, a *simplicial sheaf* $\mathcal{S}$ on X with values in $\mathrm{Mod}_{R_{k,m}}$ is a rule assigning

- an $R_{k,m}$-module $\mathcal{S}(v)$ for every vertex v of X,
- an $R_{k,m}$-module $\mathcal{S}(e)$ for every edge e of X,

- an $R_{k,m}$-module homomorphism $\psi_v^e : \mathcal{S}(v) \to \mathcal{S}(e)$ whenever the vertex v is an endpoint of the edge e.

A *global section* of $\mathcal{S}$ is a collection $\{\kappa_v \in \mathcal{S}(v) : v \text{ is a vertex of } X\}$ such that, for every edge $e = \{v, v'\}$ of X, we have $\psi_v^e(\kappa_v) = \psi_{v'}^e(\kappa_{v'})$ in $\mathcal{S}(e)$. We write $\Gamma(\mathcal{S})$ for the $R_{k,m}$-module of global sections of $\mathcal{S}$.

Definition 3.3. For the Selmer triple $(T_{k,m}, \mathcal{F}_{\text{can}}, \mathcal{P}_{k,m})$, we define a graph $\mathcal{X}_{k,m} = \mathcal{X}(\mathcal{P}_{k,m})$ by taking the set of vertices of $\mathcal{X}_{k,m}$ to be $\mathcal{N}_{k,m}$, and the edges to be $\{n, n\ell\}$ whenever $n, n\ell \in \mathcal{N}_{k,m}$ (with ℓ prime).

The *Selmer sheaf* $\mathcal{H}$ is the simplicial sheaf on $\mathcal{X}_{k,m}$ given as follows. Set $G_n := \otimes_{\ell|n} \mathbb{F}_\ell^\times$. We take

- $\mathcal{H}(n) := H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{k,m}) \otimes G_n$ for $n \in \mathcal{N}_{k,m}$,
- if e is the edge $\{n, n\ell\}$ then $\mathcal{H}(e) := H^1_s(\mathbb{Q}_\ell, T_{k,m}) \otimes G_{n\ell}$.

We define the vertex-to-edge maps to be

- $\psi_{n\ell}^e : H^1_{\mathcal{F}_{\text{can}}(n\ell)}(\mathbb{Q}, T_{k,m}) \otimes G_{n\ell} \to H^1_s(\mathbb{Q}_\ell, T_{k,m}) \otimes G_{n\ell}$ is localization followed by the projection to the singular cohomology $H^1_s(\mathbb{Q}_\ell, T_{k,m})$.
- $\psi_n^e : H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{k,m}) \otimes G_n \to H^1_s(\mathbb{Q}_\ell, T_{k,m}) \otimes G_{n\ell}$ is the composition of localization at ℓ with the finite-singular comparison map ϕ_ℓ^{fs}.

A *Kolyvagin system* for the triple $(T_{k,m}, \mathcal{F}_{\text{can}}, \mathcal{P}_{k,m})$ is simply a global section of the Selmer sheaf $\mathcal{H}$.

Recall the definition of the modified Selmer structure $\mathcal{F}_{\text{can}}^n$ on $T_{k,m}$ (Definition 2.4).

Proposition 3.4. *If $n \in \mathcal{N}_{k,m}$ is a core vertex for $(T_{k,m}, \mathcal{F}_{\text{can}}, \mathcal{P}_{k,m})$, then the $R_{k,m}$-module $H^1_{\mathcal{F}_{\text{can}}^n}(\mathbb{Q}, T_{k,m})$ is free of rank $\nu(n) + 1$.*

Proof. We have the following exact sequences:

$$0 \longrightarrow H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{k,m}) \longrightarrow H^1_{\mathcal{F}_{\text{can}}^n}(\mathbb{Q}, T_{k,m}) \longrightarrow \bigoplus_{\ell|n} \frac{H^1(\mathbb{Q}_\ell, T_{k,m})}{H^1_{\text{tr}}(\mathbb{Q}_\ell, T_{k,m})}$$

$$0 \longrightarrow H^1_{(\mathcal{F}_{\text{can}}^n)^*}(\mathbb{Q}, T_{k,m}^*) \longrightarrow H^1_{\mathcal{F}_{\text{can}}(n)^*}(\mathbb{Q}, T_{k,m}^*) \longrightarrow \bigoplus_{\ell|n} H^1_{\text{tr}}(\mathbb{Q}_\ell, T_{k,m}^*)$$

We have $H^1_{\mathcal{F}_{\text{can}}(n)^*}(\mathbb{Q}, T_{k,m}^*) = 0$ since $n \in \mathcal{N}_{k,m}$ is a core vertex, hence the Poitou-Tate global duality theorem (see [Rub00, Theorem 1.3.5] and [MR04, Theorem 2.3.4]) implies that the right-most map in the first sequence is surjective. Thus the sequence

$$0 \longrightarrow H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{k,m}) \longrightarrow H^1_{\mathcal{F}_{\text{can}}^n}(\mathbb{Q}, T_{k,m}) \longrightarrow \bigoplus_{\ell|n} \frac{H^1(\mathbb{Q}_\ell, T_{k,m})}{H^1_{\text{tr}}(\mathbb{Q}_\ell, T_{k,m})} \longrightarrow 0$$

is exact. By Theorem 2.27, the $R_{k,m}$-module $H^1_{\mathcal{F}_{\text{can}}(n)}(\mathbb{Q}, T_{k,m})$ is free of rank one, and the sum $\bigoplus_{\ell|n} \frac{H^1(\mathbb{Q}_\ell, T_{k,m})}{H^1_{\text{tr}}(\mathbb{Q}_\ell, T_{k,m})}$ is free (hence projective) of rank $\nu(n)$ by Lemma 2.19 and Lemma 2.20. This completes the proof. $\square$

Fixing a generator of $\text{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$, we may view (by Lemma 2.19 and Lemma 2.20) the finite-singular comparison map as an isomorphism

$$H^1_f(\mathbb{Q}_\ell, T_{k,m}) \xrightarrow{\phi_\ell^{\text{fs}}} H^1_s(\mathbb{Q}_\ell, T_{k,m}) \cong H^1_{\text{tr}}(\mathbb{Q}_\ell, T_{k,m}).$$

For each $\ell \in \mathcal{P}_{k,m}$, we fix an isomorphism $\iota_\ell : H^1_{\mathrm{tr}}(\mathbb{Q}_\ell, T_{k,m}) \to R_{k,m}$. Fix a core vertex $n \in \mathcal{N}_{k,m}$ and order the primes $\ell_1, \ldots, \ell_{\nu(n)}$ dividing n arbitrarily. Let $\mathrm{loc}^{\mathrm{f}}_i$ (resp., $\mathrm{loc}^{\mathrm{tr}}_i$) be the map $H^1(\mathbb{Q}, T_{k,m}) \to R_{k,m}$ defined as the localization at ℓ_i, followed by the projection onto the finite (resp., the transverse) submodule, an then followed by $\iota_{\ell_i} \circ \phi^{\mathrm{fs}}_{\ell_i}$ (resp., ι_{ℓ_i}) :

$$
\begin{array}{ccccc}
H^1(\mathbb{Q}, T_{k,m}) & \longrightarrow & H^1(\mathbb{Q}_{\ell_i}, T_{k,m}) & \xrightarrow{\mathrm{proj}} & H^1_f(\mathbb{Q}_{\ell_i}, T_{k,m}) \\
 & & & & \phi^{\mathrm{fs}}_{\ell_i} \downarrow \cong \\
 & & & & H^1_{\mathrm{s}}(\mathbb{Q}_{\ell_i}, T_{k,m}) \\
 & & & & \downarrow \cong \\
 & \mathrm{loc}^{\mathrm{f}}_i & & & H^1_{\mathrm{tr}}(\mathbb{Q}_{\ell_i}, T_{k,m}) \\
 & & & & \iota_{\ell_i} \downarrow \cong \\
 & & & & R_{k,m}
\end{array}
$$

and

$$
\begin{array}{ccccc}
H^1(\mathbb{Q}, T_{k,m}) & \longrightarrow & H^1(\mathbb{Q}_{\ell_i}, T_{k,m}) & \xrightarrow{\mathrm{proj}} & H^1_{\mathrm{s}}(\mathbb{Q}_{\ell_i}, T_{k,m}) \\
 & & & & \downarrow \cong \\
 & & & & H^1_{\mathrm{tr}}(\mathbb{Q}_{\ell_i}, T_{k,m}) \\
 & \mathrm{loc}^{\mathrm{tr}}_i & & & \iota_{\ell_i} \downarrow \cong \\
 & & & & R_{k,m}
\end{array}
$$

Definition 3.5. For each $r \mid n$, define

$$
\psi^{(r)}_i = \begin{cases} \mathrm{loc}^{\mathrm{f}}_i, & \text{if } \ell_i \text{ divides } r, \\ \mathrm{loc}^{\mathrm{tr}}_i, & \text{if } \ell_i \text{ does not divide } r \end{cases}
$$

and let

$$
\begin{aligned}
\psi^{(r)} &= \psi^{(r)}_1 \oplus \cdots \oplus \psi^{(r)}_{\nu(n)} &:& \quad H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) \to R^{\nu(n)}_{k,m}, \\
\Psi^{(r)} &= \psi^{(r)}_1 \wedge \cdots \wedge \psi^{(r)}_{\nu(n)} &:& \quad \overset{\nu(n)+1}{\bigwedge} H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) \to H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}).
\end{aligned}
$$

Proposition 3.6. *Suppose $n \in \mathcal{N}_{k,m}$ is a core vertex, then for all $r \mid n$,*

$$
\begin{aligned}
\Psi^{(r)} \left(\overset{\nu(n)+1}{\bigwedge} H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) \right) &\subset H^1_{\mathcal{F}_{\mathrm{can}(r)}}(\mathbb{Q}, T_{k,m}) \\
&= H^1_{\mathcal{F}_{\mathrm{can}(r)}}(\mathbb{Q}, T_{k,m}), \text{ if } r \text{ is a core vertex.}
\end{aligned}
$$

Proof. For $r \mid n$, the following sequence is exact:

$$
(17) \qquad 0 \longrightarrow H^1_{\mathcal{F}_{\mathrm{can}(r)}}(\mathbb{Q}, T_{k,m}) \longrightarrow H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) \xrightarrow{\psi^{(r)}} R^{\nu(n)}_{k,m} \longrightarrow \mathrm{coker}(\psi^{(r)}) \longrightarrow 0.
$$

If r is a core vertex, then $H^1_{\mathcal{F}_{\mathrm{can}(r)}}(\mathbb{Q}, T_{k,m})$ is free of rank one by definition, and $H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m})$ is free of rank $\nu(n) + 1$ by Proposition 3.4. Counting lengths in the exact sequence (17), one checks

that $\mathrm{coker}(\psi^{(r)}) = 0$, i.e., $\psi^{(r)}$ is surjective. Now Lemma 3.1 concludes that

$$\Psi^{(r)}\left(\bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m})\right) = H^1_{\mathcal{F}_{\mathrm{can}(r)}}(\mathbb{Q}, T_{k,m})$$

when r is a core vertex. The general containment also follows similarly from Lemma 3.1. $\square$

Definition 3.7. Choose $c \in \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m})$ and for each divisor r of n, define

$$\kappa_r := \kappa_r(n, c) = (-1)^{\nu(r)}\Psi^{(r)}(c) \in H^1_{\mathcal{F}_{\mathrm{can}(r)}}(\mathbb{Q}, T_{k,m}).$$

Proposition 3.8. *For every $r\ell_i \mid n$, we have $\mathrm{loc}^{\mathrm{f}}_{\ell_i}(\kappa_r) = \mathrm{loc}^{\mathrm{tr}}_{\ell_i}(\kappa_{r\ell_i})$.*

Proof.

$$\begin{aligned}
\mathrm{loc}^{\mathrm{f}}_{\ell_i}(\kappa_r) &= (-1)^{\nu(r)}\mathrm{loc}^{\mathrm{f}}_{\ell_i}(\Psi^{(r)}(c)) \\
&= (-1)^{\nu(r)}(\Psi^{(r)} \wedge \mathrm{loc}^{\mathrm{f}}_{\ell_i})(c) \\
&= -(-1)^{\nu(r)}(\Psi^{(r\ell_i)} \wedge \mathrm{loc}^{\mathrm{tr}}_{\ell_i})(c) \\
&= (-1)^{\nu(r\ell_i)}\mathrm{loc}^{\mathrm{tr}}_{\ell_i}(\Psi^{(r\ell_i)}(c)) \\
&= \mathrm{loc}^{\mathrm{tr}}_{\ell_i}(\kappa_{r\ell_i}).
\end{aligned}$$

where the we obtain third equality by transposing $\mathrm{loc}^{\mathrm{f}}_{\ell_i}$ and $\mathrm{loc}^{\mathrm{tr}}_{\ell_i}$ which occur in $\Psi^{(r)} \wedge \mathrm{loc}^{\mathrm{f}}_{\ell_i}$. $\square$

Thus the collection $\{\kappa_r(n, c)\}$ for $r \mid n$ gives a section of the Selmer sheaf $\mathcal{H}$ to the subgraph $\mathcal{X}_n$ of $\mathcal{X}(\mathcal{P}_{k,m})$, whose vertices are all the positive divisors r of n. We will show that if $n' = nd$ is another core vertex, then this section can be extended to a section of $\mathcal{H}$ over the graph $\mathcal{X}_{nd}$.

Remark 3.9. Note that the section $\kappa(n, c) = \{\kappa_r(n, c) : r \mid n\}$ depends on the choice of ordering of primes dividing n, but only up to a sign. We will adopt the convention in [MR04, Appendix B]; namely we will maintain the same ordering of primes dividing n when we extend to $n' = nd$, but place them after the *new* primes which divide d.

Lemma 3.10. *In the following diagram, the image of the horizontal arrow contains the image of the vertical arrow:*

$$\bigwedge^{\nu(n')+1} H^1_{\mathcal{F}^{nd}_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) \xrightarrow{\mathrm{loc}^{\mathrm{tr}}_1 \wedge \cdots \wedge \mathrm{loc}^{\mathrm{tr}}_{\nu(d)}} \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^{nd}_{\mathrm{can}}}(\mathbb{Q}, T_{k,m})$$

$$\Big\uparrow$$

$$\bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m})$$

If the image of $c' \in \bigwedge^{\nu(n')+1} H^1_{\mathcal{F}^{nd}_{\mathrm{can}}}(\mathbb{Q}, T_{k,m})$ under the horizontal map agrees with the image of c under the vertical map, then the section $\kappa(n', c')$ of $\mathcal{X}_{nd}$ extends the section $\kappa(n, c)$ of $\mathcal{X}_n$.

Proof. As in the proof of Theorem 3.4, global duality and the vanishing of $H^1_{(\mathcal{F}^n_{\mathrm{can}})^*}(\mathbb{Q}, T^*_{k,m})$ imply that we have an exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) \longrightarrow H^1_{\mathcal{F}^{nd}_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) \xrightarrow{\mathrm{loc}_d} \bigoplus_{\ell \mid d} \frac{H^1(\mathbb{Q}_\ell, T_{k,m})}{H^1_{\mathrm{loc}}(\mathbb{Q}_\ell, T_{k,m})} \longrightarrow 0.$$

The right-most term is projective, hence we may choose a free rank-$\nu(d)$ summand A, complementary to $H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) \subset H^1_{\mathcal{F}^{nd}_{\mathrm{can}}}(\mathbb{Q}, T_{k,m})$. Thus the map $\bigoplus \mathrm{loc}^{\mathrm{tr}}_i : A \to R^{\nu(d)}_{k,m}$ is an isomorphism. This shows that the map $\bigwedge \mathrm{loc}^{\mathrm{tr}}_i : \bigwedge^{\nu(d)} A \longrightarrow \bigwedge^{\nu(d)} R^{\nu(d)}_{k,m} = R_{k,m}$ and the map

$$\bigwedge^{\nu(d)} A \otimes \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) \xrightarrow{\mathrm{loc}^{\mathrm{tr}}_1 \wedge \cdots \wedge \mathrm{loc}^{\mathrm{tr}}_{\nu(d)} \otimes \mathrm{id}} \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m})$$

are isomorphisms as well. Thus, in the commutative diagram

$$
\begin{array}{ccc}
\bigwedge^{\nu(n')+1} H^1_{\mathcal{F}^{nd}_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) & \xrightarrow{\mathrm{loc}^{\mathrm{tr}}_1 \wedge \cdots \wedge \mathrm{loc}^{\mathrm{tr}}_{\nu(d)}} & \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^{nd}_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) \\
\uparrow & & \uparrow \\
\bigwedge^{\nu(d)} A \otimes \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m}) & \xrightarrow{\mathrm{loc}^{\mathrm{tr}}_1 \wedge \cdots \wedge \mathrm{loc}^{\mathrm{tr}}_{\nu(d)} \otimes \mathrm{id}} & \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^n_{\mathrm{can}}}(\mathbb{Q}, T_{k,m})
\end{array}
$$

the lower horizontal map is surjective, and hence the first claim is proved. To prove the second claim, we observe for $r \mid n$ that

$$
\begin{aligned}
\kappa_r(n, c) &= (-1)^{\nu(r)} \left(\psi^{(r)}_{\nu(d)+1} \wedge \cdots \wedge \psi^{(r)}_{\nu(nd)} \right)(c) \\
&= (-1)^{\nu(r)} \left(\psi^{(r)}_{\nu(d)+1} \wedge \cdots \wedge \psi^{(r)}_{\nu(nd)} \right) \left(\mathrm{loc}^{\mathrm{tr}}_1 \wedge \cdots \wedge \mathrm{loc}^{\mathrm{tr}}_{\nu(d)} \right)(c') \\
&= (-1)^{\nu(r)} \left(\psi^{(r)}_{\nu(d)+1} \wedge \cdots \wedge \psi^{(r)}_{\nu(nd)} \right) \left(\psi^{(r)}_1 \wedge \cdots \wedge \psi^{(r)}_{\nu(d)} \right)(c') \\
&= (-1)^{\nu(r)} \left(\psi^{(r)}_1 \wedge \cdots \wedge \psi^{(r)}_{\nu(nd)} \right)(c') \\
&= \kappa_r(n', c').
\end{aligned}
$$

$\square$

Let $\Gamma(\mathcal{H})$ denote the *global sections* of the Selmer sheaf $\mathcal{H}$ on the graph $\mathcal{X}_{k,m}$.

Theorem 3.11. *For any core vertex $r \in \mathcal{N}_{k,m}$, the map $\Gamma(\mathcal{H}) \to \mathcal{H}(r)$ is surjective.*

Proof. Fixing a generator of $G_r := \bigotimes_{\ell \mid r} \mathbb{F}^\times_\ell$, we may identify $\mathcal{H}(r)$ with $H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m})$. Fix an arbitrary $\alpha \in H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m})$. Using Proposition 3.6, one may choose $c_0 \in \bigwedge^{\nu(r)+1} H^1_{\mathcal{F}^r_{\mathrm{can}}}(\mathbb{Q}, T_{k,m})$ such that $\kappa_r(r, c_0) = \alpha$.

By [MR04, Lemma 4.1.9(iii)] and Theorem 2.27, we may choose a sequence of core vertices $r = r_0 \mid r_1 \mid r_2 \ldots$, such that, every $n \in \mathcal{N}_{k,m}$ divides an r_i for some i. By Lemma 3.10, one may choose for each $i > 0$ and element $c_i \in \bigwedge^{\nu(r_i)+1} H^1_{\mathcal{F}^{r_i}_{\mathrm{can}}}(\mathbb{Q}, T_{k,m})$ in such a way that the section $\kappa(r_{i+1}, c_{i+1})$ of $\mathcal{X}_{n_{i+1}}$ restricts to $\kappa(r_i, c_i)$ on $\mathcal{X}_{n_i}$. We now define $\kappa \in \Gamma(\mathcal{H})$ to be

$$\kappa := \{\kappa_n\}_{n \in \mathcal{N}_{k,m}} = \{\kappa_n(r_i, c_i) \text{ for } i \text{ chosen sufficiently large}\}_{n \in \mathcal{N}_{k,m}}.$$

By construction, κ maps to α under the map $\Gamma(\mathcal{H}) \to \mathcal{H}(r)$. $\square$

3.1.3. *The upper bound.* In this section, we will obtain an upper bound on the size of the $R_{k,m}$-module $\mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k,m})$.

Theorem 3.12. *For any core vertex $r \in \mathcal{N}_{k,m}$ the map $\Gamma(\mathcal{H}) \to \mathcal{H}(r)$ is injective.*

As an immediate corollary to Theorem 3.11 and Theorem 3.12 we obtain:

Corollary 3.13. *For any core vertex $r \in \mathcal{N}_{k,m}$, the map*

$$\mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k,m}) \longrightarrow H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m})$$

is an isomorphism. In particular, $\mathrm{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k,m})$ *is a free* $R_{k,m}$*-module of rank one.*

The rest of this section is devoted to the proof of Theorem 3.12. We will be closely following the techniques from [MR04, §4.3], many times repeating the same arguments.

Recall that $\overline{T} = T/\mathfrak{m}T \cong T_{k,m}/(\mathfrak{m}, \mathbf{X})T_{k,m}$ and $\mathcal{X}_{k,m}$ is the graph defined as in §3.1.2 equipped with the Selmer sheaf $\mathcal{H}$. We define a subgraph $\mathcal{X}_{k,m}^0 = \mathcal{X}_{k,m}^0(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k,m})$ of $\mathcal{X}_{k,m}$ whose vertices are the core vertices of $\mathcal{X}_{k,m}$ and whose edges are defined as follows: We join n and $n\ell$ by an edge in $\mathcal{X}_{k,m}^0$ if and only if the localization map $H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, \overline{T}) \to H^1_f(\mathbb{Q}_\ell, \overline{T})$ is *non-zero*.

We now define the sheaf $\mathcal{H}^0$ on $\mathcal{X}_{k,m}^0$ as simply the restriction of the Selmer sheaf $\mathcal{H}$ to $\mathcal{X}_{k,m}^0$.

Definition 3.14. A simplicial sheaf $\mathcal{H}$ on a graph $\mathcal{X}$ is *locally free of rank one* if for every vertex v and edge $e = \{v, v'\}$ the modules $\mathcal{H}(v)$ and $\mathcal{H}(e)$ are free of rank one and the vertex edge homomorphisms ψ_v^e are isomorphisms.

We will prove below that the graph $\mathcal{X}_{k,m}^0$ is connected and $\mathcal{H}^0$ is locally free of rank one. This will be the essential step to prove Theorem 3.12.

Proposition 3.15. *The graph* $\mathcal{X}_{k,m}^0$ *defined above is connected.*

Proof. Since the edges of $\mathcal{X}_{k,m}^0$ are defined in terms of $\overline{T}$ (and not $T_{k,m}$ itself), [MR04, Theorem 4.3.12] applies. $\qquad\square$

Proposition 3.16. *The sheaf* $\mathcal{H}^0$ *is locally free of rank one.*

Proof. If n is a vertex of $\mathcal{X}_{k,m}^0$, then n is a core vertex, thus $\mathcal{H}^0(n)$ is free of rank one by the definition of a core vertex. Further, $\mathcal{H}^0(n) := H^1_s(\mathbb{Q}_\ell, T_{k,m}) \otimes G_{n\ell}$ is free of rank one as well by Lemma 2.19, since $\ell \in \mathcal{P}_{k,m}$.

Suppose e is the edge $\{n, n\ell\}$ in $\mathcal{X}_{k,m}^0$. By (11), we have $H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{k,m})[\mathcal{M}] \cong H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, \overline{T})$, and by Proposition 2.11, $H^1_f(\mathbb{Q}_\ell, T_{k,m})[\mathcal{M}] \cong H^1_f(\mathbb{Q}_\ell, \overline{T})$.

Further, by the choice of n and by Lemma 2.19, both $H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{k,m})$ and $H^1_f(\mathbb{Q}_\ell, T_{k,m})$ are free of rank one over $R_{k,m}$, so the non-triviality of the map $H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, \overline{T}) \to H^1_f(\mathbb{Q}_\ell, \overline{T})$ implies, by Nakayama's lemma, that the map

$$H^1_{\mathcal{F}_{\mathrm{can}}(n)}(\mathbb{Q}, T_{k,m}) \longrightarrow H^1_f(\mathbb{Q}_\ell, T_{k,m})$$

is an isomorphism. By Lemma 2.19, the map

$$\mathcal{H}^0(n) \longrightarrow \mathcal{H}^0(e) := H^1_s(\mathbb{Q}_\ell, T_{k,m}) \otimes G_{n\ell}$$

is an isomorphism. A similar argument (and making use of Lemma 2.20 this time instead of Lemma 2.19) shows that the map $\mathcal{H}^0(n\ell) \to \mathcal{H}^0(e)$ is an isomorphism as well. $\qquad\square$

Proposition 3.17. *Suppose that* $\boldsymbol{\kappa} \in \mathrm{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k,m})$ *and* $\kappa_r = 0$ *for some core vertex* r, *then* $\kappa_n = 0$ *for all core vertices* n.

Proof. For any core vertex n, one can find a path $P = \{r = v_0, v_1, \ldots, v_k = n\}$ by Proposition 3.15. Let e_i denote the edge $\{v_i, v_{i+1}\}$. Then by Proposition 3.16, the map

$$\Psi_P := (\psi_{v_k}^{e_{k-1}})^{-1} \circ \psi_{v_{k-1}}^{e_{k-1}} \circ \cdots \circ (\psi_{v_1}^{e_0})^{-1} \circ \psi_{v_0}^{e_0} : \mathcal{H}(r) \longrightarrow \mathcal{H}(n)$$

is well-defined and is an isomorphism. By the definition of a Kolyvagin system, $\Psi_P(\kappa_r) = \kappa_n$. This proves the theorem. $\qquad\square$

For a class $c \in H^1(\mathbb{Q}, M)$ and any prime ℓ, define $c_\ell := \mathrm{loc}_\ell(c) \in H^1(\mathbb{Q}_\ell, T)$ and write $c_{\ell,s} := \mathrm{loc}_\ell^s(c) \in H_s^1(\mathbb{Q}_\ell, M)$ for the projection of the class c_ℓ to the singular quotient $H_s^1(\mathbb{Q}_\ell, M)$.

Lemma 3.18 and Lemma 3.19 below are extensions of [MR04, Proposition 3.6.1] and [MR04, Lemma 4.1.7(iv)], respectively.

Lemma 3.18. *Suppose c_1 , $c_2 \in H^1(\mathbb{Q}, T_{k,m})$ and c_3 , $c_4 \in H^1(\mathbb{Q}, T_{k,m}^*)$ are all non-zero. For every $u, v \in \mathbb{Z}^+$, there is a subset $S \subset \mathcal{P}_{u,v}$ of positive density such that, for $\ell \in S$, the localizations $(c_i)_\ell$ are all non-zero.*

Mazur and Rubin state Proposition 3.6.1 of loc.cit. only in the case when the coefficient ring R is principal artinian. One can check that the arguments of [MR04, Page 31] go through *verbatim* when the coefficient ring is assumed only to be an artinian ring (not necessarily principal artinian) and give a proof of Lemma 3.18.

Following [MR04], define

$$\lambda(n, M) := \mathrm{length}_\mathcal{O} \, H_\mathcal{F}^1(\mathbb{Q}, M)$$

for $M = T_{k,m}, T_{k,m}^*, \overline{T}, \overline{T}^*$; and $\mathcal{F} = \mathcal{F}_{\mathrm{can}}(n)$ or $\mathcal{F}_{\mathrm{can}}(n)^*$.

Lemma 3.19. *Suppose $n\ell \in \mathcal{N}_{k,m}$ and assume that the maps induced from the natural localization maps*

$$H_{\mathcal{F}_{\mathrm{can}}(n)}^1(\mathbb{Q}, T_{k,m})[\mathcal{M}] \longrightarrow H_f^1(\mathbb{Q}_\ell, T_{k,m})$$

$$H_{\mathcal{F}_{\mathrm{can}}(n)^*}^1(\mathbb{Q}, T_{k,m}^*)[\mathcal{M}] \longrightarrow H_f^1(\mathbb{Q}_\ell, T_{k,m}^*)$$

are both non-zero. Then

    (i) $\lambda(n\ell, \overline{T}) = \lambda(n, \overline{T}) - 1$.
    (ii) $\lambda(n\ell, \overline{T}^*) = \lambda(n, \overline{T}^*) - 1$.

We will include the proof of Lemma 3.19 despite following [MR04] quite closely.

Proof. Since the difference $\lambda(r, \overline{T}) - \lambda(r, \overline{T}^*)$ is independent of r (by [MR04, Corollary 2.3.6]), it suffices to check only (ii). There is a commutative diagram

$$
\begin{array}{ccc}
H_{\mathcal{F}_{\mathrm{can}}(n)^*}^1(\mathbb{Q}, T_{k,m}^*)[\mathcal{M}] & \xrightarrow{\mathrm{loc}_\ell} & H_f^1(\mathbb{Q}_\ell, T_{k,m}^*)[\mathcal{M}] \\
\cong \Big\uparrow & & \cong \Big\uparrow \\
H_{\mathcal{F}_{\mathrm{can}}(n)^*}^1(\mathbb{Q}, \overline{T}^*) & \xrightarrow{\mathrm{loc}_\ell} & H_f^1(\mathbb{Q}_\ell, \overline{T}^*)
\end{array}
$$

where the left vertical isomorphism is [MR04, Lemma 3.5.3]. By the assumption of the Lemma, the upper horizontal map is non-zero, therefore the lower horizontal map is non-zero as well. However, $H_f^1(\mathbb{Q}_\ell, \overline{T}^*)$ is a one-dimensional $\mathbb{F}$-vector space, hence the lower horizontal map is surjective. Similarly, one may prove that the localization map $H_{\mathcal{F}_{\mathrm{can}}(n)}^1(\mathbb{Q}, \overline{T}) \to H_f^1(\mathbb{Q}_\ell, \overline{T})$ is surjective as well. By [MR04, Lemma 4.1.7(ii)] (which still holds since we are working with the same residual representation $\overline{T} = T_{k,m}/\mathcal{M} \cdot T_{k,m}$), we conclude that

$$H_{\mathcal{F}_{\mathrm{can}}(n\ell)^*}^1(\mathbb{Q}, \overline{T}^*) = H_{\mathcal{F}_{\mathrm{can}}^\ell(n)^*}^1(\mathbb{Q}, \overline{T}^*) \subset H_{\mathcal{F}_{\mathrm{can}}(n)^*}^1(\mathbb{Q}, \overline{T}^*).$$

Thus, we have a short exact sequence

$$0 \longrightarrow H_{\mathcal{F}_{\mathrm{can}}(n\ell)^*}^1(\mathbb{Q}, \overline{T}^*) \longrightarrow H_{\mathcal{F}_{\mathrm{can}}(n)^*}^1(\mathbb{Q}, \overline{T}^*) \longrightarrow H_f^1(\mathbb{Q}_\ell, \overline{T}^*) \longrightarrow 0.$$

This, together with the fact that $H_f^1(\mathbb{Q}_\ell, \overline{T}^*)$ is a one dimensional $\mathbb{F}$-vector space (as $\ell \in \mathcal{P}_{k,m}$) completes the proof of (ii). $\qquad\square$

Proposition 3.20. *Suppose that* $\boldsymbol{\kappa} \in \mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k,m})$ *and* $\kappa_n = 0$ *for any core vertex* n*, then* $\boldsymbol{\kappa} = 0$.

Proof. We need to show that $\kappa_r = 0$ for every $r \in \mathcal{N}_{k,m}$. We prove this by induction on $\lambda(r, \overline{T}^*)$ as in [MR04]. By the assumption of Proposition, $\kappa_r = 0$ for all r with $\lambda(r, \overline{T}^*) = 0$.

Suppose now that $\lambda(r, \overline{T}^*) > 0$ and suppose $\kappa_r \neq 0$. Using[3] Lemma 3.18, we may choose a prime $\ell \in \mathcal{P}_{k,m}$ such that

  (a) $(\kappa_r)_\ell \neq 0$,
  (b) The maps

$$H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m})[\mathcal{M}] \longrightarrow H^1_f(\mathbb{Q}_\ell, T_{k,m})$$

$$H^1_{\mathcal{F}_{\mathrm{can}}(r)^*}(\mathbb{Q}, T^*_{k,m})[\mathcal{M}] \longrightarrow H^1_f(\mathbb{Q}_\ell, T^*_{k,m})$$

  are both non-zero.

Now Lemma 3.19 and (b) above imply that $\lambda(r\ell, \overline{T}^*) < \lambda(r, \overline{T}^*)$, therefore $\kappa_{r\ell} = 0$ by the induction hypothesis. However, by the definition of a Kolyvagin system and by (a), it follows that $(\kappa_{r\ell})_{\ell,\mathrm{s}} \neq 0$. This contradicts with the induction hypothesis that $\kappa_{r\ell} = 0$, which shows that $\kappa_r = 0$ for all $r \in \mathcal{N}_{k,m}$. $\qquad\square$

Proof of Theorem 3.12. Suppose that $\boldsymbol{\kappa} \in \Gamma(\mathcal{H})$ and that $\kappa_r = 0$ for the core vertex r given in the statement of Theorem 3.12. It follows from Proposition 3.17 that $\kappa_n = 0$ for any core vertex n, therefore $\boldsymbol{\kappa} = 0$ by Proposition 3.20. $\qquad\square$

3.2. **Kolyvagin Systems for** $T \otimes \Lambda$. Using the results from §3.1, we prove (Theorem 3.23 below)

$$\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P}) := \varprojlim_{k,m} \left(\varinjlim_j \mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_j) \right)$$

is a free Λ-module of rank one, under the hypotheses which we set in §2.2.

Lemma 3.21. *For any* $j \geq k + m$*, the natural restriction map*

$$\mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k+m}) \longrightarrow \mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_j)$$

is an isomorphism.

Proof. By Corollary 3.13 applied with a core vertex $r \in \mathcal{N}_j$ (such r exists by [MR04, Corollary 4.1.9] and Theorem 2.27), we have isomorphisms

$$\mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k+m}) \overset{\sim}{\longrightarrow} H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m}) \overset{\sim}{\longleftarrow} \mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_j)$$

compatible with the restriction map $\mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k+m}) \to \mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_j)$. $\qquad\square$

---

[3]We make use of Lemma 3.18 as follows: By our assumption that $\lambda(r, \overline{T}^*) > 0$ and using the isomorphism (11) above along with [MR04, Lemma 3.5.3], it follows that

$$H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m})[\mathcal{M}] \neq 0 \neq H^1_{\mathcal{F}_{\mathrm{can}}(r)^*}(\mathbb{Q}, T^*_{k,m})[\mathcal{M}].$$

Hence, there are non-zero classes

$$c \in H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m})[\mathcal{M}] \subset H^1(\mathbb{Q}, T_{k,m}) \text{ and } c^* \in H^1_{\mathcal{F}_{\mathrm{can}}(r)^*}(\mathbb{Q}, T^*_{k,m})[\mathcal{M}] \subset H^1(\mathbb{Q}, T^*_{k,m}).$$

Now given also that $0 \neq \kappa_r \in H^1(\mathbb{Q}, T_{k,m})$, we invoke Lemma 3.18 with non-zero κ_r and $c \in H^1(\mathbb{Q}, T_{k,m})$ and $c^* \in H^1(\mathbb{Q}, T^*_{k,m})$, in order to find a prime ℓ with the desired properties enlisted above.

Lemma 3.22. *The maps*

$$H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m}) \longrightarrow H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k',m'})$$
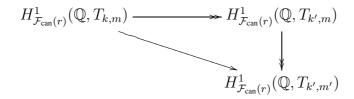
$$\mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k+m}) \longrightarrow \mathbf{KS}(T_{k',m'}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k+m})$$

are surjective for $k \geq k'$, $m \geq m'$ and for any core vertex $r \in \mathcal{N}_{k,m}$.

Proof. We will first prove that the second map is surjective assuming the first map is. By Corollary 3.13 and Lemma 3.21 applied with a core vertex $r \in \mathcal{N}_{k,m}$ to both $T_{k,m}$ and $T_{k',m'}$, we obtain the following commutative diagram with vertical isomorphisms:

$$
\begin{array}{ccc}
\mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k+m}) & \longrightarrow & \mathbf{KS}(T_{k',m'}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k+m}) \\
\cong \downarrow & & \cong \downarrow \\
H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m}) \otimes G_r & \longrightarrow & H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k',m'}) \otimes G_r
\end{array}
$$

It now follows at once that the upper horizontal map in the diagram is surjective as well.

So it remains to prove that the map

$$H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m}) \longrightarrow H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k',m'})$$

is surjective. We have the following commutative diagram, where the vertical isomorphism is obtained from an appropriate version of Lemma 2.28:

$$
\begin{array}{ccc}
H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m}) & \xrightarrow{\ \mathrm{Reduction}\ } & H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k',m}) \\
& \searrow^{\varpi^{k-k'}} & \quad\ \cong \downarrow [\varpi^{k-k'}] \\
& & H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m})[p^{k'}]
\end{array}
$$

Since $r \in \mathcal{N}_{k,m}$ is a core vertex (therefore $H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m})$ is a free $R_{k,m}$-module of rank one), the map on the diagonal is surjective. This proves that the horizontal map is surjective as well. One shows in a similar manner that the map $H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k',m}) \to H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k',m'})$ is also surjective. We therefore have a commutative diagram

$$
\begin{array}{ccc}
H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k,m}) & \longrightarrow & H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k',m}) \\
& \searrow & \quad \downarrow \\
& & H^1_{\mathcal{F}_{\mathrm{can}}(r)}(\mathbb{Q}, T_{k',m'})
\end{array}
$$

which shows that the map on the diagonal is surjective, and the proof is complete. $\qquad \square$

Theorem 3.23. *Under our running hypotheses,*

  (i) *the Λ-module $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ is free of rank one,*
  (ii) *the specialization map $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P}) \to \overline{\mathbf{KS}}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ is surjective.*

Proof. By Lemma 3.21, it follows that $\varinjlim_j \mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_j) = \mathbf{KS}(T_{k,m}, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_{k+m})$. Now using Corollary 3.13 and Lemma 3.22, the proof follows. $\qquad \square$

Remark 3.24. Notice that the collection of ideals $\{(\mathfrak{m}^k, \mathbf{X}^m)\}_{k,m \in \mathbb{Z}^+}$ form a base of neighborhoods at $0 \in \Lambda$. Using this fact, one may see without difficulty that our definition above for the module of Λ-adic Kolyvagin systems $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P})$ agrees with Mazur and Rubin's definition [MR04, §5.3] of *generalized* module of Kolyvagin Systems $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_\Lambda, \mathcal{P})$. We also recall the module $\mathbf{KS}(T \otimes \Lambda, \mathcal{F}_\Lambda, \mathcal{P})$; what Mazur and Rubin define in [MR04, Definition 3.1.3] as the module of Kolyvagin systems. By definition, there are natural maps

$$\mathbf{KS}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P}) \longrightarrow \mathbf{KS}(T_{k,m}, \mathcal{F}_{\text{can}}, \mathcal{P}_{k,m})$$

for every $k, m \in \mathbb{Z}^+$. These in the limit give rise to a homomorphism of Λ-modules

$$(18) \qquad \mathbf{KS}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P}) \longrightarrow \overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P}).$$

In this paper, we leave the question whether the map (18) is an isomorphism or not aside, since, as far as the applications of the Kolyvagin system machinery is concerned (i.e., bounding Selmer groups), any element of $\mathbf{KS}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P})$ has the exact same use as an element of the module $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P})$. For this reason, when we say κ is a Λ-adic Kolyvagin system, we mean (by slight abuse) that κ is an element of one of the three modules of Kolyvagin systems discussed above.

Remark 3.25. Theorem 3.23 says, under the running hypotheses, that $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P})$ is generated by a Kolyvagin system κ whose *blind spot* (see [MR04, Definition 3.1.6] for a definition) does not contain any prime ideal of Λ. Even if $\mathbb{H}.\mathbf{T}$ and $\mathbb{H}.\mathbf{sEZ}$ fails, but $\mathbb{H}.\mathbf{EZ}$ holds for T, we still expect to have a Λ-adic Kolyvagin system for the triple $(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P})$ which does not have the ideal $(\gamma - 1)$ in its blind spot. However, we no longer expect that the specialization map

$$\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P}) \longrightarrow \overline{\mathbf{KS}}(T, \mathcal{F}_{\text{can}}, \mathcal{P})$$

to be surjective in this case. Although we are unable to formulate a precise conjecture for the size of the cokernel of this map, we expect that its size will be related to $\#(T^*)^{G_{\mathbb{Q}_p}}$ and $\#A^{\mathcal{I}_\ell}/(A^{\mathcal{I}_\ell})_{\text{div}}$ (for $\ell \neq p$). In fact, using the proof of [MR04, Proposition 6.2.6], one can show that

$$p \mid \#\text{coker}\left\{\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P}) \longrightarrow \overline{\mathbf{KS}}(T, \mathcal{F}_{\text{can}}, \mathcal{P})\right\}$$

if one of $\#(T^*)^{G_{\mathbb{Q}_p}}$ and $\#A^{\mathcal{I}_\ell}/(A^{\mathcal{I}_\ell})_{\text{div}}$ is greater than one. Furthermore, the author proves in [Büy09c] that if $p^\alpha | \#A^{\mathcal{I}_\ell}/(A^{\mathcal{I}_\ell})_{\text{div}}$, then

$$p^\alpha \mid \#\text{coker}\left\{\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P}) \longrightarrow \overline{\mathbf{KS}}(T, \mathcal{F}_{\text{can}}, \mathcal{P})\right\}.$$

4. Applications and Further Discussion

In this section, we exhibit several arithmetic implications of Theorem 3.23. First in §4.1, we go over well-known examples of Kolyvagin Systems over the cyclotomic Iwasawa algebra and their applications, such as the Kolyvagin Systems derived from cyclotomic unit Euler system and Kato's Euler system. Theorem 3.23 does not prove anything new here, except for the fact that the cyclotomic unit Kolyvagin system (resp., Kato's Kolyvagin system) over the cyclotomic Iwasawa algebra lies inside the free rank-one Λ-module of Λ-adic Kolyvagin systems.

Next in §4.2, we discuss the relation of the cohomology classes we prove to exist in Theorem 3.23 with p-adic L-functions. Although our construction of these classes has no reference to the L-values, the rigidity of the Λ-adic Kolyvagin Systems (i.e.,Theorem 3.23(i)) enables us to set up a connection with p-adic L-functions via Perrin-Riou and Rubin's (conjectural) Euler systems (c.f., [Rub00, §8]).

At the end in §4.3, we apply our results to study the *Rubin-Stark elements* [Rub96] along the cyclotomic $\mathbb{Z}_p$-tower. This is the only section that the base field is different from $\mathbb{Q}$, and we will

utilize a version of Theorem 3.23 with a Selmer structure different from $\mathcal{F}_{\text{can}}$. We explain how to use these classes (that we prove to exist, and that also independently come (thanks to [Büy09b]) from the conjectural Rubin-Stark elements which we assume that they exist) to study the Iwasawa theory of totally real fields. Wiles [Wil90b] proved the main conjecture in this setting. In §4.3, we sketch a strategy (that is developed in full in [Büy09b]) to give a proof (conditional on the Rubin-Stark conjectures) of Iwasawa's main conjecture for totally real fields. Along the way, we obtain a result on the local Iwasawa theory of Rubin-Stark elements (see Theorem 4.15 below).

See also [Büy08] for an important arithmetic application of our rigidity result (Theorem 3.23(i)) which we do not include here. In loc.cit., the author establishes a connection between the *Stickelberger elements* and Rubin-Stark elements using Theorem 3.23(i). More precisely, let k be a totally real field and let $\chi : G_k \to \mathcal{O}^\times$ be a totally odd character of finite prime-to-p order. Let $\rho_{\text{cyc}} : G_k \to \mathbb{Z}_p^\times$ be the cyclotomic character. In [Büy08], the author constructs a Λ-adic Kolyvagin system for the representation $\mathcal{O}(\chi)$ (a similar, yet different construction was given by Kurihara [Kur03] prior to this work). Using a formal twisting argument, this Kolyvagin system gives rise to a Kolyvagin system for the Galois representation $\rho_{\text{cyc}}\omega^{-1} \otimes \mathcal{O}(\chi) = \mathcal{O}(1) \otimes \mathcal{O}(\chi\omega^{-1})$. For the Galois representation $\mathcal{O}(1) \otimes \mathcal{O}(\chi\omega^{-1})$, the author used in [Büy09b] the (conjectural) Rubin-Stark elements to construct a Λ-adic Kolyvagin system. Thanks to Theorem 3.23(i) (slightly enhanced as Theorem 4.10(i) below), these two Λ-adic Kolyvagin systems should therefore differ from each other at most by multiplication by an element of Λ, as they both live in a free Λ-module of rank one. Note that the existence of the Stickelberger element Kolyvagin system constructed in [Büy08] relies only on a special case of Brumer's conjecture, see [Wil90a, Kur03, Gre04] for a proof of Brumer's conjecture in various cases.

4.1. **Classical Examples.** Fix once and for all a rational prime $p > 2$. In this section we do not claim any new results, except in Proposition 4.1 (resp., Proposition 4.2), we explain that the Kolyvagin system of cyclotomic units (resp., Kato's Kolyvagin system) generate the cyclic module of Λ-adic Kolyvagin systems, under certain hypotheses.

4.1.1. *Cyclotomic Units.* Let $T = \mathcal{O}(1) \otimes \rho^{-1}$, where $\rho : G_\mathbb{Q} \to \mathcal{O}^\times$ is an even character of finite prime-to-p order. Let L be the cyclic extension of $\mathbb{Q}$ which is cut out by the character ρ and set $\Delta = \text{Gal}(L/\mathbb{Q})$. For any $\mathcal{O}[\Delta]$-module A, let A^ρ denote the ρ-isotypic component of A.

Fix a collection $\{\zeta_n : n \in \mathbb{Z}^+\}$ such that ζ_n is a primitive n-th root of unity and $\zeta_{mn}^m = \zeta_n$ for every $m \in \mathbb{Z}^+$. Whenever F is a finite abelian extension of $\mathbb{Q}$ of conductor f, we define c_F as the image of $\mathbf{N}_{\mathbb{Q}(\mu_{fp})/F}(\zeta_{fp} - 1) \in F^\times$ under the Kummer map $F^\times \hookrightarrow H^1(F, \mathcal{O}(1))$. The collections $\{c_F\}_F$ is an Euler system in the sense of [Rub00, §II] for the representation $\mathcal{O}(1)$, and is called the *cyclotomic unit Euler system*. One can modify these units, as in [Rub00, §IX.6], to obtain an Euler system $\mathbf{c}$ for $\mathcal{O}(1)$ satisfying [MR04, Definition 3.2.2].

By a standard twisting argument (c.f., [Rub00, Proposition II.4.2]), the Euler system $\mathbf{c}$ gives an Euler system $\mathbf{c}^\rho$ for the representation $T = \mathcal{O}(1) \otimes \rho^{-1}$. By [MR04, Theorem V.3.3], the Euler system $\mathbf{c}^\rho$ gives rise to a Λ-adic Kolyvagin system $\boldsymbol{\kappa}^{\rho,\infty} \in \overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P})$.

Assume now that $\rho(p) \neq 1$ and assume for simplicity that ρ is unramified at p. Then it is straightforward to check that T satisfies our hypotheses **H**.1-**H**.4, $\mathbb{H}.\mathbf{T}$ and $\mathbb{H}.\mathbf{sEZ}$; thus Theorem 3.23 applies to conclude that the Λ-module $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P})$ is free of rank one.

Proposition 4.1. *The Λ-adic Kolyvagin system $\boldsymbol{\kappa}^{\rho,\infty}$ is Λ-primitive* (*in the sense of* [MR04, Definition 5.3.9]) *and it generates the free Λ-module* $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P})$.

Proof. For any sub-quotient M of $T \otimes \Lambda$, we simply write $\overline{\mathbf{KS}}(M)$ instead of $\overline{\mathbf{KS}}(M, \mathcal{F}_{\text{can}}, \mathcal{P})$. Let $\boldsymbol{\kappa}^\rho$ denote the image of $\boldsymbol{\kappa}^{\rho,\infty}$ under the specialization map $\overline{\mathbf{KS}}(T \otimes \Lambda) \to \overline{\mathbf{KS}}(T)$. By [MR04,

Remark 6.1.8], the Kolyvagin system κ^ρ is primitive, i.e., its image $\overline{\kappa^\rho}$ under the map

$$\overline{\mathbf{KS}}(T) \longrightarrow \mathbf{KS}(T/\mathfrak{m}T)$$

is non-zero. This proves that the image of $\kappa^{\rho,\infty}$ under the map $\overline{\mathbf{KS}}(T \otimes \Lambda) \to \overline{\mathbf{KS}}(T \otimes \Lambda/\mathfrak{p})$ is non-zero for any height-one prime $\mathfrak{p} \subset \Lambda$; as we have a commutative diagram

$$
\begin{array}{ccc}
\kappa^{\rho,\infty} \in \overline{\mathbf{KS}}(T \otimes \Lambda) & & \\
\Big\downarrow & \Big\downarrow & \searrow \\
& & \overline{\mathbf{KS}}(T \otimes \Lambda/\mathfrak{p}) \\
\overline{\kappa^\rho} \in \mathbf{KS}(T/\mathfrak{m}T) & & \nearrow
\end{array}
$$

and $\overline{\kappa^\rho} \neq 0$. $\hfill\square$

See [MR04, Theorem 5.3.10] for the standard application of the Λ-adic Kolyvagin system $\kappa^{\rho,\infty}$.

4.1.2. *Kato's Euler System.* Fix an elliptic curve $E_{/\mathbb{Q}}$, assume that $p > 3$ and $\mathcal{O} = \mathbb{Z}_p$. Let $T = T_p(E)$ be the p-adic Tate module. Suppose also that the p-adic representation

$$\rho_E : G_\mathbb{Q} \to \mathrm{Aut}(E[p^\infty]) \cong \mathrm{GL}_2(\mathbb{Z}_p)$$

is surjective. Let N be the conductor of E, and let N_1 (resp., N_2) be the product of primes $\ell | N$ such that E has split (resp., non-split) multiplicative reduction at ℓ. Kato [Kat04] has constructed an Euler system for $(T_p(E), \mathcal{P}')$, where $\mathcal{P}'$ is the set of rational primes not dividing $NpDD'$ with two auxiliary positive integers D and D' used in Kato's construction. Set $\mathcal{P}^{(0)} = \mathcal{P}' \cap \mathcal{P}$ (recall the definition of $\mathcal{P}$ from §2.4 above) and $\mathcal{P}^{(0)}_{k,m} = \mathcal{P}' \cap \mathcal{P}_{k,m}$. Using [MR04, Theorem 5.3.3], Kato's Euler system gives rise to a Λ-adic Kolyvagin system $\kappa^{\mathrm{Kato},\infty} \in \overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P}^{(0)})$. Let κ^{Kato} denote the image of $\kappa^{\mathrm{Kato},\infty}$ under the map $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P}^{(0)}) \to \overline{\mathbf{KS}}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P}^{(0)})$.

Proposition 4.2. *Assume that E has good reduction at p, and also that,*
   (E0) $L(E,1) \neq 0$, *where $L(E,s)$ is the Hasse-Weil L-function attached to E,*
   (E1) $\mathbb{H}.\mathbf{sEZ}$ *holds: $E(\mathbb{Q}_p)[p] = 0$,*
   (E2) $\mathbb{H}.\mathbf{T}$ *holds: p does not divide the Tamagawa factors c_ℓ for any prime $\ell \neq p$,*
   (E3) $p \nmid \prod_{\ell | N_1}(\ell - 1) \prod_{\ell | N_2}(\ell + 1)$,
   (E4) *the p-part of the Birch and Swinnerton-Dyer conjecture holds for E.*
Then $\kappa^{\mathrm{Kato},\infty}$ is Λ-primitive and generates the free Λ-module $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P}^{(0)})$.

Proof. Let $L_N(E,s)$ be the L-function with the Euler factors at primes dividing the conductor N of E removed, and let Ω be a fundamental period. As in the proof of Proposition 4.1, the assertion that $\kappa^{\mathrm{Kato},\infty}$ is Λ-primitive will follow once we verify that the Kolyvagin system κ^{Kato} is primitive. This, however, follows at once from [MR04, Theorem 6.2.4 and Corollary 5.2.13(ii)], along with the observation that we have

$$\mathrm{ord}_p\left(\frac{L(E,1)}{\Omega}\right) = \mathrm{ord}_p\left(\frac{L_N(E,1)}{\Omega}\right)$$

thanks to (E3).

We also note that, thanks to our assumptions on ρ_E, the hypotheses **H.1**-**H.3** hold for $T = T_p(E)$, and **H.4** holds since we assumed $p > 3$. Furthermore, the core Selmer rank $\chi(T, \mathcal{F}_{\mathrm{can}})$ of the Selmer structure $\mathcal{F}_{\mathrm{can}}$ on T equals to $\mathrm{rank}_{\mathbb{Z}_p} T^- = 1$, where T^- is the -1-eigenspace for any complex conjugation. Hence, thanks to (E1) and (E2), Theorem 3.23 applies to conclude that the Λ-module $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P}^{(0)})$ is free of rank one. $\hfill\square$
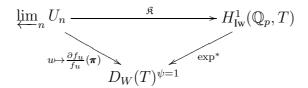
Remark 4.3.

(i) We note that the assumption that E has good reduction at p is not necessary for Theorem 3.23 to hold; we only need this assumption to use Kato's calculations with his Euler system: We prove in Theorem 3.23 above that the Λ-module $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P}^{(0)})$ is free of rank one even when only (E1) and (E2) holds.

(ii) If (E1) or (E2) fails, we do not expect the Λ-adic Kolyvagin system $\boldsymbol{\kappa}^{\mathrm{Kato},\infty}$ to be Λ-primitive; see [MR04, Proposition 6.2.6] and [Büy09c].

4.2. Λ-adic Kolyvagin Systems and p-adic L-functions.

Examples we discuss in the previous section suggests that the Λ-adic Kolyvagin Systems we prove to exist should relate to the p-adic L-functions. In this section, we explore this in much greater generality and establish a link between our Λ-adic Kolyvagin systems and Perrin-Riou's conjectural p-adic L-functions.

To motivate, we revisit the case $T = \mathbb{Z}_p(1)$ and the Euler system of cyclotomic units. See [Rub00, §VIII.5] or [PR94a] for a detailed discussion of what follows in this paragraph. Let U_n be the local units inside $\mathbb{Q}_{p,n}$, the unique extension of $\mathbb{Q}_p$ of degree p^n inside the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$; and let $\mathcal{O}_n$ be the ring of integers of $\mathbb{Q}_{p,n}$. There is an isomorphism

$$\exp^* : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T) \xrightarrow{\sim} D_W(T)^{\psi=1}$$

(see Theorem A.5 and Theorem A.8 below), where W is the prime-to-p part of $\mathrm{Gal}(\mathbb{Q}_p(\mu_p^\infty)/\mathbb{Q}_p)$; and $D_W(T)^{\psi=1}$ is the W-fixed part of $D(T)^{\psi=1}$, and finally, $D(T)$ is Fontaine's (φ, Γ)-module attached to T. We then have a commutative diagram (which is essentially the explicit reciprocity law of Iwasawa [Iwa68] in this setting)

$$
\begin{array}{ccc}
\varprojlim_n U_n & \xrightarrow{\;\;\mathfrak{K}\;\;} & H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T) \\
{\scriptstyle u \mapsto \frac{\partial f_u}{f_u}(\boldsymbol{\pi})} \searrow & & \swarrow {\scriptstyle \exp^*} \\
& D_W(T)^{\psi=1} &
\end{array}
$$

Here, f_u is the Coleman's power series attached to $u \in \varprojlim_n U_n$; $\boldsymbol{\pi} = \{\pi_n\} \in \varprojlim_n \mathcal{O}_n$ and π_n is a distinguished uniformizer of $\mathcal{O}_n$ (which we will not define here); and $\mathfrak{K}$ is the Kummer map. It turns out that the image of $\{\mathbf{c}^{\mathrm{cycl}}_{\mathbb{Q}_n}\}_n \in \varprojlim_n U_n$ under $\exp^* \circ \mathfrak{K}$, where $\mathbf{c}^{\mathrm{cycl}}$ is the cyclotomic unit of Euler system, is the measure whose Amice transform gives rise to the Kubota-Leopoldt p-adic zeta function.

This example is part of a big conjectural picture (due to Perrin-Riou [PR95]). For a general $\mathbb{Z}_p[[G_{\mathbb{Q}}]]$-representation T, we conjecturally have the following diagram:

$$
\left\{ \begin{array}{c} \text{Leading terms of } \Lambda\text{-adic} \\ \text{Kolyvagin Systems for } T \otimes \Lambda \end{array} \right\} \longrightarrow H^1(\mathbb{Q}, T \otimes \Lambda) \xrightarrow{\exp^*} D_W(T)^{\psi=1} \xrightarrow{\mathfrak{A}} \left\{ \begin{array}{c} p\text{-adic} \\ L\text{-functions} \end{array} \right\}
$$

Here, $\mathfrak{A}$ is the Amice transform and the leading term of a Λ-adic Kolyvagin system κ^∞ is the term $\kappa_1^\infty \in \varprojlim_{k,m} H^1(\mathbb{Q}, T_{k,m}) \cong H^1(\mathbb{Q}, T \otimes \Lambda)$.

In [Rub00, §VIII], Rubin proposes to go the other way in the diagram above: To construct an Euler system for T starting from a collection of p-adic L-functions associated to T over various abelian extensions of $\mathbb{Q}$. In what follows, we will closely follow Rubin's exposition from [Rub00].

Suppose until the end of this section that

- T is a $G_{\mathbb{Q}}$-stable lattice inside the p-adic realization $V = T \otimes \mathbb{Q}_p$ of a *motivic structure* (in the sense of [FPR94, §III]) and that V is crystalline at p,
- $\mathcal{O} = \mathbb{Z}_p$.

Assume further that the *generic core Selmer rank* of $\mathcal{F}_{\mathrm{can}}$ on $T \otimes \Lambda$ is one. Throughout this section, a different ring of periods will be utilized than the one mentioned in Appendix A, which was also constructed by Fontaine, called the crystalline period ring and denoted by $\mathbb{B}_{\mathrm{cris}}$.

Let $D_{\text{cris}}(V) = (\mathbb{B}_{\text{cris}} \otimes_{\mathbb{Q}_p} V)^{G_{\mathbb{Q}_p}}$ denote Fontaine's filtered vector space attached to V and let $V^* = \text{Hom}(V, \mathbb{Q}_p(1))$. If F is an abelian extension of $\mathbb{Q}$ which is unramified at p, we also let $D_{\text{cris}}^F(V) = D_{\text{cris}}(\text{Ind}_{F/\mathbb{Q}}V)$. Let $\mathbb{H}$ denote the extended Iwasawa algebra defined by Perrin-Riou [PR94b, §1], and let $\mathbb{K} = \text{Frac}(\mathbb{H})$ denote the field of fractions of $\mathbb{H}$. In [PR94b], Perrin-Riou constructs a $\mathbb{Z}_p[[\text{Gal}(F\mathbb{Q}_\infty)/\mathbb{Q}]]$-module homomorphism (what she calls an expanded logarithm, and which is closely related to $\exp^*$ of Theorem A.5 and Theorem A.8)

$$\mathcal{L}_F : \bigoplus_{v|p} \varprojlim_n H^1((F\mathbb{Q}_n)_v, T) \longrightarrow \mathbb{K} \otimes D_{\text{cris}}^F(V).$$

Furthermore, Perrin-Riou and Rubin conjecture that for every extension E of $\mathbb{Q}_p$ and every character $\chi : G_{\mathbb{Q}} \to E^\times$ of finite order, unramified at p, and $r \in \mathbb{Z}^+$ that is divisible by the conductor of χ, there is an element

$$\mathbf{L}_r^{(p)}(T \otimes \chi) \in \mathbb{K} \otimes D_{\text{cris}}(V^* \otimes \chi^{-1})$$

which is characterized by a certain interpolation property (c.f., [PR95, §4.2]). We will not give any details on $\mathbf{L}_r^{(p)}(T \otimes \chi)$ and refer the reader to [PR95], except for the following rough version of the interpolation property which it conjecturally satisfies for characters ρ of Γ of finite order and for sufficiently large positive integers k:

$$\langle \chi_{\text{cycl}} \rangle^k \rho(\mathbf{L}_r^{(p)}(T \otimes \chi)) = (p\text{-Euler factor}) \times \frac{L_r(V \otimes \chi \omega^k \rho^{-1}, -k)}{\text{archimedean period}} \times (p\text{-adic period}).$$

Here, ω is the Teichmüller character and $\langle \chi_{\text{cycl}} \rangle$ is the character given by

$$\langle \chi_{\text{cycl}} \rangle := \omega^{-1} \chi_{\text{cycl}} : G_{\mathbb{Q}} \twoheadrightarrow \Gamma = \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}),$$

and $L_r(V \otimes \chi \omega^k \rho^{-1}, s)$ is the conjectural complex L-function of $V \otimes \chi \omega^k \rho^{-1}$ with the Euler factors at primes dividing r removed.

Let $\mathbb{Q}(\mu_r)^+$ be the maximal real subfield of $\mathbb{Q}(\mu_r)$ and write $\Delta_r = \text{Gal}(\mathbb{Q}(\mu_r)^+/\mathbb{Q})$. For every character $\chi : \Delta_r \to E^\times$ (where E is a finite extension of $\mathbb{Q}_p$ as above), let $\epsilon_\chi \in E[\Delta_r]$ be the idempotent associated with χ.

For $f \in \mathbb{K}$, let f^ι denote the image of f under the involution induced by $\gamma \mapsto \gamma^{-1}$ for $\gamma \in \text{Gal}(\mathbb{Q}_\infty(\mu_r)^+/\mathbb{Q})$. Define also $H^1_\infty(\mathbb{Q}(\mu_r)^+, T) := \varprojlim_n H^1(\mathbb{Q}_n(\mu_r)^+, T)$.

Conjecture. [Rub00, Conjecture VIII.2.6] *Assume $r \in \mathbb{Z}^+$ is prime to p, and T is as above. Suppose $\alpha \in \mathbb{Z}_p[[G_{\mathbb{Q}}]]$ annihilates $H^0(\mathbb{Q}_\infty(\mu_r), A)$.*

Then there is an element $\boldsymbol{\xi}_r = \boldsymbol{\xi}_r^{(\alpha)} \in H^1_\infty(\mathbb{Q}(\mu_r)^+, T)$ such that for every character χ as above

$$\epsilon_\chi \mathcal{L}_{\mathbb{Q}(\mu_r)^+}(\boldsymbol{\xi}_r) = \chi(\alpha) \mathbf{L}_r^{(p)}(T^* \otimes \chi)^\iota,$$

where $\chi(\alpha)$ is the image of α under the composition

$$\mathbb{Z}_p[[G_Q]] \longrightarrow \Lambda \otimes \mathbb{Z}_p[\Delta_r] \xrightarrow{1 \otimes \chi} \Lambda \otimes E \longrightarrow \mathbb{K} \otimes E.$$

Let N be the product of all rational primes where T is ramified. It follows from [Rub00, Lemma IV.2.5(i)] that

$$H^0(\mathbb{Q}_\infty(\mu_r), T) = H^0(\mathbb{Q}_\infty, T) \quad \text{and} \quad H^0(\mathbb{Q}_\infty(\mu_r), A) = H^0(\mathbb{Q}_\infty, A),$$

if r is prime to Np. Fix an element $\alpha \in \mathbb{Z}_p[[G_{\mathbb{Q}}]]$ which annihilates $H^0(\mathbb{Q}_\infty, A)$ (therefore also $H^0(\mathbb{Q}_\infty(\mu_r), A)$ for every $r \in \mathbb{Z}^+$ prime to Np). Assume that the weak Leopoldt conjecture (c.f., [PR95, §1.3]) holds for T^*, and $H^0(\mathbb{Q}_\infty, T) = 0$.

For every $r \in \mathbb{Z}^+$ prime to Np, let

$$\boldsymbol{\xi}_r = \{\xi_{n,r}\} \in H^1_\infty(\mathbb{Q}(\mu_r)^+, T) \text{ with } \xi_{n,r} \in H^1(\mathbb{Q}_n(\mu_r)^+, T)$$

be an element that satisfies Rubin's conjecture above. Then Rubin shows:

Proposition 4.4.[Rub00, Corollary VIII.3.2] *The collection*

$$\{\xi_{n,r} \in H^1(\mathbb{Q}_n(\mu_r)^+, T) : n \geq 0, \ r \ prime \ to \ Np\}$$

is an Euler system for $(T, \mathbb{Q}_\infty \mathbb{Q}^{\mathrm{ab},Np,+}, Np)$ *in the sense of* [Rub00, Definition II.1.1 and Remark II.1.3], *where* $\mathbb{Q}^{\mathrm{ab},Np,+}$ *is the maximal real subfield of the maximal abelian extension of* $\mathbb{Q}$ *unramified outside* Np.

Remark 4.5. Assume in this Remark that T satisfies the hypotheses **H.1**-**H.4**, $\mathbb{H}.\mathbf{T}$ and $\mathbb{H}.\mathbf{sEZ}$, in addition to the hypotheses of of the Conjecture above. We also assume that $\chi(T, \mathcal{F}_{\mathrm{can}}) = 1$. It therefore follows from Theorem 3.23 that the Λ-module $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ is free of rank one, and in fact it is generated by a Λ-primitive Kolyvagin system $\boldsymbol{\kappa}^\infty$. In this paragraph, we explain how $\boldsymbol{\kappa}^\infty$ we prove to exist relates to the conjectural collection $\{\xi_{n,r}\}$ of Perrin-Riou and Rubin. Theorem 5.3.3 of [MR04] applied on the conjectural Euler system $\{\xi_{n,r}\}$ of Proposition 4.4 gives rise to a Λ-adic Kolyvagin system $\boldsymbol{\kappa}^{\mathrm{PR}} \in \overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$. As $\boldsymbol{\kappa}^\infty$ generates the Λ-module $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$, there is a $\lambda \in \Lambda$ [†] such that

$$\boldsymbol{\kappa}^{\mathrm{PR}} = \lambda \cdot \boldsymbol{\kappa}^\infty.$$

This means the Λ-adic Kolyvagin system $\boldsymbol{\kappa}^\infty$ that we prove to exist in Theorem 3.23 is linked to the p-adic L-functions, as it is related to the conjectural classes of Perrin-Riou and Rubin.

   We also note that Theorem 3.23 proves a consequence of the conjectures of Perrin-Riou and Rubin we mentioned above, namely the existence of Λ-adic Kolyvagin Systems. In this sense, these conjectures borrow evidence (although quite weak) from Theorem 3.23.

4.3. **Iwasawa theory of Rubin-Stark elements and Kolyvagin Systems.** Let F be a totally real number field of degree r over $\mathbb{Q}$ and fix an algebraic closure $\overline{F}$ of F. For any rational prime ℓ and a G_F-module M, write $H^*(F_\ell, M)$ for the semi-local cohomology group at ℓ.

   In this section, our base field will be different from $\mathbb{Q}$, however our results from Sections 2 and 3 will apply (almost) verbatim.

   Let ρ be a totally even character of G_F (i.e., ρ is trivial on all complex conjugations inside G_F) into $\mathcal{O}^\times$ that has finite prime-to-p order, and let L be the fixed field of $\ker(\rho)$. We define f_ρ to be the conductor of ρ, and set $\Delta := \mathrm{Gal}(L/F)$. We assume that $(p, f_\chi) = 1$ and $\rho(\wp) \neq 1$ for any prime $\wp$ of F lying above p. Assume also for notational simplicity that p is unramified in $F/\mathbb{Q}$. Let T be the G_F-representation $\mathcal{O}(1) \otimes \rho^{-1}$.

Remark 4.6. T clearly satisfies the hypotheses **H.1**-**H.4** ($\mathbb{Q}$ replaced by F). Observe that the following versions of the hypotheses $\mathbb{H}.\mathbf{T}$ and $\mathbb{H}.\mathbf{sEZ}$ also hold for T:

   ($\mathbb{H}.\mathbf{T}_{/F}$) $A^{\mathcal{I}_{F_\lambda}}$ is divisible for every $\lambda \nmid p$.
   ($\mathbb{H}.\mathbf{sEZ}_{/F}$) $H^0(F_\wp, T^*) = 0$ for $\wp \mid p$.

   Let F_∞ denote the cyclotomic $\mathbb{Z}_p$-extension of F, and $\Gamma = \mathrm{Gal}(F_\infty/F)$. Since we assumed p is unramified in $F/\mathbb{Q}$, note that F_∞/F is then totally ramified at all primes $\wp$ over p. Let $F_\wp$ denote the completion of F at $\wp$, and let $F_{\wp,\infty}$ denote the cyclotomic $\mathbb{Z}_p$-extension of $F_\wp$. We may identify $\mathrm{Gal}(F_{\wp,\infty}/F_\wp)$ with Γ for all $\wp | p$ and henceforth Γ will stand for any of these Galois groups. Let $\Lambda = \mathcal{O}[[\Gamma]]$ as usual.

[†]Under the assumptions of Theorem 3.23, we expect $\boldsymbol{\kappa}^{\mathrm{PR}}$ to be also Λ-primitive (just as the cyclotomic unit Kolyvagin system $\boldsymbol{\kappa}^{\rho,\infty}$ in §4.1.1 and Kato's Kolyvagin system $\boldsymbol{\kappa}^{\mathrm{Kato},\infty}$ in §4.1.2 above are, under suitable assumptions), so we in fact expect that $\lambda \in \Lambda^\times$ under the running assumptions.

4.3.1. *Modified Selmer structures on $T \otimes \Lambda$.* In [Büy09a], the author modifies the classical local conditions at p in order to obtain a Selmer structure $\mathcal{F}_\mathcal{L}$ on T (see [Büy09a, §1]). The objective of this section is to lift the Selmer structure $\mathcal{F}_\mathcal{L}$ to a Selmer structure on $T \otimes \Lambda$.

Write $H^1_{\mathrm{Iw}}(F_\wp, T) := \varprojlim_n H^1(F_{\wp,n}, T)$, where $F_{\wp,n}$ denotes the unique subfield of $F_{\wp,\infty}$ which has degree p^n over $F_\wp$. Using Shapiro's Lemma, one may canonically identify $H^i_{\mathrm{Iw}}(F_\wp, T)$ with $H^i(F_\wp, T \otimes \Lambda)$ for all $i \in \mathbb{Z}^+$ (c.f., [MR04, Lemma 5.3.1]). Let

$$H^i_{\mathrm{Iw}}(F_p, T) := \oplus_{\wp|p} H^i_{\mathrm{Iw}}(F_\wp, T) \text{ and } H^i(F_p, T \otimes \Lambda) := \oplus_{\wp|p} H^i(F_\wp, T \otimes \Lambda).$$

As in Appendix A, set $H_K := \mathrm{Gal}(\overline{K}/K_\infty)$ for any local field K. Recall that $T_m = T \otimes \Lambda/(\mathbf{X}^m)$.

Proposition 4.7. *Suppose $\rho(\wp) \neq 1$ for any prime $\wp$ of F above p. Then:*
  (i) *The Λ-module $H^1(F_p, T \otimes \Lambda) = H^1_{\mathrm{Iw}}(F_p, T)$ is free of rank r.*
  (ii) *The map $H^1(F_p, T \otimes \Lambda) \to H^1(F_p, T_m)$ is surjective for every $m \in \mathbb{Z}^+$.*

Proof. Since we assumed $\rho(\wp) \neq 1$ for any $\wp|p$, it follows that $H^0(H_{F_\wp}, T) = 0$, and thus (i) follows from Theorem A.8. By our assumption on ρ, it follows that $H^0(F_\wp, T^*) = 0$, hence, by the proof of Lemma 2.12, also that $H^2(F_\wp, T \otimes \Lambda) = 0$. But

$$\mathrm{coker}\{H^1(F_p, T \otimes \Lambda) \to H^1(F_p, T_m)\} = H^2(F_p, T \otimes \Lambda)[\mathbf{X}^m],$$

hence (ii) follows.   □

We recall the definition of the Selmer structure $\mathcal{F}_\Lambda$ of [MR04, Definition 5.3.2]. We fix a set $\Sigma(\mathcal{F}_\Lambda)$ of places of F which contains all the places above p and infinite places of F, as well as the places at which T is ramified. We then let $H^1_{\mathcal{F}_\Lambda}(F_v, T \otimes \Lambda) = H^1(F_v, T \otimes \Lambda)$ for all $v \in \Sigma(\mathcal{F}_\Lambda)$. By [MR04, Lemma 5.3.1], this definition of $\mathcal{F}_\Lambda$ does not depend on the choice of $\Sigma(\mathcal{F}_\Lambda)$. It also follows from the proofs of Proposition 2.11 and Proposition 2.13 that the propagated Selmer structure $\mathcal{F}_\Lambda$ on the quotients $\{T_m\}$ coincides with $\mathcal{F}_{\mathrm{can}}$, as long as the hypotheses $\mathbb{H}.\mathbf{T}_{/F}$ and $\mathbb{H}.\mathbf{sEZ}_{/F}$ hold for T.

Fix a free, rank one Λ-direct summand $\mathbb{L}_\infty \subset H^1(F_p, T \otimes \Lambda)$. By Proposition 4.7, this also fixes a free, rank one $\Lambda/(\mathbf{X}^m)$-direct summand $\mathcal{L}_m \subset H^1(F_p, T_m)$. When $m = 1$, we denote $\mathcal{L}_1$ simply by $\mathcal{L}$.

Definition 4.8. The $\mathbb{L}_\infty$-*modified Selmer structure* $\mathcal{F}_{\mathbb{L}_\infty}$ on $T \otimes \Lambda$ is given by
  • $\Sigma(\mathcal{F}_{\mathbb{L}_\infty}) = \Sigma(\mathcal{F}_\Lambda)$,
  • $H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(F_v, T \otimes \Lambda) = H^1_{\mathcal{F}_\Lambda}(F_v, T \otimes \Lambda)$, for $v \nmid p$,
  • $H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(F_p, T \otimes \Lambda) = \mathbb{L}_\infty \subset H^1(F_p, T \otimes \Lambda)$.

The induced Selmer structure on the quotients $\mathcal{T}_0 = \{T_{k,m}\}$ will also be denoted by $\mathcal{F}_{\mathbb{L}_\infty}$ (except for the induced Selmer structure on T, which we will denote by $\mathcal{F}_\mathcal{L}$ for the sake of consistency with [Büy09a]). Note that the local conditions on $T_{k,m}$ at the primes $\lambda \nmid p$ determined by $\mathcal{F}_{\mathbb{L}_\infty}$ coincide with the local conditions determined by $\mathcal{F}_\Lambda$, and therefore also by $\mathcal{F}_{\mathrm{can}}$ since $\mathbb{H}.\mathbf{T}_{/F}$ is true.

Proposition 4.9. *Under the assumptions of Proposition 4.7,*
  (i) *the Selmer structure $\mathcal{F}_{\mathbb{L}_\infty}$ is cartesian on $\mathcal{T}_0$ in the sense of Definition 2.5,*
  (ii) *the core Selmer rank $\chi(T, \mathcal{F}_\mathcal{L})$ of the Selmer structure $\mathcal{F}_\mathcal{L}$ on T is one.*

Proof. (ii) is [Büy09a, Proposition 1.8].

Since $\mathcal{F}_{\mathrm{can}}$ and $\mathcal{F}_{\mathbb{L}_\infty}$ determine the same local conditions at $v \nmid p$, the Selmer structure $\mathcal{F}_{\mathbb{L}_\infty}$ is cartesian at $v \nmid p$ by Proposition 2.11. Therefore, it remains to check that $\mathcal{F}_{\mathbb{L}_\infty}$ is cartesian on $\mathcal{T}_0$ at the prime p.

The property **C1** holds by the definition of $\mathcal{F}_{\mathbb{L}_\infty}$ on $\mathcal{T}_0$, and property **C.3** follows easily from [MR04, Lemma 3.7.1] (which applies since $H^1(F_p, T_m)/\mathcal{L}_m$ is a free $\Lambda/(\mathbf{X}^m)$-module for every m).

We now verify **C2**. Let $\mathcal{L}_{k,m}$ be the image of $\mathcal{L}_m$ under the reduction map

$$H^1(F_p, T_m) \longrightarrow H^1(F_p, T_{k,m}).$$

It is easy to see that the $R_{k,m}$-module $\mathcal{L}_{k,m}$ (resp., $H^1(F_p, T_{k,m})/\mathcal{L}_{k,m}$) is free of rank one (resp., of rank $r-1$). We need to check that the map

$$H^1(F_p, T_{k,m})/\mathcal{L}_{k,m} \xrightarrow{[\mathbf{X}^{M-m}]} H^1(F_p, T_{k,M})/\mathcal{L}_{k,M}$$

is injective for all $M \geq m$. But this is evident, since the quotient $H^1(F_p, T_{k,m})/\mathcal{L}_{k,m}$ (resp., $H^1(F_p, T_{k,M})/\mathcal{L}_{k,M}$) is a free $R_{k,m}$-module (resp., a free $R_{k,M}$-module) of rank $r-1$. $\qquad\square$

As a corollary of Proposition 4.9 and a trivial extension of Theorem 3.23 we obtain:

Theorem 4.10. *Under the assumptions of Proposition 4.7,*

    (i) *the Λ-module of Λ-adic Kolyvagin Systems $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$ is free of rank one.*

    (ii) *the map $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P}) \to \overline{\mathbf{KS}}(T, \mathcal{F}_\mathcal{L}, \mathcal{P})$ is surjective.*

Proof. This is exactly Theorem 3.23 with $T = \mathcal{O}(1) \otimes \rho^{-1}$ and the base field $\mathbb{Q}$ replaced by F. The proof of Theorem 3.23 generalizes verbatim to the case when the base field is F, under the running hypotheses. $\qquad\square$

4.3.2. *Rubin-Stark elements and Λ-adic Kolyvagin Systems.* Fix a Λ-line $\mathbb{L}_\infty$ as above. Fix also a finite set S of places of F that does *not* contain any prime above p, but contains all the infinite places S_∞, all primes λ that divide the conductor f_ρ of ρ. Assume that $|S| \geq r+1$ (where we recall that $r = [F : \mathbb{Q}]$). Let

$$\mathcal{K}_0 = \{F_n(\tau) : \tau \text{ is an integral ideal of } F \text{ which is prime to } f_\rho p \, ; \; n \in \mathbb{Z}_{\geq 0}\}$$

and let $\mathcal{K} = \{L \cdot F_n(\tau) : F_n(\tau) \in \mathcal{K}_0\}$. Here, $F_n(\tau) = F_n F(\tau)$, and $F(\tau)$ denotes the maximal pro-p extension of F inside the ray class field of F modulo τ. For each $K \in \mathcal{K}$, let $S_K = S \cup \{\text{places of } F \text{ at which } K \text{ is ramified}\}$ be another set of places of F. Let $O_{K,S_K}^\times$ denote the S_K units of K, and Δ_K (resp., δ_K) denote $\mathrm{Gal}(K/k)$ (resp., $|\mathrm{Gal}(K/k)|$). Conjecture B' of [Rub96] predicts the existence of certain elements

$$\varepsilon_{K,S_K} \in \Lambda_{K,S_K} \subset \frac{1}{\delta_K} \wedge^r O_{K,S_K}^\times \subset \frac{1}{\delta_K} \wedge^r H^1(K, \mathbb{Z}_p(1))$$

where Λ_{K,S_K} is defined as in [Rub96, §2.1], the exterior products are taken in the category of $\mathbb{Z}_p[\Delta_K]$-modules, and the final inclusion is induced by Kummer theory. Throughout this section, we assume the Rubin-Stark conjecture [Rub96, Conjecture B'].

Using elements of $\varprojlim_{K \in \mathcal{K}} \bigwedge^{r-1} \mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K, \mathbb{Z}_p(1)), \mathbb{Z}_p[\Delta_K])$ (or the images of the elements of

$$\varprojlim_{K \in \mathcal{K}} \bigwedge^{r-1} \mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K_p, \mathbb{Z}_p(1)), \mathbb{Z}_p[\Delta_K])$$

under the canonical map

$$\varprojlim_{K \in \mathcal{K}} \bigwedge^{r-1} \mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K_p, \mathbb{Z}_p(1)), \mathbb{Z}_p[\Delta_K]) \longrightarrow \varprojlim_{K \in \mathcal{K}} \bigwedge^{r-1} \mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K, \mathbb{Z}_p(1)), \mathbb{Z}_p[\Delta_K])$$

induced from localization at p) and the Rubin-Stark elements above, Rubin shows [Rub96, §6] (see also [PR98]) how to obtain an Euler system for the G_F-representation $\mathbb{Z}_p(1)$. One may then

obtain an Euler system for $T = \mathcal{O}(1) \otimes \rho^{-1}$ using a standard twisting argument (c.f., [Rub00, §II.4] and [Büy09a, §2.2]).

In [Büy09a], the author explicitly determines a generator for the $\mathcal{O}$-module $\overline{\mathbf{KS}}(T, \mathcal{F}_{\mathcal{L}}, \mathcal{P})$ (which is a free $\mathcal{O}$-module of rank one by [MR04, Theorem 5.2.10]) using an Euler system of Rubin-Stark elements. Let $\boldsymbol{\kappa}^{\text{Stark}} \in \overline{\mathbf{KS}}(T, \mathcal{F}_{\mathcal{L}}, \mathcal{P})$ denote this generator constructed in [Büy09a] and denoted there by $\{\kappa_\eta^{\Phi_0}\}$, where $\Phi_0 = \{\phi_0^{(\tau)}\} \in \varprojlim_\tau \bigwedge^{r-1} \text{Hom}_{\mathcal{O}[\Delta_\tau]}(H^1(F(\tau)_p, T), \mathcal{O}[\Delta_\tau])$ is a distinguished element which plays an important role in loc.cit. Here $\Delta_\tau = \Delta_{F(\tau)}$. See [Büy09a, §2.3-§2.4] for details. We further recall from [Büy09a] that $\kappa_1^{\Phi_0} = \phi_0^{(1)}(\varepsilon_{L,S_L}^\chi)$, where ε_{L,S_L}^ρ is the ρ-part of the Rubin-Stark element ε_{L,S_L}.

Let $\Gamma_n = \text{Gal}(F_n/F)$ and let γ be a fixed generator of Γ. Let $\mathbb{L}_n$ be the image of $\mathbb{L}_\infty$ under the (surjective) homomorphism

$$H^1(F_p, T \otimes \Lambda) \longrightarrow H^1(F_p, T \otimes \Lambda/(\gamma^{p^n} - 1)) \cong H^1(F_{n,p}, T),$$

where the last isomorphism follows from Shapiro's Lemma. Using the arguments of [Büy09a, §2.3], one may choose an element

$$\Phi^\infty = \{\Phi^{(n)}\} \in \varprojlim_n \bigwedge^{r-1} \text{Hom}_{\mathcal{O}[\Gamma_n]}(H^1(F_{n,p}, T), \mathcal{O}[\Gamma_n])$$

with the following properties:

- $\Phi^{(n)}$ maps $\bigwedge^r H^1(F_{n,p}, T)$ isomorphically onto $\mathbb{L}_n$ for all $n \in \mathbb{Z}^+$ (and therefore Φ^∞ maps $\bigwedge^r H^1(F_p, T \otimes \Lambda)$ isomorphically onto $\mathbb{L}_\infty$).
- $\Phi^{(0)} = \phi_0^{(1)}$ in $\bigwedge^{r-1} \text{Hom}_{\mathcal{O}}(H^1(F_p, T), \mathcal{O})$.

Let $L_n = L \cdot F_n$ and let $\varepsilon_{L_n, S_{L_n}}^\rho$ be the ρ-part of the Rubin-Stark element. Set

$$\varepsilon_{F_\infty}^{\text{Stark}} = \{\varepsilon_{L_n, S_{L_n}}^\rho\} \in \varprojlim \bigwedge^r H^1(F_n, T)$$

and $\mathbf{c}_1^{\text{Stark}\infty} = \Phi^\infty(\varepsilon_{F_\infty}^{\text{Stark}}) := \{\Phi^{(n)}(\varepsilon_{L_n, S_{L_n}}^\rho)\}_n \in \varprojlim_n H^1(F_n, T) = H^1(F, T \otimes \Lambda)$. Note that, since $\Phi^{(0)} = \phi_0^{(1)}$ by definition, it follows that

$$\Phi^{(0)}(\varepsilon_{L,S_L}^\rho) = \phi_0^{(1)}(\varepsilon_{L,S_L}^\rho) = \kappa_1^{\Phi_0},$$

i.e., $\kappa_1^{\Phi_0}$ is the image of $\mathbf{c}_1^{\text{Stark}\infty}$ under the projection $H^1(F, T \otimes \Lambda) \to H^1(F, T)$.

Using methods of Perrin-Riou [PR98], one may show that there is a Λ-adic Kolyvagin system $\boldsymbol{\kappa}^{\text{pr},\infty} \in \overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P})$ such that

$$\kappa_1^{\text{pr},\infty} = \mathbf{c}_1^{\text{Stark}\infty} \quad \text{and} \quad \boldsymbol{\kappa}^{\text{pr},\infty} \equiv \boldsymbol{\kappa}^{\text{Stark}} \bmod (\gamma - 1),$$

The trouble is that $\boldsymbol{\kappa}^{\text{pr},\infty}$ does not necessarily belong to $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$.

On the other hand, Theorem 4.10 proves the existence of a Λ-adic Kolyvagin system

$$\boldsymbol{\kappa}^\infty \in \overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$$

such that $\boldsymbol{\kappa}^\infty \equiv \boldsymbol{\kappa}^{\text{Stark}} \bmod (\gamma - 1)$. Let us pause at this point and briefly summarize the situation:

- The Kolyvagin system $\boldsymbol{\kappa}^{\text{pr},\infty}$ is constructed in terms of the Rubin-Stark elements $\varepsilon_{F_\infty}^{\text{Stark}}$, however, $\boldsymbol{\kappa}^{\text{pr},\infty}$ does not necessarily live in $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$, but only in $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\text{can}}, \mathcal{P})$.
- The Kolyvagin system $\boldsymbol{\kappa}^\infty \in \overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$ abstractly lifts the Kolyvagin system $\boldsymbol{\kappa}^{\text{Stark}} \in \overline{\mathbf{KS}}(T, \mathcal{F}_{\mathcal{L}}, \mathcal{P})$ which is constructed in [Büy09a], but it is not a priori related to the Rubin-Stark elements $\varepsilon_{F_\infty}^{\text{Stark}}$.

It requires to extend the methods of [Büy09a] to conclude that there is a Λ-primitive Kolyvagin system $\boldsymbol{\kappa}^{\text{Stark},\infty} \in \overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$ for which $\kappa_1^{\text{Stark},\infty} = \mathbf{c}_1^{\text{Stark}\infty} \in H^1(F, T \otimes \Lambda)$. This is the subject of a forthcoming paper [Büy09b].

We now illustrate how one utilizes $\boldsymbol{\kappa}^\infty \in \overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$ which our Theorem 4.10 proves to exist. We assume Leopoldt's conjecture for every L_n/L until the end of this section. This in particular implies that $H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(F, T \otimes \Lambda)$ injects into $\mathbb{L}_\infty$. We identify $\kappa_1^\infty \in H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(F, T \otimes \Lambda)$ with its image inside $\mathbb{L}_\infty$ under this injection.

For any $\mathcal{O}$-module M, let $M^\vee := \text{Hom}(M, \Phi/\mathcal{O})$ denote its Pontryagin dual.

Proposition 4.11. *The following sequence of Λ-modules is exact:*

$$0 \longrightarrow \frac{H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(F, T \otimes \Lambda)}{\Lambda \cdot \kappa_1^\infty} \longrightarrow \frac{\mathbb{L}_\infty}{\Lambda \cdot \kappa_1^\infty} \longrightarrow H^1_{\mathcal{F}^*_{\text{str}}}(F, (T \otimes \Lambda)^*)^\vee \longrightarrow H^1_{\mathcal{F}^*_{\mathbb{L}_\infty}}(F, (T \otimes \Lambda)^*)^\vee \longrightarrow 0$$

Here $\mathcal{F}_{\text{str}}$ (resp., $\mathcal{F}^*_{\text{str}}$) is the Selmer structure $\mathcal{F}_\Lambda$ (resp., $\mathcal{F}^*_\Lambda$), but local conditions at p are replaced by the strict (resp., relaxed) conditions in the sense of [MR04, Definition 1.1.6] *and Definition 2.4 above.*

Proof. First injection follows from Leopoldt's conjecture, and the rest of the sequence is exact by class field theory (c.f., [Rub00, Theorems I.7.3 and Theorem III.2.10], [dS87, §III.1.7] and [Büy09b, Proposition 2.12]). $\qquad\square$

Since $\boldsymbol{\kappa}^\infty$ maps to $\boldsymbol{\kappa}^{\text{Stark}} \in \overline{\mathbf{KS}}(T, \mathcal{F}_\mathcal{L}, \mathcal{P})$ under the map

$$\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P}) \longrightarrow \overline{\mathbf{KS}}(T, \mathcal{F}_\mathcal{L}, \mathcal{P})$$

by its construction, and since $\boldsymbol{\kappa}^{\text{Stark}}$ is primitive (see the argument following the proof of [Büy09a, Theorem 3.11]), it follows that $\boldsymbol{\kappa}^\infty$ is Λ-primitive. We therefore conclude using [MR04, Theorem 5.3.10] that

$$\text{char}\left(H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(F, T \otimes \Lambda)/\Lambda \cdot \kappa_1^\infty\right) = \text{char}\left(H^1_{\mathcal{F}^*_{\mathbb{L}_\infty}}(F, (T \otimes \Lambda)^*)^\vee\right).$$

This together with Proposition 4.11 gives:

Corollary 4.12. *Suppose $\rho(\wp) \neq 1$ for any prime $\wp$ of F above p. If Leopoldt's conjecture holds for fields L_n (with $n \in \mathbb{Z}_{\geq 0}$), then*

$$\text{char}\left(\mathbb{L}_\infty/\Lambda \cdot \kappa_1^\infty\right) = \text{char}\left((H^1_{\mathcal{F}^*_{\text{str}}}(F, (T \otimes \Lambda)^*)^\vee\right).$$

Remark 4.13. Attentive reader will notice that we do not need to know the existence of Rubin-Stark elements for the proofs of Proposition 4.11 and Corollary 4.12, but only the existence of a Λ-primitive Λ-adic Kolyvagin system $\boldsymbol{\kappa}^\infty$, which we proved above in Theorem 4.10.

Assume that one could choose the Kolyvagin system $\boldsymbol{\kappa}^\infty$ so that $\kappa_1^\infty = \mathbf{c}_1^{\text{Stark}\infty} \in H^1(F, T \otimes \Lambda)$. We prove in [Büy09b] that this in fact is possible.

Since Φ^∞ maps $\bigwedge^r H^1(F_p, T \otimes \Lambda)$ isomorphically onto $\mathbb{L}_\infty$ (and maps the element $\varepsilon_{F_\infty}^{\text{Stark}} \in \bigwedge^r H^1(F_p, T \otimes \Lambda)$ to $\mathbf{c}_1^{\text{Stark}\infty} \in \mathbb{L}_\infty \subset H^1(F_p, T \otimes \Lambda)$), it follows that

$$\bigwedge^r H^1(F_p, T \otimes \Lambda)/\Lambda \cdot \varepsilon_{F_\infty}^{\text{Stark}} \cong \mathbb{L}_\infty/\Lambda \cdot \mathbf{c}_1^{\text{Stark}\infty}.$$

Corollary 4.14. *Assume that the Rubin-Stark element $\varepsilon_{F_\infty}^{\text{Stark}}$ above exists. Then, under the assumptions of Corollary 4.12,*

$$\text{char}\left(\bigwedge^r H^1(F_p, T \otimes \Lambda)/\Lambda \cdot \varepsilon_{F_\infty}^{\text{Stark}}\right) = \text{char}\left(H^1_{\mathcal{F}_{\text{str}}^*}(F, (T \otimes \Lambda)^*)^\vee\right).$$

Using the explicit description of the Galois cohomology groups in question (see [Rub00, §I.6.3]), one may identify $H^1_{\mathcal{F}_{\text{str}}^*}(k, \mathbb{T}^*)^\vee$ with $\text{Gal}(M_\infty/L_\infty)^\rho$, where M_∞ is the maximal abelian p-extension of L_∞ which is unramified outside the primes above p. This is the Iwasawa module which is involved in the formulation of the "main conjectures" in this setting. Let $\mathcal{L}_F^\rho$ denote (an appropriate normalization of) the Deligne-Ribet [DR80] p-adic L-function attached to the character ρ. As a consequence of the work of Wiles [Wil90b], we therefore deduce:

Theorem 4.15. *Under the assumptions of Corollary 4.14,*

$$\mathcal{L}_F^\rho \cdot \Lambda = \text{char}\left(\bigwedge^r H^1(F_p, T \otimes \Lambda)/\Lambda \cdot \varepsilon_{F_\infty}^{\text{Stark}}\right).$$

Remark 4.16. Although Corollary 4.14 relies on the Rubin-Stark conjectures, the existence of the Λ-adic Kolyvagin systems derived from them is unconditional and is proved in Theorem 4.10 above.

Remark 4.17. Theorem 4.15 generalizes (assuming the truth of the Rubin-Stark conjecture) a classical theorem of Iwasawa [Iwa64], which states when $r = 1$ (namely, when $k - \mathbb{Q}$) that the characteristic ideal of the local units modulo the cyclotomic units is generated by the Kubota-Leopoldt p-adic L-function.

APPENDIX A. LOCAL IWASAWA THEORY VIA (φ, Γ)-MODULES

In this Appendix, we give an overview of certain results due to Benois, Colmez, Fontaine, Herr, and Perrin-Riou. We use these results to determine the structure of the semi-local cohomology groups $H^1(k_n(\tau)_p, T)$. This could have been achieved without appealing to the theory of (φ, Γ)-modules, however, the approach via (φ, Γ)-modules adds more perspective to local Iwasawa theory.

Throughout this Appendix, let K denote a finite extension of $\mathbb{Q}_p$ and set $\tilde{K}_n := K(\mu_{p^n})$, $\tilde{K}_\infty := \bigcup_n \tilde{K}_n$. Define the Galois groups $\tilde{H}_K := \text{Gal}(\overline{K}/\tilde{K}_\infty)$ and $\tilde{\Gamma}_K := G_K/\tilde{H}_K = \text{Gal}(\tilde{K}_\infty/K)$. Let $\tilde{\gamma}$ be a topological generator of the pro-cyclic group $\tilde{\Gamma}_K$, and let $\tilde{\Lambda}_K := \mathbb{Z}_p[[\tilde{\Gamma}_K]]$. Let $\tilde{\gamma}_n$ be a fixed topological generator of $\text{Gal}(\tilde{K}_\infty/\tilde{K}_n) := \tilde{\Gamma}^{(n)}$ for $n \in \mathbb{Z}^+$, which is chosen in a way that $\tilde{\gamma}_n = \tilde{\gamma}_1^{p^{\alpha_n}}$, where $\alpha_n \in \mathbb{Z}^+$ is such that $[\tilde{K}_n : \tilde{K}] = p^{\alpha_n}$.

Let K_n be the maximal p-extension of K inside $\tilde{K}_n$, and let $\bigcup_n K_n =: K_\infty \subset \tilde{K}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of K. We set $\Gamma_K := \mathrm{Gal}(K_\infty/K)$ and $\Lambda_K := \mathbb{Z}_p[[\Gamma_K]]$. Note then that

$$\tilde{\Gamma}_K = W \times \Gamma_K, \text{ and that } \tilde{\Lambda}_K = \mathbb{Z}_p[W] \otimes_{\mathbb{Z}_p} \Lambda_K,$$

where W is a finite group whose order is prime to p. (In fact W can be identified by $\mathrm{Gal}(K(\mu_p)/K)$.) Let γ denote the restriction of $\tilde{\gamma}$ to K_∞; so that the element γ is a topological generator of Γ_K. Let γ_n denote the image of $\tilde{\gamma}_n$ under the natural isomorphism

$$\mathrm{Gal}(\tilde{K}_\infty/\tilde{K}_n) \cong \mathrm{Gal}(K_\infty/K_n),$$

and set $H_K := \mathrm{Gal}(\overline{K}/K_\infty)$ (so that $H_K/\tilde{H}_K \cong W$).

In [Fon90], Fontaine[4] introduces the notion of a (φ, Γ)-module over a certain period ring which he denotes by $\mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}}$ (and which is the ring of integers of the field $\widehat{\varepsilon^{\mathrm{nr}}}$). We set $\mathcal{O}_{\varepsilon(K)} := (\mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}})^{H_K}$. We will not include a detailed discussion of these objects here, we refer the reader to [Fon90, A.3.1-3.2] for the definitions and the basic properties of these rings. Briefly, a (φ, Γ)-module over $\mathcal{O}_{\varepsilon(K)}$ is a finitely generated $\mathcal{O}_{\varepsilon(K)}$-module with semi-linear continuous and commuting actions of φ and $\Gamma := \tilde{\Gamma}_K$. A (φ, Γ)-module D over $\mathcal{O}_{\varepsilon(K)}$ is called *étale* if $\varphi(D)$ generates D as an $\mathcal{O}_{\varepsilon(K)}$-module.

Using his theory, Fontaine established an equivalence between the category of $\mathbb{Z}_p$-representations of the absolute Galois group G_K of K, and the category of étale (φ, Γ)-modules over $\mathcal{O}_{\varepsilon(K)}$. This equivalence is given by

$$T \longmapsto D(T) := (\mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}} \otimes_{\mathbb{Z}_p} T)^{H_K}$$
$$(\mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}} \otimes_{\mathcal{O}_{\varepsilon(K)}} D)^{\varphi=1} =: T(D) \longleftarrow D$$

See [Fon90, A.1.2.4-1.2.6] for details.

Suppose T is any $\mathbb{Z}_p[[G_K]]$-module which is free of finite rank over $\mathbb{Z}_p$. In [Her98], Herr makes use of the theory of (φ, Γ)-modules to compute the Galois cohomology groups $H^*(K, T)$. One of the benefits of his approach is that the complex he constructs with cohomology $H^*(K, T)$ is quite explicit. This allows one to compute certain local Galois cohomology groups of p-adic fields. In [Her01], Herr gives a proof of the local Tate duality, where the local pairing (c.f., [Her01, §5]) is explicitly defined in terms of the residues of the differential forms on $\mathcal{O}_{\varepsilon(K)}$. The rest of this Appendix is a survey of Herr's results and their applications [Ben00, CC99] to Iwasawa theory.

In Fontaine's theory of (φ, Γ)-modules, there is an important operator[5]

$$\psi : \mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}} \longrightarrow \mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}},$$
$$\psi(x) := \frac{1}{p}\varphi^{-1}(\mathrm{Tr}_{\widehat{\varepsilon^{\mathrm{nr}}}/\varphi(\widehat{\varepsilon^{\mathrm{nr}}})}(x)),$$

which is crucial for what follows. The map ψ is a left inverse of φ, and its action on $\mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}}$ commutes with the action of G_K. It induces an operator (which we still denote by ψ)

$$\psi : D(T) \longrightarrow D(T)$$

for any G_K-representation T.

Let $C_{\psi, \tilde{\gamma}}$ be the complex

$$C_{\psi, \tilde{\gamma}} : 0 \longrightarrow D(T) \xrightarrow{(\psi-1, \tilde{\gamma}-1)} D(T) \oplus D(T) \xrightarrow{(\tilde{\gamma}-1) \ominus (\psi-1)} D(T) \longrightarrow 0$$

---

[4]However, one should be cautious as Fontaine uses K_n for our $\tilde{K}_n$, etc. For example, his Γ_K is our $\tilde{\Gamma}_K$.

[5]This definition makes sense because:

- $\mathrm{Tr}_{\widehat{\varepsilon^{\mathrm{nr}}}/\varphi(\widehat{\varepsilon^{\mathrm{nr}}})}(\mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}}) \subset p\mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}}$,
- φ is injective.

The main result of [Her98] is the following:

Theorem A.1. *The complex $C_{\psi,\tilde{\gamma}}$ computes the G_K-cohomology of T:*

(i) $H^0(K,T) \cong D(T)^{\psi=1,\tilde{\gamma}=1}$,

(ii) $H^2(K,T) \cong D(T)/(\psi-1,\tilde{\gamma}-1)$,

(iii) *There is an exact sequence*

$$0 \longrightarrow \frac{D(T)^{\psi=1}}{\tilde{\gamma}-1} \longrightarrow H^1(K,T) \longrightarrow \left(\frac{D(T)}{\psi-1}\right)^{\tilde{\gamma}=1} \longrightarrow 0.$$

All the isomorphisms and maps that appear above are functorial in T and K.

Definition A.2. Let

$$H^1_{\tilde{\mathrm{Iw}}}(K,T) := \varprojlim_n H^1(\tilde{K}_n, T) \text{ and,}$$

$$H^1_{\mathrm{Iw}}(K,T) := \varprojlim_n H^1(K_n, T),$$

where the inverse limits are taken with respect to the corestriction maps.

Remark A.3. Since the order of W is prime to p, it follows that

$$H^1_{\mathrm{Iw}}(K,T) \stackrel{\sim}{\longrightarrow} H^1_{\tilde{\mathrm{Iw}}}(K,T)^W$$

by the Hochschild-Serre spectral sequence.

We now determine the structure of $H^1_{\tilde{\mathrm{Iw}}}(K,T)$ using Theorem A.1.

Proposition A.4. *Define $\tau_n := 1 + \tilde{\gamma}_{n-1} + \cdots + \tilde{\gamma}_{n-1}^{p-1} \in \mathbb{Z}_p[[\tilde{\Gamma}_K]]$. There is a commutative diagram with exact rows:*

$$
\begin{array}{ccccccccc}
C_{\psi,\tilde{\gamma}_n}(\tilde{K}_n, T) : 0 & \longrightarrow & D(T) & \longrightarrow & D(T) \oplus D(T) & \longrightarrow & D(T) & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle \tau_n^*} & & \downarrow{\scriptstyle \tau_n} & & \downarrow{\scriptstyle \tau_n \oplus \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} \\
C_{\psi,\tilde{\gamma}_{n-1}}(\tilde{K}_{n-1}, T) : 0 & \longrightarrow & D(T) & \longrightarrow & D(T) \oplus D(T) & \longrightarrow & D(T) & \longrightarrow & 0
\end{array}
$$

Furthermore, the map induced from the morphism τ_n^* on the cohomology of $C_{\psi,\tilde{\gamma}_n}(\tilde{K}_n, T)$ coincides with the corestriction map under Herr's identification $H^*(C_{\psi,\tilde{\gamma}_n}(\tilde{K}_n, T)) \cong H^*(\tilde{K}_n, T)$ of Theorem A.1.

Proof. This follows from the fact that τ_n^* is a cohomological functor and induces $\mathrm{Tr}_{\tilde{K}_n/\tilde{K}_{n-1}}$ on H^0, hence it induces corestrictions on H^i. $\qquad\square$

Using Proposition A.4, one may compute $H^*_{\tilde{\mathrm{Iw}}}(K,T)$:

Theorem A.5.

(i) $H^i_{\tilde{\mathrm{Iw}}}(K,T) = 0$ *if $i \neq 1, 2$,*

(ii) $H^1_{\tilde{\mathrm{Iw}}}(K,T) \stackrel{\sim}{\longrightarrow} D(T)^{\psi=1}$,

(iii) $H^2_{\tilde{\mathrm{Iw}}}(K,T) \stackrel{\sim}{\longrightarrow} D(T)/(\psi-1)$.

See [CC99, §II.3] for a proof of this theorem.

Remark A.6. The isomorphism $\exp^* : H^1_{\tilde{\mathrm{Iw}}}(K,T) \stackrel{\sim}{\longrightarrow} D(T)^{\psi=1}$ of Theorem A.5(ii) can be considered as a vast generalization of Coleman's map [Col79]. The isomorphism $\exp^*$ conjecturally gives rise to the (conjectural) p-adic L-function attached to T. This viewpoint we gain is one of the important benefits of using the theory of (φ, Γ)-modules to compute Galois cohomology.

Let $\mathcal{C}(T) := (\varphi - 1)D(T)^{\psi=1}$. Since ψ is a left inverse of φ, it follows that

$$\ker\{D(T)^{\psi=1} \xrightarrow{\varphi-1} \mathcal{C}(T)\} = D(T)^{\varphi=1},$$

hence we have an exact sequence:

(19) $$0 \longrightarrow D(T)^{\varphi=1} \longrightarrow D(T)^{\psi=1} \xrightarrow{\varphi-1} \mathcal{C}(T) \longrightarrow 0.$$

Using techniques from the theory of (φ, Γ)-modules, one can determine the structure of $\mathcal{C}(T)$:

Proposition A.7. *The $\tilde{\Lambda}_K$-module $\mathcal{C}(T)$ is free of rank $[K : \mathbb{Q}_p] \cdot \mathrm{rank}_{\mathbb{Z}_p}T$.*

One may also check that $D(T)^{\varphi=1} \cong T^{\tilde{H}_K}$. In particular, $D(T)^{\varphi=1}$ is finitely generated over $\mathbb{Z}_p$, hence is a torsion $\mathbb{Z}_p[[\tilde{\Gamma}_K]]$-module. Thus, it follows from Proposition A.7 and Theorem A.5 that $D(T)^{\varphi=1} = H^1_{\mathrm{Iw}}(K, T)_{\mathrm{tors}}$, the torsion submodule of $H^1_{\mathrm{Iw}}(K, T)$.

If we now take the W-invariance of the exact sequence (19) (and use the fact that taking W-invariance is an exact functor) and apply Remark A.3 along with Theorem A.5 and Proposition A.7, we see that:

Theorem A.8.(Perrin-Riou, see [CC99] for the proof we sketch in this Appendix)

(i) *For the Λ_K-torsion submodule $H^1_{\mathrm{Iw}}(K, T)_{\mathrm{tors}}$ of $H^1_{\mathrm{Iw}}(K, T)$, we have $H^1_{\mathrm{Iw}}(K, T)_{\mathrm{tors}} \cong T^{H_K}$.*

(ii) *The Λ_K-module $H^1_{\mathrm{Iw}}(K, T)/H^1_{\mathrm{Iw}}(K, T)_{\mathrm{tors}}$ is free of rank $[K : \mathbb{Q}_p] \cdot \mathrm{rank}_{\mathbb{Z}_p}T$.*

REFERENCES

[Ben00]   Denis Benois. On Iwasawa theory of crystalline representations. *Duke Math. J.*, 104(2):211–267, 2000.

[Büy08]   Kâzım Büyükboduk. Stickelberger elements and Kolyvagin systems, 2008. 36pp., submitted.

[Büy09a] Kâzım Büyükboduk. Kolyvagin systems of Stark units. *J. Reine Angew. Math.*, 631:85–107, 2009.

[Büy09b] Kâzım Büyükboduk. Stark units and the main conjectures for totally real fields. *Compositio Math.*, 145:1163–1195, 2009.

[Büy09c] Kâzım Büyükboduk. Tamagawa defect of Euler systems. *J. Number Theory*, 129(2):402–417, 2009.

[CC99]   Frédéric Cherbonnier and Pierre Colmez. Théorie d'Iwasawa des représentations p-adiques d'un corps local. *J. Amer. Math. Soc.*, 12(1):241–268, 1999.

[Col79]   Robert F. Coleman. Division values in local fields. *Invent. Math.*, 53(2):91–116, 1979.

[Dar95]   Henri Darmon. Thaine's method for circular units and a conjecture of Gross. *Canad. J. Math.*, 47(2):302–317, 1995.

[DR80]   Pierre Deligne and Kenneth A. Ribet. Values of abelian L-functions at negative integers over totally real fields. *Invent. Math.*, 59(3):227–286, 1980.

[dS87]   Ehud de Shalit. *Iwasawa theory of elliptic curves with complex multiplication*, volume 3 of *Perspectives in Mathematics*. Academic Press Inc., Boston, MA, 1987. p-adic L functions.

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

[FPR94]   Jean-Marc Fontaine and Bernadette Perrin-Riou. Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 599–706. Amer. Math. Soc., Providence, RI, 1994.

[Gre04]   Cornelius Greither. Computing Fitting ideals of Iwasawa modules. *Math. Z.*, 246(4):733–767, 2004.

[Her98]   Laurent Herr. Sur la cohomologie galoisienne des corps p-adiques. *Bull. Soc. Math. France*, 126(4):563–600, 1998.

[Her01]   Laurent Herr. Une approche nouvelle de la dualité locale de Tate. *Math. Ann.*, 320(2):307–337, 2001.

[Iwa64]   Kenkichi Iwasawa. On some modules in the theory of cyclotomic fields. *J. Math. Soc. Japan*, 16:42–82, 1964.

[Iwa68]   Kenkichi Iwasawa. On explicit formulas for the norm residue symbol. *J. Math. Soc. Japan*, 20:151–165, 1968.

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

[Kur03]   Masato Kurihara. On the structure of ideal class groups of CM-fields. *Doc. Math.*, J. DMV Extra Vol.:539–563, 2003.

[Maz72] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.

[MR04] Barry Mazur and Karl Rubin. Kolyvagin systems. *Mem. Amer. Math. Soc.*, 168(799):viii+96, 2004.

[MR09] Barry Mazur and Karl Rubin. Refined class number formulas and Kolyvagin systems, 2009. arXiv:0909.3916.

[Och05] Tadashi Ochiai. Euler system for Galois deformations. *Ann. Inst. Fourier (Grenoble)*, 55(1):113–146, 2005.

[PR94a] Bernadette Perrin-Riou. La fonction L p-adique de Kubota-Leopoldt. In *Arithmetic geometry (Tempe, AZ, 1993)*, volume 174 of *Contemp. Math.*, pages 65–93. Amer. Math. Soc., Providence, RI, 1994.

[PR94b] Bernadette Perrin-Riou. Théorie d'Iwasawa des représentations p-adiques sur un corps local. *Invent. Math.*, 115(1):81–161, 1994. With an appendix by Jean-Marc Fontaine.

[PR95] Bernadette Perrin-Riou. Fonctions L p-adiques des représentations p-adiques. *Astérisque*, (229):198, 1995.

[PR98] Bernadette Perrin-Riou. Systèmes d'Euler p-adiques et théorie d'Iwasawa. *Ann. Inst. Fourier (Grenoble)*, 48(5):1231–1307, 1998.

[Rub96] Karl Rubin. A Stark conjecture "over **Z**" for abelian L-functions with multiple zeros. *Ann. Inst. Fourier (Grenoble)*, 46(1):33–62, 1996.

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

[Was82] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

[Wil90a] A. Wiles. On a conjecture of Brumer. *Ann. of Math. (2)*, 131(3):555–565, 1990.

[Wil90b] Andrew Wiles. The Iwasawa conjecture for totally real fields. *Ann. of Math. (2)*, 131(3):493–540, 1990.

LIST OF SYMBOLS

KAZIM BUYUKBODUK
MAX PLANCK INSTITUT FÜR MATHEMATIK,
VIVATSGASSE 7
53111 BONN
GERMANY
E-mail address: kazim@math.stanford.edu
Current address:
Koç University, Mathematics
Rumeli Feneri Yolu
34450 Sarıyer / İstanbul
Turkey