COMPOSITIO MATHEMATICA

Stark units and the main conjectures for totally real fields

Kâzım Büyükboduk

Compositio Math. **145** (2009), 1163–1195.

doi:10.1112/S0010437X09004163

FOUNDATION COMPOSITIO MATHEMATICA

The London Mathematical Society

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press

Compositio Math. 145 (2009) 1163–1195
doi:10.1112/S0010437X09004163

Stark units and the main conjectures for totally real fields

Kâzım Büyükboduk

Abstract

The main theorem of the author's thesis suggests that it should be possible to lift the Kolyvagin systems of Stark units, constructed by the author in an earlier paper, to a Kolyvagin system over the cyclotomic Iwasawa algebra. In this paper, we verify that this is indeed the case. This construction of Kolyvagin systems over the cyclotomic Iwasawa algebra from Stark units provides the first example towards a more systematic study of Kolyvagin system theory over an Iwasawa algebra when the core Selmer rank (in the sense of Mazur and Rubin) is greater than one. As a result of this construction, we reduce the main conjectures of Iwasawa theory for totally real fields to a statement in the context of local Iwasawa theory, assuming the truth of the Rubin–Stark conjecture and Leopoldt's conjecture. This statement in the local Iwasawa theory context turns out to be interesting in its own right, as it suggests a relation between the solutions to p-adic and complex Stark conjectures.

Contents

1. Introduction

This paper is the result of an attempt to understand Kolyvagin system theory (over an Iwasawa algebra) when the core Selmer rank (in the sense of [MR04, Definitions 4.1.8 and 4.1.11]) is greater than one; the work here should be considered as a continuation of our earlier paper [Buy09].

The Kolyvagin system machinery is designed to bound the size of a Selmer group. In all well-known cases, the bounds obtained relate to L-values and thus provide a link between arithmetic and analytic data. Well-known prototypes for such a relation between arithmetic and analytic data are the Birch and Swinnerton-Dyer conjecture (or, more generally, Bloch–Kato conjectures)

Received 5 March 2008, accepted in final form 21 January 2009.
2000 Mathematics Subject Classification 11R23, 11R27, 11R29, 11R42 (primary); 11R34 (secondary).
Keywords: Iwasawa theory, Kolyvagin systems, Stark conjectures.

and the main conjectures of Iwasawa theory. The Kolyvagin system machinery has been successfully applied by many authors to obtain deep results towards proving these conjectures.

In this paper, we construct and study Kolyvagin systems over the cyclotomic Iwasawa algebra (henceforth denoted by Λ). In [Buy07], Kolyvagin systems over Λ were proved to exist in a wide variety of settings, provided that the core Selmer rank is one. Further, Mazur and Rubin [MR04, § 5.3] showed that these Kolyvagin systems can be used to compute the correct size of an appropriately defined Selmer group. However, when the core Selmer rank is greater than one, not much is known.

The most basic example of a situation where the core Selmer rank is greater than one arises when one attempts to utilize the Euler system that would come from the Rubin–Stark elements introduced in [Rub96]. Rubin was the first to study the Euler system of Stark units in [Rub92], where he proved a Gras-type formula for the χ-isotypic component of a certain ideal class group under some assumptions on the character χ (which essentially ensured that the core Selmer rank of the Galois representation $T = \mathbb{Z}_p(1) \otimes \chi^{-1}$, in the sense of [MR04, Definitions 4.1.8 and 4.1.11], is one). These assumptions were removed and a more general Gras-type conjecture proved in [Buy09]. The proof of the main result in [Buy09] relies on the introduction of an auxiliary Selmer structure in a systematic way so as to cut the core Selmer rank down to one. One then obtains a useful collection of Kolyvagin systems for this auxiliary Selmer structure, reducing the problem so that it becomes amenable to the treatment of [MR04].

The principal objective of this article is to generalize the methods of [Buy09] to an Iwasawa-theoretic setting. We first show how to lift the Kolyvagin systems for the auxiliary Selmer structure constructed in [Buy09] to Kolyvagin systems over the cyclotomic Iwasawa algebra. To achieve this, we modify (in § 2) the classical Selmer structure along the cyclotomic tower. The main theorem of [Buy07] implies that there are Kolyvagin systems over Λ for the modified Selmer structure (see also § 2.5 below). In § 3, we show how to obtain these Kolyvagin systems from the *Euler system of Stark units* (which were introduced in [Rub96, § 6]).

This approach of constructing Kolyvagin systems from Euler systems is, of course, standard. Kolyvagin's original descent argument has been systematized by Mazur and Rubin, who constructed in [MR04, Theorem 5.3.3] what they call the *Euler system to Kolyvagin system map*. The problem one faces here is that when the Euler system to Kolyvagin system map is directly applied to the Euler system of Stark units, one obtains, in general, a Kolyvagin system not for the modified Selmer structure but, rather, for a much coarser Selmer structure. This issue is tackled in § 3.3. Once we have obtained the Kolyvagin system for the modified Selmer structure, we can apply the Kolyvagin system machinery of [MR04] to deduce the main results of this paper.

Before stating our main results, we introduce some notation and state the hypotheses that will be in effect throughout the paper.

1.1 Notation and hypotheses

For any field F and a fixed separable closure $\overline{F}$ of F, we write $G_F := \mathrm{Gal}(\overline{F}/F)$ for the Galois group of $\overline{F}/F$.

Fix a totally real number field k and let $r = [k : \mathbb{Q}]$; fix also an algebraic closure $\overline{k}$ of k and a rational odd prime p. Let k_∞ denote the cyclotomic $\mathbb{Z}_p$-extension of k. Let k_n be the unique sub-extension of k_∞/k such that $[k_n : k] = p^n$. Let μ_{p^n} denote the p^nth roots of unity, and let $\mu_{p^\infty} = \varinjlim_n \mu_{p^n}$.

Let $\chi : G_k \to \mathbb{Z}_p^\times$ be a non-trivial *totally even* character of G_k (i.e. it is trivial on all complex conjugations inside G_k) that has finite order, and let L be the fixed field of $\ker(\chi)$ inside $\overline{k}$. Denote the conductor of χ by f_χ, and let Δ be the Galois group $\mathrm{Gal}(L/k)$.

Let S be a finite set of places of k which contains the infinite places but does not contain any prime of k lying above p. Suppose also that $|S| \geqslant r+1$.

For any abelian group A, let $A^\wedge$ denote its p-adic completion; also define A^χ to be the χ-isotypic component of $A^\wedge$.

In this paper T will always stand for the G_k-representation $\mathbb{Z}_p(1) \otimes \chi^{-1}$ (except in the appendix, where T will be an arbitrary $\mathbb{Z}_p[[G_k]]$-module which is free, of finite rank over $\mathbb{Z}_p$, and unramified outside a finite number of places of k).

The following hypotheses will be assumed occasionally (and all of them are required for our main results).

(A1) $p \nmid f_\chi$ (i.e. L/k is unramified at all primes of k above p).

(A2) k is unramified at all primes above p.

(A3) $\chi(\mathrm{Frob}_\wp) \neq 1$ for any prime $\wp$ of k above p, where $\mathrm{Frob}_\wp$ denotes a Frobenius element at $\wp$ inside $\mathrm{Gal}(\overline{k}/k)$.

Hypothesis (A1) was assumed already in [Buy09], although we believe that removing it may be possible (both in [Buy09] and in this paper) via an argument similar to the one used in the proof of Proposition 3.9.

We are almost certain that the results in this paper could be established without (A2) as well. However, this would at least have necessitated fixing a prime $\wp \subset k$ above p to define our auxiliary local conditions (§ 2.2). We decided to avoid making this choice of a prime $\wp$ for the sake of consistency with [Buy09]. In fact, one of the major goals of this paper is to initiate a study of Λ-adic Kolyvagin systems (in the sense of [Buy07]) when the core Selmer rank is strictly greater than one. In view of this, we decided that we would rather assume the extra condition (A2) than lose our liberty in modifying the local conditions at p.

Hypothesis (A3) is, however, a more serious assumption. This is the assumption $\mathbb{H}.\mathbf{sEZ}$ of [Buy07, § 2.2] translated to our setting, and it appears here for exactly the same reason that it appeared in [Buy07]: to avoid the interference of the *exceptional zeros* (in the sense of [Gre94, MTT86]) of the relevant p-adic L-function.

1.2 Statement of the main results

Suppose that the finite set of places S does not contain any non-archimedean prime which splits completely in L/k. Let $\mathbf{c}_{k_\infty}^{\mathrm{stark}} := \{\varepsilon_{k_n}^\chi\}_n$, where $\varepsilon_{k_n}^\chi$ denotes an appropriate twist of the Rubin–Stark element[1] (see §§ 3.1, 3.2 and 4 as well as Remark 4.5 for details). Let M_∞ be the maximal abelian p-extension of L_∞ unramified outside the set of primes lying above p, and set $\mathbb{T} = T \otimes \Lambda$. Let $H^1(k_p, \mathbb{T})$ denote the semi-local cohomology group[2] at p. Finally, for a torsion Λ-module $\mathbb{A}$, let $\mathrm{char}(\mathbb{A})$ denote its characteristic ideal.

[1] The definition of $\varepsilon_{k_n}^\chi$ actually depends on the choice of the set S; however, as long as we assume that S contains no non-archimedean prime which splits completely in L/k, this choice does not affect our main results. That is why we feel free to drop S from our notation.

[2] Let k_n be the unique sub-extension of k_∞/k such that $[k_n : k] = p^n$. Set $L_n = L \cdot k_n$, and let $\mathcal{U}_n^\chi$ denote the local units inside $(L_n \otimes \mathbb{Q}_p)^\chi$. By Kummer theory (see, e.g., [Rub00, § 1.6.C and Proposition 3.2.6] and Lemma 3.4 in this paper) $H^1(k_p, \mathbb{T})$ may be identified with $\varprojlim_n \mathcal{U}_n^\chi$.

Theorem A. *Assume that the hypotheses (A1)–(A3) hold. Fix a finite set* S *as above, and suppose that the Rubin–Stark conjecture [Rub96, Conjecture B′] is true for* S *and for every* $K \in \mathcal{K}$*, where* $\mathcal{K}$ *is the collection of fields defined in § 3. Assume also that Leopoldt's conjecture is true for the number fields* $L_n := L \cdot k_n$, $n \geqslant 0$*. Then*

$$\mathrm{char}(\mathrm{Gal}(M_\infty/L_\infty)^\chi) = \mathrm{char}\bigg(\bigwedge^r H^1(k_p, \mathbb{T})/\Lambda \cdot \mathbf{c}^{\mathrm{stark}}_{k_\infty}\bigg). \tag{1}$$

We remark that when $k = \mathbb{Q}$ (i.e. when $r = 1$), the element $\mathbf{c}^{\mathrm{stark}}_{k_\infty}$ can be obtained from the cyclotomic units. Furthermore, in this case, the ideal on the right-hand side of (1) is generated by a certain Kubota–Leopoldt p-adic L-function. This fact goes back to Iwasawa [Iwa64]. Therefore, when $k = \mathbb{Q}$, Theorem A is equivalent to the main conjecture of Iwasawa theory in the most classical setting.

Let $\mathcal{L}_k^\chi$ denote the Deligne–Ribet p-adic L-function attached to the character χ (see [DR80] for the construction of this p-adic L-function). In light of the main conjectures for totally real fields (proved by Wiles in [Wil90]), Theorem A yields the following result.

Theorem B. *Under the hypotheses of Theorem A,* $\mathrm{char}(\bigwedge^r H^1(k_p, \mathbb{T})/\Lambda \cdot \mathbf{c}^{\mathrm{stark}}_{k_\infty}) \subset \Lambda$ *is generated by* $\mathcal{L}_k^\chi$.

It would be more reasonable to expect a relation such as the one given in Theorem B between the Rubin–Stark elements and the p-adic L-function to exist, rather, between the Deligne–Ribet p-adic L-function and the 'p-adic' Stark elements (which would be solutions to a p-adic Stark conjecture [Sol02, Sol04] instead of the 'complex' Rubin–Stark conjecture). This suggests a link between solutions to the p-adic Stark conjectures and complex Stark conjectures at $s = 0$. We hope to formulate this relation more precisely in a future paper. Motivated by the example above in the $k = \mathbb{Q}$ case, and referring to the work of Perrin-Riou [Per94a, Per95], one might hope to deduce Theorem B directly (i.e. without appealing to the truth of the main conjectures) and also deduce the main conjecture for the totally real field k itself (modulo, of course, the hypotheses of Theorem A).

2. Modified Selmer structures

2.1 Selmer groups for $T = \mathbb{Z}_p(1) \otimes \chi^{-1}$

Throughout this section, we use the notation defined in § 1.1. In addition, set $\Gamma := \mathrm{Gal}(k_\infty/k)$ and let $\Lambda := \mathbb{Z}_p[[\Gamma]]$ be the cyclotomic Iwasawa algebra.

We first recall Mazur and Rubin's definition of a *Selmer structure* and, in particular, the *canonical Selmer structure* on $T \otimes \Lambda$.

2.1.1 *Local conditions.* Let R be a complete local noetherian ring, and let M be a $R[[G_k]]$-module which is free of finite rank over R. We will be interested in the case where R is Λ or certain quotients of it and M is $T \otimes \Lambda$ or its relevant quotients by an ideal of Λ.

For each prime λ of k, a *local condition* $\mathcal{F}$ (at the prime λ) on M is a choice of an R-submodule $H^1_{\mathcal{F}}(k_\lambda, M)$ of $H^1(k_\lambda, M)$. For the prime p, a local condition $\mathcal{F}$ at p will be a choice of an R-submodule $H^1_{\mathcal{F}}(k_p, M)$ of the semi-local cohomology group

$$H^1(k_p, M) := \bigoplus_{\wp | p} H^1(k_\wp, M),$$

where the direct sum is over all the primes of k which lie above p.

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press

For examples of local conditions, see [MR04, Definitions 1.1.6 and 3.2.1].

Suppose that $\mathcal{F}$ is a local condition (at a prime λ of k) on M. If M' is a submodule of M (respectively, if M'' is a quotient module), then $\mathcal{F}$ induces local conditions (which we will still denote by $\mathcal{F}$) on M' (respectively, M'') upon taking $H^1_{\mathcal{F}}(k_\lambda, M')$ (respectively, $H^1_{\mathcal{F}}(k_\lambda, M'')$) to be the inverse image (respectively, the image) of $H^1_{\mathcal{F}}(k_\lambda, M)$ under the natural maps induced from

$$M' \hookrightarrow M \quad \text{and} \quad M \twoheadrightarrow M''.$$

DEFINITION 2.1. The *propagation* of a local condition $\mathcal{F}$ on M to a submodule M' (or a quotient M'') of M is the local condition $\mathcal{F}$ on M' (or on M'') obtained by following the procedure in the paragraph above.

For example, if I is an ideal of R, then a local condition on M induces local conditions on M/IM and $M[I]$ by *propagation*.

DEFINITION 2.2. The *Cartier dual* of M is defined to be the $R[[G_k]]$-module

$$M^* := \mathrm{Hom}(M, \mu_{p^\infty}),$$

where μ_{p^∞} stands for the p-power roots of unity.

Let λ be a prime of k. There is the perfect local Tate pairing

$$\langle \cdot\,, \cdot \rangle_\lambda : H^1(k_\lambda, M) \times H^1(k_\lambda, M^*) \longrightarrow H^2(k_\lambda, \mu_{p^\infty}) \xrightarrow{\sim} \mathbb{Q}_p/\mathbb{Z}_p.$$

2.1.2 *Selmer structures and Selmer groups.* The notation from § 2.1.1 is in effect throughout this subsection. We will also write $\mathcal{D}_\lambda$ for $G_{k_\lambda} := \mathrm{Gal}(\overline{k_\lambda}/k_\lambda)$ whenever we wish to identify the group G_{k_λ} with a closed subgroup of G_k, namely with a particular decomposition group $\mathcal{D}_\lambda \subset G_k$ at λ. We further define $\mathcal{I}_\lambda \subset \mathcal{D}_\lambda$ to be the inertia group and $\mathrm{Frob}_\lambda \in \mathcal{D}_\lambda/\mathcal{I}_\lambda$ to be the arithmetic Frobenius element at λ.

DEFINITION 2.3. A *Selmer structure* $\mathcal{F}$ on M is a collection of the following data:

- a finite set $\Sigma(\mathcal{F})$ of places of k, including all infinite places and primes above p as well as all primes where M is ramified;
- for every $\lambda \in \Sigma(\mathcal{F})$, a local condition (in the sense of § 2.1.1) on M (which we now view as a $R[[\mathcal{D}_\lambda]]$-module), i.e. a choice of an R-submodule

$$H^1_{\mathcal{F}}(k_\lambda, M) \subset H^1(k_\lambda, M).$$

If $\lambda \notin \Sigma(\mathcal{F})$, we will also write $H^1_{\mathcal{F}}(k_\lambda, M) = H^1_{\mathrm{f}}(k_\lambda, M)$, where the module $H^1_{\mathrm{f}}(k_\lambda, M)$ is the *finite* part of $H^1(k_\lambda, M)$, defined as in [MR04, Definition 1.1.6].

DEFINITION 2.4. If $\mathcal{F}$ is a Selmer structure on M, we define the *Selmer module* $H^1_{\mathcal{F}}(k, M)$ to be the kernel of the sum of the restriction maps

$$H^1(\mathrm{Gal}(k_{\Sigma(\mathcal{F})}/k), M) \longrightarrow \bigoplus_{\lambda \in \Sigma(\mathcal{F})} H^1(k_\lambda, M)/H^1_{\mathcal{F}}(k_\lambda, M),$$

where $k_{\Sigma(\mathcal{F})}$ is the maximal extension of k which is unramified outside $\Sigma(\mathcal{F})$.

Example 2.5. In this example we recall [MR04, Definition 5.3.2]. Let $R = \Lambda$ be the cyclotomic Iwasawa algebra, and let $\mathbb{M}$ be a free R-module endowed with a continuous action of G_k which is unramified outside a finite set of places of k. Fix a finite set of places Σ containing all the primes

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press

of k which lie above p, all the places at infinity, and all the primes of k where $\mathbb{M}$ is ramified. We define a Selmer structure $\mathcal{F}_\Lambda$ on $\mathbb{M}$ by setting $\Sigma(\mathcal{F}_\Lambda)=\Sigma$ and $H^1_{\mathcal{F}_\Lambda}(k_\lambda,\mathbb{M})=H^1(k_\lambda,\mathbb{M})$ for $\lambda\in\Sigma(\mathcal{F}_\Lambda)$. This is what we call the *canonical Selmer structure* on $\mathbb{M}$. As remarked in [MR04, Definition 5.3.2], this definition is independent of the choice of Σ.

As in Definition 2.1, the induced Selmer structure on the quotients $\mathbb{M}/I\mathbb{M}$ will still be denoted by $\mathcal{F}_\Lambda$. Note that $H^1_{\mathcal{F}_\Lambda}(k_\lambda,\mathbb{M}/I\mathbb{M})$ will not usually be the same as $H^1(k_\lambda,\mathbb{M}/I\mathbb{M})$.

Remark 2.6. When $R=\Lambda$ and $\mathbb{M}=T\otimes\Lambda$ with $T=\mathbb{Z}_p(1)\otimes\chi^{-1}$, we shall see in § 2.5 that the Selmer structure $\mathcal{F}_{\text{can}}$ of [Buy07, § 2.1] on the quotients $T\otimes\Lambda/(f)$ may be identified, under hypothesis (A3) on χ, with the propagation of $\mathcal{F}_\Lambda$ to the quotients $T\otimes\Lambda/(f)$, for every distinguished polynomial f inside Λ.

Definition 2.7. A *Selmer triple* is a triple $(M,\mathcal{F},\mathcal{P})$ where $\mathcal{F}$ is a Selmer structure on M and $\mathcal{P}$ is a set of rational primes that is disjoint from $\Sigma(\mathcal{F})$.

Remark 2.8. Although, thanks to Kummer theory, one could identify the cohomology groups in our setting (when the Galois module in question is $T\otimes\Lambda$ with $T=\mathbb{Z}_p(1)\otimes\chi^{-1}$ or its quotients by certain ideals of Λ) with certain groups of units, we shall insist on using the cohomological language for the sake of notational consistency with [MR04], from which we borrow the main technical results. This way, we also hope that it will be easier to hypothesize our approach for potential generalizations to other settings.

2.2 Modifying the local conditions at p

In [Buy09, § 1], the classical local conditions at the primes above p are modified to obtain a Selmer structure $\mathcal{F}_\mathcal{L}$ on T. The objective of this section is to lift the Selmer structure $\mathcal{F}_\mathcal{L}$ on T to a Selmer structure on $T\otimes\Lambda$.

In this section, we will make use of the results from Appendix A to determine the structure of the semi-local cohomology group $H^1(k_p,T\otimes\Lambda)$ as a Λ-module. Although there may be a more direct way (in this particular setting where $T=\mathbb{Z}_p(1)\otimes\chi^{-1}$) of obtaining these results on the structure of $H^1(k_p,T\otimes\Lambda)$ without appealing to the description of the Galois cohomology groups in terms of (φ,Γ)-modules, we believe that the more general approach via Fontaine's theory of (φ,Γ)-modules might allow our strategy to be applied in many other settings.

Recall that k_∞ denotes the cyclotomic $\mathbb{Z}_p$-extension of k and that $\Gamma=\mathrm{Gal}(k_\infty/k)$. Assume that the hypotheses (A1)–(A3) hold until the end of § 2.2. Hypothesis (A2) implies that the extension k_∞/k is totally ramified at all primes $\wp\subset k$ over p. Let $k_\wp$ denote the completion of k at $\wp$, and let $k_{\wp,\infty}$ denote the cyclotomic $\mathbb{Z}_p$-extension of $k_\wp$. We may therefore identify $\mathrm{Gal}(k_{\wp,\infty}/k_\wp)$ with Γ for all $\wp|p$, so henceforth Γ will stand for any of these Galois groups. Let $\Lambda=\mathbb{Z}_p[[\Gamma]]$ be the cyclotomic Iwasawa algebra, as usual. We also fix a topological generator γ of Γ and set $\mathbf{X}=\gamma-1$ (and we occasionally identify Λ with the power series ring $\mathbb{Z}_p[[\mathbf{X}]]$).

Following the notation of Appendix A, write

$$H^1_{\mathrm{Iw}}(k_\wp,T):=\varprojlim_n H^1(k_{\wp,n},T),$$

where $k_{\wp,n}$ denotes the unique subfield of $k_{\wp,\infty}$ which has degree p^n over $k_\wp$. By Shapiro's lemma, one may canonically identify $H^i_{\mathrm{Iw}}(k_\wp,T)$ with $H^i(k_\wp,T\otimes\Lambda)$ (see [Col98, Proposition II.1.1]) for all $i\in\mathbb{Z}^+$. Define

$$H^i_{\mathrm{Iw}}(k_p,T):=\bigoplus_{\wp|p}H^i_{\mathrm{Iw}}(k_\wp,T)\quad\text{and}\quad H^i(k_p,T\otimes\Lambda):=\bigoplus_{\wp|p}H^i(k_\wp,T\otimes\Lambda)$$

(these two Λ-modules are canonically isomorphic by the argument above).

Set $H_K := \mathrm{Gal}(\overline{K}/K_\infty)$ for any local field K. Also define $T_m := T \otimes \Lambda/(\mathbf{X}^m)$ and $T_{s,m} := T \otimes \Lambda/(p^s, \mathbf{X}^m)$ for $s, m \in \mathbb{Z}^+$, following the notation of [Buy07, § 2.3.2].

Proposition 2.9.

(i) *$H^1(k_p, T \otimes \Lambda) = H^1_{\mathrm{Iw}}(k_p, T)$ is a free Λ-module of rank r.*

(ii) *The map $H^1(k_p, T \otimes \Lambda) \to H^1(k_p, T_m)$ is surjective for all $m \in \mathbb{Z}^+$.*

Proof. For every $\wp \subset k$ above p, it follows from hypothesis (A3) that $T^{H_{k_\wp}} = 0$, and thus (i) is immediate from Theorem A.8. It also follows that $(T^*)^{G_{k_\wp}} = 0$, again thanks to (A3); hence the proof of [Buy07, Lemma 2.11] shows that $H^2(k_\wp, T \otimes \Lambda) = 0$. But then

$$\mathrm{coker}\{H^1(k_p, T \otimes \Lambda) \longrightarrow H^1(k_p, T_m)\} = \bigoplus_{\wp | p} H^2(k_\wp, T \otimes \Lambda)[\mathbf{X}^m] = 0,$$

and (ii) follows. □

Fix a free Λ-direct summand $\mathbb{L}_\infty$ inside of $H^1(k_p, T \otimes \Lambda)$ which is free of rank one as a Λ-module. By Proposition 2.9, this also fixes a free $\Lambda/(\mathbf{X}^m)$-direct summand $\mathbb{L}_m$ of $H^1(k_p, T_m)$ which is free of rank one (as a $\Lambda/(\mathbf{X}^m)$-module). When $m = 1$, we denote $\mathbb{L}_1$ by $\mathcal{L}$.

Definition 2.10. Let $\mathbb{L}_\infty$ be as above. We define the $\mathbb{L}_\infty$-*modified Selmer structure* $\mathcal{F}_{\mathbb{L}_\infty}$ on $T \otimes \Lambda$ as follows:

- $\Sigma(\mathcal{F}_{\mathbb{L}_\infty}) = \Sigma(\mathcal{F}_\Lambda)$;
- $H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k_p, T \otimes \Lambda) = \mathbb{L}_\infty \subset H^1(k_p, T \otimes \mathbb{L}_\infty)$;
- $H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k_\lambda, T \otimes \Lambda) = H^1_{\mathcal{F}_\Lambda}(k_\lambda, T \otimes \Lambda)$ for $\lambda \nmid p$.

The induced Selmer structure on the collection of quotients $\mathcal{T}_0 := \{T_{s,m}\}$ will also be denoted by $\mathcal{F}_{\mathbb{L}_\infty}$ (except for the induced Selmer structure on $T_1 = T \otimes \Lambda/(\mathbf{X}) = T$ and its quotients $T_{s,1} = T \otimes \Lambda/(p^s, \mathbf{X}) = T/p^sT$, which will be denoted by $\mathcal{F}_\mathcal{L}$ for notational consistency with [Buy09]).

2.3 Local duality and the dual Selmer structure

We will discuss local duality in great generality. Let R be a complete local noetherian ring and let M be a free R-module of finite rank which is endowed with a continuous action of G_k. Let $M^* = \mathrm{Hom}(M, \mu_{p^\infty})$ be the Cartier dual of M. For each prime λ of k, there is a perfect pairing

$$\langle \cdot\, , \cdot \rangle_\lambda : H^1(k_\lambda, M) \times H^1(k_\lambda, M^*) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p,$$

called the local Tate pairing.

Let $\mathcal{F}$ be a Selmer structure on M. For each prime λ of k, define $H^1_{\mathcal{F}^*}(k_\lambda, M^*) := H^1_{\mathcal{F}}(k_\lambda, M)^\perp$ as the orthogonal complement of $H^1_{\mathcal{F}}(k_\lambda, M)$ under the local Tate pairing. The Selmer structure $\mathcal{F}^*$ on M^* defined in this way will be called the *dual Selmer structure*.

As in Definition 2.4, the dual Selmer structure gives rise to the *dual Selmer module*

$$H^1_{\mathcal{F}^*}(k, M^*) := \ker\left\{ H^1(\mathrm{Gal}(k_{\Sigma(\mathcal{F})}/k), M^*) \longrightarrow \bigoplus_{\lambda \in \Sigma(\mathcal{F})} \frac{H^1(k_\lambda, M^*)}{H^1_{\mathcal{F}^*}(k_\lambda, M^*)} \right\}.$$

2.4 Comparison of Selmer modules

As our sights are set on Iwasawa's main conjecture over totally real number fields, we now construct the *correct* Iwasawa module: a Selmer module which should relate to the appropriate p-adic L-function (which, in our setting, is the Deligne–Ribet p-adic L-function; see [DR80] for its construction).

Once this Selmer module is defined, we will use Poitou–Tate global duality to compare it to $H^1_{\mathcal{F}^*_{\mathbb{L}_\infty}}(k,(T\otimes\Lambda)^*)$, the dual Selmer module attached to the dual $\mathbb{L}_\infty$-modified Selmer structure.

Definition 2.11. The *p-strict Selmer structure* $\mathcal{F}_{\mathrm{str}}$ on $T\otimes\Lambda$ is defined by the following data:

- $\Sigma(\mathcal{F}_{\mathrm{str}})=\Sigma(\mathcal{F}_\Lambda)$;
- $H^1_{\mathcal{F}_{\mathrm{str}}}(k_p,T\otimes\Lambda)=0$;
- $H^1_{\mathcal{F}_{\mathrm{str}}}(k_\lambda,T\otimes\Lambda)=H^1_{\mathcal{F}_\Lambda}(k_\lambda,T\otimes\Lambda)=H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k_\lambda,T\otimes\Lambda)$ for $\lambda\nmid p$.

Hence, for the dual Selmer structure $\mathcal{F}^*_{\mathrm{str}}$ (in the sense of § 2.3) we have:

- $H^1_{\mathcal{F}^*_{\mathrm{str}}}(k_p,(T\otimes\Lambda)^*)=H^1(k_p,(T\otimes\Lambda)^*)$;
- $H^1_{\mathcal{F}^*_{\mathrm{str}}}(k_\lambda,(T\otimes\Lambda)^*)=H^1_{\mathcal{F}^*_{\mathbb{L}_\infty}}(k_\lambda,(T\otimes\Lambda)^*)$ for $\lambda\nmid p$.

For any $\mathbb{Z}_p$-module A, let $A^\vee:=\mathrm{Hom}(A,\mathbb{Q}_p/\mathbb{Z}_p)$ denote its Pontryagin dual.

Later, in § 4, we will explain why $H^1_{\mathcal{F}^*_{\mathrm{str}}}(k_p,(T\otimes\Lambda)^*)^\vee$ is the *correct* Iwasawa module in this setting which relates[3] to the Deligne–Ribet p-adic L-function.

Proposition 2.12. *Assume that Leopoldt's conjecture holds. Then there is an exact sequence*

$$0\longrightarrow H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k,T\otimes\Lambda)\xrightarrow{\mathrm{loc}_p}\mathbb{L}_\infty\longrightarrow H^1_{\mathcal{F}^*_{\mathrm{str}}}(k,(T\otimes\Lambda)^*)^\vee\longrightarrow H^1_{\mathcal{F}^*_{\mathbb{L}_\infty}}(k,(T\otimes\Lambda)^*)^\vee\longrightarrow 0.$$

Proof. We allow ourselves to be sketchy in this proof, since similar versions of this proposition can be found in the literature (see, e.g., [Rub00, Theorem I.7.3 and III.2.10] or [deS87, § III.1.7]).

Set $\gamma_n=\gamma^{p^n}$ for $n\in\mathbb{Z}_{\geqslant 0}$, and let $\mathcal{L}_n\subset H^1(k_p,T\otimes\Lambda/(\gamma_n-1))$ be the image of $\mathbb{L}_\infty$ under the surjective map

$$H^1(k_p,T\otimes\Lambda)\longrightarrow H^1(k_p,T\otimes\Lambda/(\gamma_n-1)).$$

Let $\mathcal{F}_{\mathcal{L}_n}$ denote the Selmer structure on $T\otimes\Lambda/(\gamma_n-1)$, which is obtained by propagating the Selmer structure $\mathcal{F}_{\mathbb{L}_\infty}$ on $T\otimes\Lambda$ to its quotient $T\otimes\Lambda/(\gamma_n-1)$. The propagated Selmer structure from $\mathcal{F}_{\mathrm{str}}$ on $T\otimes\Lambda$ (defined in Definition 2.11) to the quotient $T\otimes\Lambda/(\gamma_n-1)$ will still be denoted by $\mathcal{F}_{\mathrm{str}}$.

By Shapiro's lemma, one may canonically identify $H^1(k,T\otimes\Lambda/(\gamma_n-1))$ with $H^1(k_n,T)$ and, for every prime $\lambda\subset k$, $H^1(k_\lambda,T\otimes\Lambda/(\gamma_n-1))$ with $H^1((k_n)_\lambda,T)$; see [Rub00, §§ B.4 and B.5]. In this way, we can view $\mathcal{F}_{\mathcal{L}_n}$ and $\mathcal{F}_{\mathrm{str}}$ as Selmer structures on the G_{k_n}-representation T.

It is easy to see that one then has the following exact sequences:

$$0\longrightarrow H^1_{\mathcal{F}_{\mathrm{str}}}(k_n,T)\longrightarrow H^1_{\mathcal{F}_{\mathcal{L}_n}}(k_n,T)\xrightarrow{\mathrm{loc}_p}\mathcal{L}_n, \tag{2}$$

$$0\longrightarrow H^1_{\mathcal{F}^*_{\mathcal{L}_n}}(k_n,T^*)\longrightarrow H^1_{\mathcal{F}^*_{\mathrm{str}}}(k_n,T^*)\xrightarrow{\mathrm{loc}_p^*}\frac{H^1_{\mathcal{F}^*_{\mathrm{str}}}((k_n)_p,T^*)}{H^1_{\mathcal{F}^*_{\mathcal{L}_n}}((k_n)_p,T^*)}.$$

[3] Wiles [Wil90] has already proved this relation using techniques that are different from ours. He systematically made use of Hida's theory of Λ-adic Hilbert modular forms to construct certain unramified extensions, from which he deduced the main conjectures.

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press

Since we assume the truth of Leopoldt's conjecture, [Buy09, Proposition 1.4] (applied with the totally real field k_n instead of k) and Kummer theory give:

(i) $H^1(k_n, T) = (L_n^\times)^\chi$ and $H^1((k_n)_p, T) = (L_n \otimes \mathbb{Q}_p)^{\times,\chi} \supset \mathcal{L}_n$;

(ii) $H^1_{\mathcal{F}_{\mathcal{L}_n}}(k_n, T) = (\mathcal{O}_{L_n}^\times)^\chi \cap \mathcal{L}_n \subset \mathcal{L}_n$;

(iii) $H^1_{\mathcal{F}_{\mathrm{str}}}(k_n, T) = \ker(H^1_{\mathcal{F}_{\mathcal{L}_n}}(k_n, T) \to \mathcal{L}_n) = 0$.

Here $\mathcal{O}_{L_n}^\times$ stands for the ring of integers of the number field L_n. Thanks to Leopoldt's conjecture, we may identify $(\mathcal{O}_{L_n}^\times)^\chi$ with its isomorphic image under the localization map at p, and the intersection in (ii) above is taken inside $(L_n \otimes \mathbb{Q}_p)^{\times,\chi}$ after this identification.

The first exact sequence of (2) can therefore be rewritten as

$$0 \longrightarrow H^1_{\mathcal{F}_{\mathcal{L}_n}}(k_n, T) \xrightarrow{\mathrm{loc}_p} \mathcal{L}_n.$$

Furthermore, the Poitou–Tate global duality theorem [Mil86, I.4.10] says that $\mathrm{im}(\mathrm{loc}_p) = \mathrm{im}(\mathrm{loc}_p^*)^\perp$ with respect to the local Tate pairing. This, in turn, translates the above diagram into the following exact sequence (see the proof of [Rub00, Theorem I.7.3] for details):

$$0 \longrightarrow H^1_{\mathcal{F}_{\mathcal{L}_n}}(k_n, T) \xrightarrow{\mathrm{loc}_p} \mathcal{L}_n \longrightarrow H^1_{\mathcal{F}^*_{\mathrm{str}}}(k_n, T^*)^\vee \longrightarrow H^1_{\mathcal{F}^*_{\mathcal{L}_n}}(k_n, T^*)^\vee \longrightarrow 0. \tag{3}$$

Now, by passing to the inverse limit with respect to n in (3) (which, owing to [Rub00, Proposition B.1.1], can be done without harming the exactness), we obtain the exact sequence that we seek. □

Suppose that $c \in H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k, T \otimes \Lambda)$ is any class.

COROLLARY 2.13. *Under the hypotheses of Proposition 2.12, the following sequence is exact:*

$$\begin{aligned} 0 \longrightarrow H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k, T \otimes \Lambda)/\Lambda \cdot c &\xrightarrow{\mathrm{loc}_p} \mathbb{L}_\infty/\Lambda \cdot c \\ &\longrightarrow H^1_{\mathcal{F}^*_{\mathrm{str}}}(k, (T \otimes \Lambda)^*)^\vee \longrightarrow H^1_{\mathcal{F}^*_{\mathbb{L}_\infty}}(k, (T \otimes \Lambda)^*)^\vee \longrightarrow 0. \end{aligned}$$

2.5 Kolyvagin systems for the $\mathbb{L}_\infty$-modified Selmer triple: I

From this section on, we shall concentrate on the particular G_k-representations $T = \mathbb{Z}_p(1) \otimes \chi^{-1}$ and $\mathbb{T} = T \otimes \Lambda$, with χ as in § 1.1. Throughout § 2.5, we assume (A1)–(A3).

Remark 2.14. Consider the following properties (which play a role also in [Buy07, MR04]).

(H1) The residual $\mathbb{F}_p[[G_k]]$-representation T/pT is absolutely irreducible.

(H2) There is a $\tau \in G_k$ such that $\tau = 1$ on μ_{p^∞} and $T/(\tau - 1)T$ is free of rank one over $\mathbb{Z}_p$.

(H3) $H^0(k, T/pT) = H^0(k, T^*[p]) = 0$.

(H4) Either (H4a) $\mathrm{Hom}_{\mathbb{F}_p[[G_k]]}(T/pT, T^*[p]) = 0$ or (H4b) $p > 4$.

Before we explain why $T = \mathbb{Z}_p(1) \otimes \chi^{-1}$ has these properties, let us point out that hypothesis (H3) above is implied by the (**H.3**) of Mazur and Rubin [MR04, § 3.5] (cf. [MR04, Lemma 3.5.2]). However, the weaker hypothesis (H3) is sufficient for our purposes.

Hypothesis (H1) holds because T/pT is one-dimensional (as an $\mathbb{F}_p$-vector space). Hypothesis (H2) holds with $\tau = \mathrm{id} \in G_k$, and (H3) holds since we assumed that χ is non-trivial. Finally, it is easy to see that (H4a) holds.

Observe further that the following versions of the hypotheses ($\mathbb{H}.\mathbf{T}$) and ($\mathbb{H}.\mathbf{sEZ}$) from [Buy07, § 2.2] hold for T as well.

($\mathbb{H}.\mathbf{T}_{/k}$) $(T \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\mathcal{I}_\lambda}$ is divisible for every prime $\lambda \nmid p$, $\lambda \subset k$.

($\mathbb{H}.\mathbf{sEZ}_{/k}$) $(T^*)^{G_{k_\wp}} = 0$ for primes $\wp | p$.

Note that ($\mathbb{H}.\mathbf{sEZ}_{/k}$) is implied by assumption (A3).

Next, we define the Selmer structure $\mathcal{F}_{\text{can}}$ on certain quotients of $T \otimes \Lambda$, following [Buy07, Definition 2.2].

Definition 2.15. Suppose that $f \in \Lambda$ is any *distinguished* polynomial, in the sense that the quotient $\Lambda/(f)$ is a free $\mathbb{Z}_p$-module of finite rank. Let $\mathcal{F}_{\text{can}}$ be the Selmer structure on $T_f := T \otimes \Lambda/(f)$ such that:

- $\Sigma(\mathcal{F}_{\text{can}}) = \Sigma(\mathcal{F}_\Lambda)$;
- the local conditions are given by

$$H^1_{\mathcal{F}_{\text{can}}}(k_\lambda, T_f) = \begin{cases} H^1(k_\lambda, T_f) & \text{if } \lambda | p, \\ H^1_{\text{f}}(k_\lambda, T_f) & \text{if } \lambda \in \Sigma(\mathcal{F}_{\text{can}}) \text{ and } \lambda \nmid p, \end{cases}$$

with

$$H^1_{\text{f}}(k_\lambda, T_f) = \ker\{H^1(k_\lambda, T_f) \longrightarrow H^1(k_\lambda^{\text{unr}}, T_f \otimes \mathbb{Q}_p)\}$$

where k_λ^{unr} is the maximal unramified extension of k_λ.

The induced Selmer structure on the quotients $T \otimes \Lambda/(p^s, f)$, which is obtained by propagating $\mathcal{F}_{\text{can}}$ (in the sense of Definition 2.1), will also be denoted by $\mathcal{F}_{\text{can}}$.

Recall the definition of the collection $\mathcal{T}_0 = \{T_{s,m}\}_{s,m}$.

Remark 2.16. By the definition of $\mathcal{F}_{\mathbb{L}_\infty}$, the local conditions on $T_{s,m}$ at primes $\lambda \nmid p$ determined by $\mathcal{F}_{\mathbb{L}_\infty}$ coincide with the local conditions determined by $\mathcal{F}_\Lambda$; and, thanks to [Buy07, Corollary 2.8 and 2.9], they also coincide with the local conditions determined by $\mathcal{F}_{\text{can}}$, since ($\mathbb{H}.\mathbf{T}_{/k}$) holds. Indeed, it was proved in [Buy07] that all of these local conditions coincide with

$$H^1_{\text{unr}}(k_\lambda, T_{s,m}) := \ker\{H^1(k_\lambda, T_{s,m}) \longrightarrow H^1(k_\lambda^{\text{unr}}, T_{s,m})\},$$

as long as hypothesis ($\mathbb{H}.\mathbf{T}_{/k}$) holds.

Recall that the rank-one $\mathbb{Z}_p$-direct summand $\mathcal{L}$ of $H^1(k_p, T)$ is defined to be the image of $\mathbb{L}_\infty$ under the canonical (surjective) map

$$H^1(k_p, T \otimes \Lambda) \longrightarrow H^1(k_p, T).$$

Let $\mathcal{F}_\mathcal{L}$ denote the Selmer structure on T which is obtained by propagating the Selmer structure $\mathcal{F}_{\mathbb{L}_\infty}$. This agrees with the definition of $\mathcal{F}_\mathcal{L}$ in [Buy09, § 1.1].

PROPOSITION 2.17.

(i) *The Selmer structure* $\mathcal{F}_{\mathbb{L}_\infty}$ *is cartesian on* $\mathcal{T}_0$ *in the sense of [Buy07, Definition 2.4].*

(ii) *The core Selmer rank* $\mathcal{X}(T, \mathcal{F}_{\mathcal{L}})$ *(in the sense of [MR04, Definition 4.1.11]) of the Selmer structure* $\mathcal{F}_{\mathcal{L}}$ *on* T *is one.*

Proof. Assertion (ii) is [Buy09, Proposition 1.8].

As pointed out in Remark 2.16, the Selmer structures $\mathcal{F}_{\text{can}}$ and $\mathcal{F}_{\mathbb{L}_\infty}$ determine the same local conditions on the quotients $T_{s,m}$ at every place $v \nmid p$. Hence, the local conditions determined by $\mathcal{F}_{\mathbb{L}_\infty}$ are cartesian at $v \nmid p$, by [Buy07, Proposition 2.10]. It therefore suffices to check that $\mathcal{F}_{\mathbb{L}_\infty}$ is cartesian on $\mathcal{T}_0$ at p, i.e. we need to verify properties (**C.1**)–(**C.3**) in [Buy07, Definition 2.4] for the local conditions at p, determined by $\mathcal{F}_{\mathbb{L}_\infty}$ on the collection $\mathcal{T}_0 = \{T_{s,m}\}$. These properties are as follows.

(**C.1**) For positive integers $s \leqslant s'$ and $m \leqslant m'$, the module $H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k_p, T_{s,m})$ is the image of the module $H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k_p, T_{s',m'})$ under the canonical map

$$H^1(k_p, T_{s',m'}) \longrightarrow H^1(k_p, T_{s,m}).$$

(**C.2**) For positive integers s, m and α, the module $H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k_p, T_{s,m})$ is the inverse image of the module $H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k_p, T_{s,m+\alpha})$ under the natural map

$$H^1(k_p, T_{s,m}) \longrightarrow H^1(k_p, T_{s,m+\alpha})$$

which is induced from the injection $T_{s,m} \xrightarrow{[\mathbf{X}^\alpha]} T_{s,m+\alpha}$, where $[\mathbf{X}^\alpha]$ stands for the multiplication-by-$\mathbf{X}^\alpha$ map.

(**C.3**) For positive integers s, m and α, the module $H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k_p, T_{s,m})$ is the inverse image of the module $H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k_p, T_{s+\alpha,m})$ under the natural map

$$H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k_p, T_{s,m}) \longrightarrow H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k_p, T_{s+\alpha,m})$$

which is induced from the injection $T_{s,m} \xrightarrow{[p^\alpha]} T_{s+\alpha,f}$, where $[p^\alpha]$ is the multiplication-by-p^α map.

Property (**C.1**) 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 the line $\mathbb{L}_m \subset H^1(k_p, T_m)$ is a direct summand of $H^1(k_p, T_m)$, i.e. the $\Lambda/(\mathbf{X}^m)$-module $H^1(k_p, T_m)/\mathbb{L}_m$ is free, for any $m \in \mathbb{Z}^+$).

We now verify (**C.2**). For $s \in \mathbb{Z}^+$, let $\mathbb{L}_{s,m}$ be the image of $\mathbb{L}_m$ under the reduction map

$$H^1(k_p, T_m) \longrightarrow H^1(k_p, T_{s,m}).$$

It is easy to see that $\mathbb{L}_{s,m}$ (respectively, $H^1(k_p, T_{s,m})/\mathbb{L}_{s,m}$) is a free $\mathbb{L}/(p^s, \mathbf{X}^m)$-module of rank one (respectively, of rank $[k : \mathbb{Q}] - 1$). To complete the proof, we need to check that the map

$$H^1(k_p, T_{s,m})/\mathbb{L}_{s,m} \xrightarrow{[\mathbf{X}^{M-m}]} H^1(k_p, T_{s,M})/\mathbb{L}_{s,M}$$

induced from the map

$$[\mathbf{X}^{M-m}] : \Lambda/(\mathbf{X}^m) \longrightarrow \Lambda/(\mathbf{X}^M)$$

is injective for all $M \geqslant m$. But this is evident, since $H^1(k_p, T_{s,m})/\mathbb{L}_{s,m}$ (respectively, $H^1(k_p, T_{s,M})/\mathbb{L}_{s,M}$) is a free $\Lambda/(p^s, \mathbf{X}^m)$-module (respectively, a free $\Lambda/(p^s, \mathbf{X}^M)$-module) of rank $[k : \mathbb{Q}] - 1$. □

Let $\mathcal{P}$ denote the set of primes of k whose elements do not divide pf_χ. For positive integers s and m, define

$$\mathcal{P}_{s+m} := \{\mathfrak{q} \in \mathcal{P} \mid \mathfrak{q} \text{ splits completely in } L(\mu_{p^{s+m+1}})/k\}.$$

Note that the set $\mathcal{P}_j$ is exactly the set of primes which are determined by [MR04, Definition 3.1.6] or [Rub00, Definition IV.1.1], in the particular case where $T = \mathbb{Z}_p(1) \otimes \chi^{-1}$. Let $\mathcal{N}$ (respectively, $\mathcal{N}_j$) denote the set of square-free products of primes $\mathfrak{q}$ in $\mathcal{P}$ (respectively, in $\mathcal{P}_j$), with the convention that $1 \in \mathcal{N}_j \subset \mathcal{N}$.

Definition 2.18 (cf. [MR04, Definition 3.1.6]).

(i) Define the (generalized) module of Kolyvagin systems by

$$\overline{\mathbf{KS}}(T, \mathcal{F}_\mathcal{L}, \mathcal{P}) := \varprojlim_s \varinjlim_j \mathbf{KS}(T/p^sT, \mathcal{F}_\mathcal{L}, \mathcal{P}_j),$$

where $\mathbf{KS}(T/p^sT, \mathcal{F}_\mathcal{L}, \mathcal{P}_j)$ is the module of Kolyvagin systems for the Selmer structure $\mathcal{F}_\mathcal{L}$ on the representation T/p^sT, as in [MR04, Definition 3.1.3].

(ii) Define the module of Λ-*adic Kolyvagin systems* by

$$\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P}) := \varprojlim_{s,m} \varinjlim_j \mathbf{KS}(T_{s,m}, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P}_j),$$

where $\mathbf{KS}(T_{s,m}, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P}_j)$ is the module of Kolyvagin systems for the Selmer structure $\mathcal{F}_{\mathbb{L}_\infty}$ on the representation $T_{s,m}$.

Theorem 2.19.

(i) *The* $\mathbb{Z}_p$*-module* $\overline{\mathbf{KS}}(T, \mathcal{F}_\mathcal{L}, \mathcal{P})$ *is free of rank one.*

(ii) *The* Λ*-module* $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$ *is free of rank one, and the canonical map*

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

is surjective.

Any generator of these cyclic modules will be called a *primitive* Kolyvagin system.

Proof. Part (i) follows from [MR04, Theorem 5.2.10(ii)]. We briefly go over the hypotheses which are needed to apply [MR04, Theorem 5.2.10(ii)] and explain why they hold in our case.

To apply Theorem 5.2.10(ii) of [MR04] with the Selmer triple $(T, \mathcal{F}_\mathcal{L}, \mathcal{P})$, we first need to know that $\mathcal{X}(T, \mathcal{F}_\mathcal{L}) = 1$, and this is true thanks to Proposition 2.17(ii). Also, one needs to check that hypotheses (H.1) through (H.6) of [MR04, § 3.5] hold. We already verified (H.1)–(H.4) above; hypothesis (H.5) holds with $\mathcal{P}$ given as above, and (H.6) holds for $\mathcal{F}_\mathcal{L}$ by Proposition 2.17(i) (in fact, we only need to know that the condition (**C.3**) holds with $m = 1$).

The result analogous to [MR04, Theorem 5.2.10(ii)] which enables us to conclude (ii) was proved by the author in [Buy07]. The statement of [Buy07, Theorem 3.23] is almost identical to the statement of (ii); the only differences are that the base field $\mathbb{Q}$ should be replaced by k and the Selmer structure $\mathcal{F}_{\text{can}}$ should be replaced by $\mathcal{F}_{\mathbb{L}_\infty}$. The proof of [Buy07, Theorem 3.23] works *verbatim* after these changes; the technical points that need to be verified are the following.

(a) The G_k-representation T satisfies (H1)–(H4) as well as $(\mathbb{H}.\mathbf{T}_{/k})$ and $(\mathbb{H}.\mathbf{sEZ}_{/k})$.

(b) We have $\mathcal{X}(T, \mathcal{F}_\mathcal{L}) = 1$ for the core Selmer rank.

(c) Properties (**C.1**)–(**C.3**) hold for $\mathcal{F}_{\mathbb{L}_\infty}$.

Proposition 2.17 shows that (b) and (c) hold, and (a) is checked in Remark 2.14. □

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press

In the next section, we will obtain a generator of the cyclic Λ-module $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$ using the (conjectural) Rubin–Stark elements. Note, however, that the existence of Λ-adic Kolyvagin systems is unconditional: it does not rely on Rubin's conjecture [Rub96, Conjecture B′].

For the convenience of the reader, we record the main application of a Λ-adic Kolyvagin system $\boldsymbol{\kappa} = \{\{\kappa_\tau(s,m)\}_{\tau \in \mathcal{N}_{s+m}}\}_{s,m}$, which is a generator of the module $\overline{\mathbf{KS}}(T \otimes \Lambda, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$. See [MR04, § 3] for an explanation of our notation. Here we say, loosely, that $\kappa_\tau(s,m) \in H^1(k, T_{s,m})$ and, by definition, there is a well-defined element

$$\kappa_1 = \{\kappa_1(s,m)\}_{s,m} \in \varprojlim_{s,m} H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k, T_{s,m}) = H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k, T \otimes \Lambda).$$

For notational simplicity, we write $\mathbb{T} = T \otimes \Lambda$. Recall that $\mathrm{char}(\mathbb{A})$ denotes the characteristic ideal of a finitely generated Λ-module $\mathbb{A}$, with the convention that $\mathrm{char}(\mathbb{A}) = 0$ unless $\mathbb{A}$ is Λ-torsion.

Theorem 2.20. *Under the assumptions (A1)–(A3),*

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

Proof. This is [MR04, Theorem 5.3.10(iii)] applied to our setting. We remark that all the hypotheses of [MR04, Theorem 5.3.10(iii)] hold thanks to (A1)–(A3) (as we have already demonstrated). □

Theorem 2.20 will be applied towards establishing the main conjectures of Iwasawa theory for totally real fields. We remark once again that Theorem 2.20 does not rely on any conjecture. However, to link the statement of Theorem 2.20 with the relevant L-values, we will need to construct a Λ-adic Kolyvagin system from the (conjectural) Rubin–Stark elements; furthermore, we will need Leopoldt's conjecture to prove that the Λ-adic Kolyvagin system constructed in this way is non-trivial.

3. Λ-adic Kolyvagin systems of Stark units

In this section, we review Rubin's integral refinement of Stark's conjectures and construct Kolyvagin systems for the modified Selmer structure $\mathcal{F}_{\mathbb{L}_\infty}$ on $T \otimes \Lambda$ coming from the Stark elements of Rubin. We note that the existence of Kolyvagin systems for $\mathcal{F}_{\mathbb{L}_\infty}$ on $T \otimes \Lambda$ was proved *unconditionally* in the previous section, building on the main result of [Buy07].

For the rest of this paper, we assume that the Rubin–Stark conjecture [Rub96, Conjecture B′] holds.

Before giving an outline of Rubin's conjectures, let us define some notation. Let $k, k_\infty, \chi, f_\chi$ and L be as above. For a cycle τ of the number field k, let $k(\tau)$ be the maximal p-extension inside the ray class field of k modulo τ. Let k_n be the unique sub-extension of k_∞/k which has degree p^n over k. For any other number field F, define $F(\tau)$ to be the composite of $k(\tau)$ and F, and define F_n to be the composite of k_n and F. Let

$$\mathcal{K} = \{L_n(\tau) \mid \tau \text{ is a (finite) cycle of } k \text{ prime to } f_\chi p \text{ and } n \in \mathbb{Z}_{\geqslant 0}\}$$

and

$$\mathcal{K}_0 = \{k_n(\tau) \mid \tau \text{ is a (finite) cycle of } k \text{ prime to } f_\chi p \text{ and } n \in \mathbb{Z}_{\geqslant 0}\}$$

be two collections of abelian extensions of k.

3.1 Stark elements and Euler systems (of rank r) for $\mathbb{Z}_p(1)$

Fix a (finite) set S of places of k that does *not* contain any prime above p, but which contains the set of infinite places S_∞ and all primes λ that divide the conductor f_χ of χ. Assume that $|S| \geqslant r+1$. For each $K \in \mathcal{K}$, let

$$S_K = S \cup \{\text{places of } k \text{ at which } K \text{ is ramified}\}$$

be another set of places of k. Let $\mathcal{O}_{K,S_K}^\times$ denote the S_K units of K (i.e. the elements of $K^\times$ that are units away from the primes of K above S_K), and let Δ_K (respectively, δ_K) denote $\mathrm{Gal}(K/k)$ (respectively, $|\mathrm{Gal}(K/k)|$). Conjecture B′ of [Rub96] predicts the existence of certain elements[4]

$$\tilde{\varepsilon}_{K,S_K} \in \Lambda_{K,S_K} \subset \frac{1}{\delta_K} \bigwedge^r \mathcal{O}_{K,S_K}^\times$$

where the module Λ_{K,S_K} defined in [Rub96, § 2.1] has the property that for any homomorphism

$$\tilde{\psi} \in \mathrm{Hom}_{\mathbb{Q}_p[\Delta_K]}\left(\bigwedge^r \mathcal{O}_{K,S_K}^{\times,\wedge} \otimes \mathbb{Q}_p, \mathcal{O}_{K,S_K}^{\times,\wedge} \otimes \mathbb{Q}_p\right)$$

which is induced from a homomorphism

$$\psi \in \mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}\left(\bigwedge^r \mathcal{O}_{K,S_K}^{\times,\wedge}, \mathcal{O}_{K,S_K}^{\times,\wedge}\right),$$

one has $\tilde{\psi}(\Lambda_{K,S_K}) \subset \mathcal{O}_{K,S_K}^{\times,\wedge}$. We remark that the rth exterior power $\bigwedge^r \mathcal{O}_{K,S_K}^{\times,\wedge}$ (and all other exterior powers which appear below) is taken in the category of $\mathbb{Z}_p[\Delta_K]$-modules.

Remark 3.1. Rubin's conjecture predicts that the elements $\tilde{\varepsilon}_{K,S_K}$ should in fact lie inside the module $(1/\delta_K)\bigwedge^r \mathcal{O}_{K,S_K,\mathcal{T}}^\times$, where $\mathcal{T}$ is a finite set of primes disjoint from S_K, chosen in such a way that the group $\mathcal{O}_{K,S_K,\mathcal{T}}^\times$ of S_K-units which are congruent to 1 modulo all the primes in $\mathcal{T}$ is torsion-free. However, in our case, any set $\mathcal{T}$ which contains a prime other than 2 will suffice (since all the fields which appear in our paper are totally real). We may therefore fix $\mathcal{T}$ to be $\{\mathfrak{q}\}$, a set consisting of a single prime $\mathfrak{q}$ which is prime to 2.

Further, $\mathcal{T} = \{\mathfrak{q}\}$ may be chosen in such a way that the extra factors appearing in the definition of the $(S_K, \mathcal{T})$-modified *zeta function* for K (see [Rub96, § 1] for details about these zeta functions) will be prime to p when they are evaluated at 0. (This could be accomplished, for example, by choosing the prime $\mathfrak{q}$ so that $\mathbf{N}\mathfrak{q} - 1$ is prime to p.) We note that for such $\mathcal{T}$ we have $\mathcal{O}_{K,S_K,\mathcal{T}}^{\times,\wedge} = \mathcal{O}_{K,S_K}^{\times,\wedge}$, by the exact sequence given in [Rub96, (1)], for instance. Since in this paper we work only with the p-adic completion of the group of units, we can safely exclude $\mathcal{T}$ from our notation.

One minor issue arises because of the appearance of the set $\mathcal{T} = \{\mathfrak{q}\}$: one should remove all the fields $k_n(\tau)$ and $L_n(\tau)$ from the collections $\mathcal{K}_0$ and $\mathcal{K}$, respectively, for which $\mathfrak{q}|\tau$. This is not a problem for our purposes either.

Definition 3.2. For $F = k$ or $F = L$, we set

$$\varepsilon_{F_n(\tau),S_{F_n(\tau)}} = \mathbf{N}^r_{F_{n+1}(\tau)/F_n(\tau)}(\tilde{\varepsilon}_{F_{n+1}(\tau),S_{F_{n+1}(\tau)}})$$

[4] Note that what we call $\tilde{\varepsilon}_{K,S_K}$ here is the ε_{K,S_K} in [Buy09, Rub96]. For an explanation for the change of notation, see Remarks 3.3 and 4.1.

where $\mathbf{N}^r_{F_{n+1}(\tau)/F_n(\tau)}$ denotes the norm map induced on the rth exterior power. It follows from [Rub96, Proposition 6.1] that

$$\varepsilon_{F_n(\tau),S_{F_n(\tau)}} = \tilde{\varepsilon}_{F_n(\tau),S_{F_n(\tau)}} \quad \text{if } n \geqslant 1.$$

Note that [Rub96, Proposition 6.1] says something also when $n=0$; we will return to this point in Remark 3.3.

The collection $\{\varepsilon_{K,S_K}\}_{K\in\mathcal{K}}$ (which we shall refer to as the collection of Rubin–Stark elements) satisfies, owing to [Rub96, Proposition 6.1], the distribution relation that ought to be satisfied by an *Euler system of rank* r (in the sense of [Per98]). Since S is fixed (and therefore S_K is, too), we shall often drop S or S_K from the notation and write ε_{K,S_K} simply as ε_K; sometimes, we will use S instead of S_K and denote $\mathcal{O}_{K,S_K}$ by $\mathcal{O}_{K,S}$.

For any number field K, Kummer theory gives a canonical isomorphism

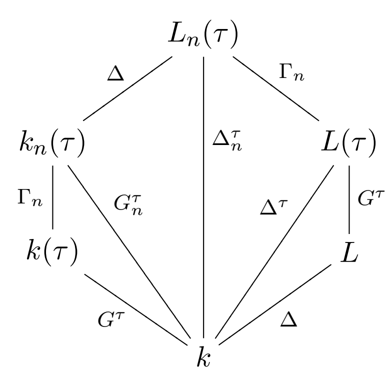
$$H^1(K,\mathbb{Z}_p(1)) \cong K^{\times,\wedge} := \varprojlim_n K^\times/(K^\times)^{p^n}.$$

Under this identification, we view each ε_{K,S_K} as an element of $(1/\delta_K)\bigwedge^r H^1(K,\mathbb{Z}_p(1))$. The distribution relation satisfied by the Stark elements (see [Rub96, Proposition 6.1]) shows that the collection $\{\varepsilon_{K,S_K}\}_{K\in\mathcal{K}}$ is an Euler system of rank r in the sense of [Per98] (except for the *denominators* $1/\delta_K$, but we ignore this subtlety for the moment, as these denominators disappear once we 'pass' to an Euler system of rank one by the defining property of these elements; see Proposition 3.14).

3.2 Twisting by the character χ

Following the formalism of [Rub00, § II.4], we may *twist* the Euler system $\{\varepsilon_{K,S_K}\}_{K\in\mathcal{K}}$ for the representation $\mathbb{Z}_p(1)$ in order to obtain an Euler system for the representation $T=\mathbb{Z}_p(1)\otimes\chi^{-1}$.

Define the Galois groups $\Gamma_n := \mathrm{Gal}(k_n/k)$, $G^\tau := \mathrm{Gal}(k(\tau)/k)$, $\Delta^\tau := \mathrm{Gal}(L(\tau)/k) = G^\tau\times\Delta$ and, finally, $G^\tau_n := \mathrm{Gal}(k_n(\tau)/k) = G^\tau\times\Gamma_n$, which is the p-part of $\Delta^\tau_n := \mathrm{Gal}(L_n(\tau)/k) \cong G^\tau_n \times \Delta = G^\tau\times\Gamma_n\times\Delta$. (These canonical factorizations of the Galois groups follow easily from the fact that $|\Delta|$ is prime to p and from ramification considerations.) This description is summarized in the following array of fields and Galois groups.



Let χ be as above, and let ϵ_χ denote the idempotent $(1/|\Delta|)\sum_{\sigma\in\Delta}\chi(\sigma)\sigma^{-1}$. We may (and will) regard this element as an element of the groups ring $\mathbb{Z}_p[\Delta^\tau_n]$ via the factorization above. For notational simplicity, we set $\delta=\delta_{k_n(\tau)}$ (note that δ also equals $\delta_{L_n(\tau)}$ up to multiplication by a p-adic unit). In what follows, δ will appear as a denominator; although δ does depend on n and τ, we will allow ourselves to be sloppy with the notation we use for these denominators, as they

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press

will not be present when the Stark elements are utilized for our main purposes (i.e. when they are used to construct a Λ-adic Kolyvagin system for the Selmer structure $\mathcal{F}_{\mathbb{L}_\infty}$).

For any cycle τ which is prime to pf_χ, we define

$$\begin{aligned}\varepsilon^{\chi}_{L_n(\tau)} := \epsilon_\chi \varepsilon_{L_n(\tau),S} &\in \frac{1}{\delta}\epsilon_\chi \bigwedge^r H^1(L_n(\tau),\mathbb{Z}_p(1)) &(4)\\ &= \frac{1}{\delta}\bigwedge^r \epsilon_\chi H^1(L_n(\tau),\mathbb{Z}_p(1)) &(5)\\ &= \frac{1}{\delta}\bigwedge^r H^1(L_n(\tau),\mathbb{Z}_p(1))^\chi. &(6)\end{aligned}$$

We note that the equality between the lines (4) and (5) above,

$$\begin{aligned}\left(\bigwedge^r H^1(L_n(\tau),\mathbb{Z}_p(1))\right)^\chi &= \epsilon_\chi \bigwedge^r H^1(L_n(\tau),\mathbb{Z}_p(1))\\ &= \bigwedge^r \epsilon_\chi H^1(L_n(\tau),\mathbb{Z}_p(1))\\ &= \bigwedge^r H^1(L_n(\tau),\mathbb{Z}_p(1))^\chi,\end{aligned}$$

holds simply because $\epsilon_\chi^r = \epsilon_\chi$.

The Hochschild–Serre spectral sequence gives rise to an exact sequence

$$H^1(\Delta,T) \longrightarrow H^1(k_n(\tau),T) \longrightarrow H^1(L_n(\tau),T)^\Delta \longrightarrow H^2(\Delta,T), \tag{7}$$

where $H^1(L_n(\tau),T)^\Delta$ stands for the largest submodule of $H^1(L_n(\tau),T)$ on which Δ acts trivially. On the other hand, since $|\Delta|$ is prime to p, it follows that the very first and very last terms in (7) vanish. We therefore have an isomorphism

$$H^1(k_n(\tau),\mathbb{Z}_p(1)\otimes\chi^{-1}) \longrightarrow H^1(L_n(\tau),\mathbb{Z}_p(1)\otimes\chi^{-1})^\Delta.$$

Now, since $G_{L_n(\tau)}$ is in the kernel of χ,

$$H^1(L_n(\tau),\mathbb{Z}_p\otimes\chi^{-1}) \cong H^1(L_n(\tau),\mathbb{Z}_p(1))\otimes\chi^{-1}$$

and hence

$$H^1(k_n(\tau),T) \xrightarrow{\sim} H^1(L_n(\tau),T)^\Delta \cong H^1(L_n(\tau),\mathbb{Z}_p(1))^\chi. \tag{8}$$

This induces an isomorphism

$$\bigwedge^r H^1(k_n(\tau),T) \xrightarrow{\sim} \bigwedge^r H^1(L_n(\tau),\mathbb{Z}_p(1))^\chi. \tag{9}$$

The inverse image of the element $\varepsilon^{\chi}_{L_n(\tau)}$ (which was defined in (4)) under the isomorphism induced from (9) will be denoted by $\varepsilon^{\chi}_{k_n(\tau)}$. The collection $\{\varepsilon^{\chi}_{k_n(\tau)}\}_{n,\tau} = \{\varepsilon^{\chi}_K\}_{K\in\mathcal{K}_0}$ will be called the *Stark element Euler system of rank r*.

Remark 3.3. Suppose that (A3) holds. From our definition of $\varepsilon_{L(\tau)}$ and [Rub96, Proposition 6.1], it follows that

$$\varepsilon_{L(\tau)} = \prod_{\wp | p}(1-\mathrm{Frob}_\wp^{-1})\tilde{\varepsilon}_{L(\tau)},$$

where the product is over all primes $\wp$ of k which lie above p and $\mathrm{Frob}_\wp$ is the Frobenius element at $\wp$ inside G_k. Hence, upon restricting to the χ-parts, we see that

$$\varepsilon_k^\chi = \prod_{\wp|p}(1-\chi^{-1}(\mathrm{Frob}_\wp))\tilde{\varepsilon}_k^\chi.$$

(We warn the reader that we are still using the additive notation.) It follows from assumption (A3) that the element ε_k^χ used in this paper differs from the element $\tilde{\varepsilon}_k^\chi$ (which is identical to the element ε_k^χ appearing in [Buy09]) only by a unit $u \in \mathbb{Z}_p^\times$:

$$\varepsilon_k^\chi = u \cdot \tilde{\varepsilon}_k^\chi.$$

See also Remark 4.1 below, where we use this fact to compare the Kolyvagin systems derived from these two families of Rubin–Stark elements.

Next, we construct an *Euler system of rank one* (i.e. an Euler system in the sense of [Rub00]), using ideas from [Rub96, § 6] and [Per98, § 1.2.3]. The main point is that if one were to apply the arguments of [Per98, Rub96] directly, all one would get (after applying Kolyvagin's descent) would be a Λ-adic Kolyvagin system for the coarser Selmer structure $\mathcal{F}_\Lambda$ on $T \otimes \Lambda$. In § 3.4, we overcome this difficulty and obtain a Λ-adic Kolyvagin system for the finer Selmer structure $\mathcal{F}_{\mathbb{L}_\infty}$ on $T \otimes \Lambda$.

3.3 Choosing homomorphisms

For any field $K \in \mathcal{K}_0$, recall that $\Delta_K := \mathrm{Gal}(K/k)$ and write $\delta = |\Delta_K|$. By using the elements of

$$\varprojlim_{K\in\mathcal{K}_0} \bigwedge^{r-1} \mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K,T), \mathbb{Z}_p[\Delta_K]) \tag{10}$$

(or the images of the elements of

$$\varprojlim_{K\in\mathcal{K}_0} \bigwedge^{r-1} \mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K_p,T), \mathbb{Z}_p[\Delta_K])$$

under the canonical map

$$\varprojlim_{K\in\mathcal{K}_0} \bigwedge^{r-1} \mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K_p,T), \mathbb{Z}_p[\Delta_K]) \longrightarrow \varprojlim_{K\in\mathcal{K}_0} \bigwedge^{r-1} \mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K,T), \mathbb{Z}_p[\Delta_K])$$

induced from the localization at p) and the Rubin–Stark elements above, Rubin [Rub96, § 6] (see also [Per98, § 1.2.3]) showed how to obtain an Euler system (in the sense of [Rub00]) for the G_k-representation T. In this section, we show how to choose the homomorphisms appearing in the inverse limit (10) carefully, so that the resulting Euler system gives rise to a Kolyvagin system for the $\mathbb{L}_\infty$-modified Selmer structure $\mathcal{F}_{\mathbb{L}_\infty}$ on $T \otimes \Lambda$. We remark also that for $\Psi = \{\psi_K\}$ belonging to the module (10),

$$\psi_K(\varepsilon_K^\chi) \in H^1(K,T)$$

by the defining (integrality) property of the elements

$$\varepsilon_K^\chi \in \frac{1}{\delta}\bigwedge^{r} H^1(K,T);$$

that is, the denominators δ will disappear once we apply the homomorphisms from (10) to the Rubin–Stark elements.

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press

One may again identify $H^1(k_n(\tau), T)$ with $(L_n(\tau)^\times)^\chi$, using the isomorphism (8) and Kummer theory. Similarly, one may identify the semi-local cohomology group $H^1(k_n(\tau)_p, T)$ with $(L_n(\tau)_p^\times)^\chi$, where $L_n(\tau)_p := L_n(\tau) \otimes \mathbb{Q}_p$. Let $V_{L_n(\tau)}$ denote the p-adic completion of the local units of $L_n(\tau)_p$.

The proof of [Rub00, Proposition III.2.6(ii)] gives the next lemma.

Lemma 3.4. *Assume that (A3) holds. Then for every $k_n(\tau) \in \mathcal{K}_0$,*

$$H^1(k_n(\tau)_p, T) \cong (L_n(\tau)_p^\times)^\chi \cong V_{L_n(\tau)}^\chi$$

for all $k_n(\tau) \in \mathcal{K}_0$.

Recall that $r = [k : \mathbb{Q}]$ and note that all the fields that appear in this paper (namely, the elements of the collections $\mathcal{K}$ and $\mathcal{K}_0$) are totally real. Further, assuming (A1) (i.e. that p is prime to f_χ), it follows that $L(\tau)/k$ is unramified at all primes above p. Therefore, Krasner's lemma [Kra39] on the structure of 1-units implies the following.

Lemma 3.5. *If (A1) holds, then $V_{L(\tau)}$ is a free $\mathbb{Z}_p[\Delta^\tau]$-module of rank r.*

Corollary 3.6. *Assume that (A1) and (A3) hold. Then, for every $k(\tau) \in \mathcal{K}_0$, the $\mathbb{Z}_p[G^\tau]$-module $H^1(k(\tau)_p, T) = V_{L(\tau)}^\chi$ is free of rank r.*

Hereafter we shall assume that (A1)–(A3) hold.

Proposition 3.7. *For every $k(\tau) \in \mathcal{K}_0$:*

(i) *the Λ-module $H^1(k(\tau)_p, T \otimes \Lambda)$ is free of rank $[k(\tau) : \mathbb{Q}] = r \cdot |G^\tau|$;*

(ii) *the canonical map $H^1(k(\tau)_p, T \otimes \Lambda) \to H^1(k(\tau)_p, T)$ is surjective.*

Proof. Let $\mathcal{Q}$ be any prime of $k(\tau)$ lying above p, and let $k(\tau)_{\mathcal{Q},\infty}$ be the cyclotomic $\mathbb{Z}_p$-extension of $k(\tau)_\mathcal{Q}$. We set

$$H_{k(\tau)_\mathcal{Q}} = \mathrm{Gal}(\overline{k(\tau)}_\mathcal{Q}/k(\tau)_{\mathcal{Q},\infty}),$$

following the notation in Appendix A. Owing to assumption (A2), the extension $k(\tau)$ is unramified at p, and we may therefore identify Γ with $\mathrm{Gal}(k(\tau)_{\mathcal{Q},\infty}/k(\tau)_\mathcal{Q})$.

It is easy to see that $H^0(k(\tau)_\mathcal{Q}, T) = 0$. Therefore, applying Theorem A.8 with the field $k(\tau)$ proves (i). To prove (ii), we need to check that

$$0 = \mathrm{coker}(H^1(k(\tau)_p, T \otimes \Lambda) \longrightarrow H^1(k(\tau)_p, T)) = H^2(k(\tau)_p, T \otimes \Lambda)[\gamma - 1].$$

As in the proof of Proposition 2.9(ii), this follows (by local duality) from the vanishing condition

$$H^0(k(\tau)_p, T^*) = H^0(k_p, T^*) = 0,$$

where the second equality holds thanks to (A3) and the first equality follows from the proof of [Rub00, Lemma IV.2.5(i)] together with the remark after [Rub00, Conjecture VIII.2.6]. □

Remark 3.8. The statement of Proposition 3.7(ii) is equivalent to the statement that the map

$$H^1(k(\tau)_p, T \otimes \Lambda)/(\gamma - 1) \longrightarrow H^1(k(\tau)_p, T)$$

is an isomorphism.

Let $\Lambda_\tau := \mathbb{Z}_p[[G^\tau \times \Lambda]] = \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G^\tau]$ and let $\mathbb{M} = \bigcup_{F \in \mathcal{K}_0} F$.

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press

Proposition 3.9. *The Λ_τ-module $H^1(k(\tau)_p, T\otimes\Lambda)$ is free of rank r.*

Proof. Let $e=\{e_1,\ldots,e_r\}$ be a $\mathbb{Z}_p[G^\tau]$-basis for $H^1(k(\tau)_p,T)$. By Proposition 3.7(ii) and Nakayama's lemma, there exists a set of generators $\mathbb{E}=\{\mathbb{E}_1,\ldots,\mathbb{E}_r\}$ of the Λ_τ-module $H^1(k(\tau)_p,T\otimes\Lambda)$ which lifts the basis e (with respect to the surjection of Proposition 3.7(ii)).

We claim that $\mathbb{E}$ is a basis for the Λ_τ-module $H^1(k(\tau)_p,T\otimes\Lambda)$. Assume the contrary, and suppose that there is a non-trivial relation

$$\sum_{i=1}^{r} a_i\mathbb{E}_i=0 \tag{11}$$

with $a_i\in\Lambda_\tau$. Since $H^1(k(\tau)_p,T\otimes\Lambda)$ is Λ-torsion free (by Proposition 3.7(i)), we may assume without loss of generality that $a_1\notin(\gamma-1)$. This implies that the relation (11), reduced modulo $(\gamma-1)$, gives rise to a non-trivial relation among $\{e_1,\ldots,e_r\}$ over $\mathbb{Z}_p[G^\tau]$. This is a contradiction; hence the set of generators $\mathbb{E}$ is a Λ_τ-basis for $H^1(k(\tau)_p,T\otimes\Lambda)$. □

Corollary 3.10. *The $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]]$-module $\mathbb{V}:=\varprojlim_{n,\tau} H^1(k_n(\tau)_p,T)=\varprojlim_{\tau} H^1(k(\tau)_p, T\otimes\Lambda)$ is free of rank r.*

Proof. This is an immediate consequence of Proposition 3.9. □

Corollary 3.11. *The $\mathbb{Z}_p[G_n^\tau]$-module $H^1(k_n(\tau)_p,T)$ is free of rank r.*

Proof. This follows from Proposition 3.9 and the fact that the map

$$H^1(k(\tau)_p,T\otimes\Lambda)\longrightarrow H^1(k_n(\tau)_p,T)$$

is surjective (as the relevant H^2 vanishes). □

Choose *any* $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]]$-line $\mathbb{L}$ inside $\mathbb{V}$ such that the quotient $\mathbb{V}/\mathbb{L}$ is also free (of rank $r-1$) as a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]]$-module.

Remark 3.12. Although the main results of this article do not 'see' the choice of the line $\mathbb{L}\subset\mathbb{V}$, our methods require us, in an essential way, to make this somewhat unnatural choice.

Choose any decomposition

$$\mathbb{V}=\bigoplus_{i=1}^{r}\mathbb{L}_i \tag{12}$$

of $\mathbb{V}$ into rank-one $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]]$-modules. This, in turn, fixes a decomposition

$$H^1(k_p,T)=\bigoplus_{i=1}^{r}\mathcal{L}_i \tag{13}$$

into rank-one $\mathbb{Z}_p$-modules $\mathcal{L}_i$, with $\mathbb{L}_i\mapsto\mathcal{L}_i$ under the obvious map $\mathbb{V}\to H^1(k_p,T)$. Consider

$$\sum_{i=1}^{r}\overline{\mathbf{KS}}(T,\mathcal{F}_{\mathcal{L}_i},\mathcal{P})\subset\overline{\mathbf{KS}}(T,\mathcal{F}_{\mathrm{can}},\mathcal{P}). \tag{14}$$

It is not hard to see (cf. [Buy08, Remark 1.27]) that the sum in (14) is, in fact, a direct sum. In view of the fact that the main applications of the Kolyvagin systems for the modified Selmer structure $\mathcal{F}_{\mathcal{L}_i}$ are independent of the choice of $\mathcal{L}_i$, it seems natural to raise the following question.

Question. Does the rank-r submodule

$$\bigoplus_{i=1}^{r} \overline{\mathbf{KS}}(T, \mathcal{F}_{\mathcal{L}_i}, \mathcal{P}) \subset \overline{\mathbf{KS}}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$$

depend on the decomposition (12)?

Unfortunately, at present we are not able to answer this question. Note that if the answer to this question were to be affirmative, one would have a natural rank-r submodule of $\overline{\mathbf{KS}}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$; see [Buy08, Theorem 1.28] for further discussion of this matter.

Definition 3.13. For all $k_n(\tau) = K \in \mathcal{K}_0$, let $\mathcal{L}_K$ be the image of $\mathbb{L}$ under the (surjective) projection map $\mathbb{V} \to H^1(K_p, T)$.

Note that, for all $K \in \mathcal{K}_0$, $\mathcal{L}_K$ is a free $\mathbb{Z}_p[\Delta_K]$-module of rank one and that

$$(\mathcal{L}_{K'})^{\mathrm{Gal}(K'/K)} = \mathcal{L}_K$$

for all $K \subset K'$. We will simply write $\mathcal{L}$ for $\mathcal{L}_k$ and $\mathcal{L}_n^\tau$ for $\mathcal{L}_{k_n(\tau)}$. We denote the image of $\mathbb{L}$ under the projection $\mathbb{V} \twoheadrightarrow H^1(k(\tau)_p, T \otimes \Lambda)$ by $\mathbb{L}_\infty^\tau$. When $\tau = 1$, we simply write $\mathbb{L}_\infty$ for $\mathbb{L}_\infty^\tau$ and $\mathcal{L}_n$ for $\mathcal{L}_n^\tau$.

We define

$$\bigwedge^{r-1} \mathbf{Hom}(\mathbb{V}, \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]]) := \varprojlim_{K \in \mathcal{K}_0} \bigwedge^{r-1} \mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K_p, T), \mathbb{Z}_p[\Delta_K]),$$

where the inverse limit is taken with respect to the natural maps induced from the restriction map

$$H^1(K_p, T) \longrightarrow H^1(K'_p, T)^{\mathrm{Gal}(K'/K)}$$

(which is easily verified to be injective, e.g. by using the identifications of the semi-local cohomology groups in question with semi-local units) and the isomorphism

$$\begin{aligned} \mathbb{Z}_p[\Delta_{K'}]^{\mathrm{Gal}(K'/K)} &\xrightarrow{\sim} \mathbb{Z}_p[\Delta_K] \\ \mathbf{N}_K^{K'} &\longmapsto 1 \end{aligned}$$

for $K \subset K'$.

The localization map at p gives rise to a map $H^1(K, T) \xrightarrow{\mathrm{loc}_p} H^1(K_p, T)$, which induces a canonical map

$$\bigwedge^{r-1} \mathbf{Hom}(\mathbb{V}, \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]]) \longrightarrow \varprojlim_{K \in \mathcal{K}_0} \bigwedge^{r-1} \mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K, T), \mathbb{Z}_p[\Delta_K]). \tag{15}$$

We will still use Φ to denote the image of $\Phi \in \bigwedge^{r-1} \mathbf{Hom}(\mathbb{V}, \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]])$ under this map. Choose an arbitrary $\{\phi_K\}_{K \in \mathcal{K}_0} = \Phi \in \bigwedge^{r-1} \mathbf{Hom}(\mathbb{V}, \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]])$ and define[5]

$$H^1(K, T) \ni \varepsilon_{K,\Phi}^\chi := \phi_K(\varepsilon_K^\chi),$$

where $\{\varepsilon_K^\chi\}_{K \in \mathcal{K}_0}$ is the Stark element Euler system of rank r defined in § 3.2.

[5] To make sense of our notation, first use the map (15) to view ϕ_K as an element of $\bigwedge^{r-1} \mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K, T), \mathbb{Z}_p[\Delta_K])$; then use [Rub96, (4)] to view it as an element of $\mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(\bigwedge^r H^1(K, T), H^1(K, T))$.

Proposition 3.14. *The collection $\{\varepsilon^{\chi}_{K,\Phi}\}_{K\in\mathcal{K}_0}$ (which will henceforth be referred to as the Euler system of Φ-Stark elements) is an Euler system for the G_k-representation $T=\mathbb{Z}_p(1)\otimes\chi^{-1}$, in the sense of [Rub00, Definition II.1.1].*

We will sometimes write $\{\varepsilon^{\chi}_{k_n(\tau),\Phi}\}_{n,\tau}$ for the Euler system $\{\varepsilon^{\chi}_{K,\Phi}\}_{K\in\mathcal{K}_0}$.

Proof. This is [Rub96, Proposition 6.6]. See also [Per98, § 1.2.3] for a more general application of this idea. □

Proposition 3.15. *For any $K\in\mathcal{K}_0$, the projection map*

$$\bigwedge^{r-1}\mathbf{Hom}(\mathbb{V},\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]])\longrightarrow\bigwedge^{r-1}\mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K_p,T),\mathbb{Z}_p[\Delta_K])$$

is surjective.

Proof. This is obvious from Corollary 3.11. □

If the *Euler system to Kolyvagin system map* of Mazur and Rubin (see [MR04, Theorem 5.3.3]) is applied to the Euler system of Φ-Stark elements, then all one gets is a Λ-adic Kolyvagin system for the coarser Selmer structure $\mathcal{F}_\Lambda$ on $T\otimes\Lambda$. In the following, we will choose a particular element $\Phi_0^{(\infty)}\in\bigwedge^{r-1}\mathbf{Hom}(\mathbb{V},\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]])$ so that the Kolyvagin system (coming from the $\Phi_0^{(\infty)}$-Stark elements) will be a Kolyvagin system for the finer Selmer structure $\mathcal{F}_{\mathbb{L}_\infty}$.

Definition 3.16. We say that an element

$$\{\phi_n^\tau\}_{n,\tau}=\Phi\in\bigwedge^{r-1}\mathbf{Hom}(\mathbb{V},\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]])$$

satisfies $\mathrm{H}_{\mathbb{L}}$ if for any $K=k_n(\tau)\in\mathcal{K}_0$ one has $\phi_n^\tau(\bigwedge^r H^1(K_p,T))\subset\mathcal{L}_n^\tau$.

Next, we will construct an element

$$\Phi_0^{(\infty)}\in\bigwedge^{r-1}\mathbf{Hom}(\mathbb{V},\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]])$$

which satisfies $\mathrm{H}_{\mathbb{L}}$ and lifts the element Φ_0 of [Buy09, § 2.3] with respect to the (surjective) map

$$\bigwedge^{r-1}\mathbf{Hom}(\mathbb{V},\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]])\longrightarrow\varprojlim_{\tau}\bigwedge^{r-1}\mathrm{Hom}_{\mathbb{Z}_p[G^\tau]}(H^1(k(\tau)_p,T),\mathbb{Z}_p[G^\tau])\ni\Phi_0.$$

The element Φ_0 was used in [Buy09] to construct a *primitive* Kolyvagin system for the Selmer structure $\mathcal{F}_{\mathcal{L}}$ on T.

Fix a basis $\{\Psi_{\mathbb{L}}^{(i)}\}_{i=1}^{r-1}$ of the free $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]]$-module

$$\mathrm{Hom}_{\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]]}(\mathbb{V}/\mathbb{L},\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]])$$

of rank $r-1$. This in turn fixes a basis $\{\psi^{(i)}_{\mathcal{L}_n^\tau}\}_{i=1}^{r-1}$ for the free $\mathbb{Z}_p[G_n^\tau]$-module

$$\mathrm{Hom}_{\mathbb{Z}_p[G_n^\tau]}(H^1(k_n(\tau)_p,T)/\mathcal{L}_n^\tau,\ \mathbb{Z}_p[G_n^\tau]),$$

for all $k_n(\tau)\in\mathcal{K}_0$, such that the homomorphisms $\{\psi^{(i)}_{\mathcal{L}_n^\tau}\}_{n,\tau}$ are compatible with respect to the surjections

$$\mathrm{Hom}_{\mathbb{Z}_p[\Delta_{K'}]}(H^1(K'_p,T)/\mathcal{L}_{K'},\mathbb{Z}_p[\Delta_{K'}])\longrightarrow\mathrm{Hom}_{\mathbb{Z}_p[\Delta_K]}(H^1(K_p,T)/\mathcal{L}_K,\mathbb{Z}_p[\Delta_K])$$

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press

for $k_n(\tau) = K \subset K' = k_{n'}(\tau')$. Furthermore, the homomorphism

$$\bigoplus_{i=1}^{r-1} \psi^{(i)}_{\mathcal{L}_n^\tau} : H^1(k_n(\tau)_p, T)/\mathcal{L}_n^\tau \longrightarrow \mathbb{Z}_p[G_n^\tau]^{r-1}$$

is an isomorphism of $\mathbb{Z}_p[G_n^\tau]$-modules, for every n and τ.

Let $\psi^{(i)}_{n,\tau}$ denote the image of $\psi^{(i)}_{\mathcal{L}_n^\tau}$ under the canonical injection

$$\mathrm{Hom}_{\mathbb{Z}_p[G_n^\tau]}(H^1(k_n(\tau)_p, T)/\mathcal{L}_n^\tau, \mathbb{Z}_p[G_n^\tau]) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_p[G^\tau]}(H^1(k_n(\tau)_p, T), \mathbb{Z}_p[G_n^\tau]).$$

Note then that the map

$$\Psi_n^\tau := \bigoplus_{i=1}^{r-1} \psi^{(i)}_{n,\tau} : H^1(k_n(\tau)_p, T) \longrightarrow \mathbb{Z}_p[G_n^\tau]^{r-1}$$

is surjective and that $\ker(\Psi_n^\tau) = \mathcal{L}_n^\tau$.

Define

$$\phi_n^\tau := \psi^{(1)}_{n,\tau} \wedge \psi^{(2)}_{n,\tau} \wedge \cdots \wedge \psi^{(r-1)}_{n,\tau} \in \bigwedge^{r-1} \mathrm{Hom}(H^1(k_n(\tau)_p, \mathbb{Z}_p[G_n^\tau]).$$

(When $\tau = 1$, we drop 'τ' from the notation and write simply ϕ_n for ϕ_n^τ and so on.) Note once again that for $\tau|\tau'$ and $n \leqslant n'$, the element $\phi_{n'}^{\tau'}$ maps to the element ϕ_n^τ under the surjective (by Corollary 3.11) homomorphism

$$\bigwedge^{r-1} \mathrm{Hom}(H^1(k_{n'}(\tau')_p, T), \mathbb{Z}_p[G_{n'}^{\tau'}]) \twoheadrightarrow \bigwedge^{r-1} \mathrm{Hom}(H^1(k_n(\tau)_p, T), \mathbb{Z}_p[G_n^\tau]).$$

We may therefore regard $\Phi_0^{(\infty)} := \{\phi_n^\tau\}_{n,\tau}$ as an element of the module

$$\varprojlim_{k_n(\tau)\in\mathcal{K}_0} \bigwedge^{r-1} \mathrm{Hom}(H^1(k_n(\tau)_p, T), \mathbb{Z}_p[G_n^\tau]) = \bigwedge^{r-1} \mathbf{Hom}(\mathbb{V}, \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]]).$$

Proposition 3.17. *Let $\{\phi_n^\tau\}_{n,\tau} = \Phi_0^{(\infty)}$ be as above. Then for every n and τ, ϕ_n^τ induces an isomorphism*

$$\phi_n^\tau : \bigwedge^{r} H^1(k_n(\tau)_p, T) \xrightarrow{\sim} \ker(\Psi_n^\tau) = \mathcal{L}_n^\tau.$$

In particular, $\Phi_0^{(\infty)}$ satisfies $\mathrm{H}_{\mathbb{L}}$.

Proof. The proof is identical to the proof of (the easy half of) [Buy07, Lemma 3.1], which also follows the proof of [MR04, Lemma B.1] almost line by line. □

Remark 3.18. It is easy to see that the element $\Phi_0^{(\infty)}$ lifts, by construction, the element Φ_0 of [Buy07, § 2.3], in the sense explained above.

Remark 3.19. Since the map

$$H^1(k_p, T \otimes \Lambda) = \varprojlim_n H^1((k_n)_p, T) \longrightarrow H^1((k_n)_p, T)$$

is surjective for every n and the Λ-module $H^1(k_p, T \otimes \Lambda)$ (respectively, the $\mathbb{Z}_p[\Gamma_n]$-module $H^1((k_n)_p, T)$) is free of rank r, it follows that the natural map

$$\bigwedge^{r} H^1(k_p, T \otimes \Lambda) = \bigwedge^{r} \varprojlim_n H^1((k_n)_p, T) \longrightarrow \varprojlim_n \bigwedge^{r} H^1((k_n)_p, T)$$

is an isomorphism. This, combined with Proposition 3.17, shows that the map $\phi_\infty := \{\phi_n\}_n$ induces an isomorphism

$$\bigwedge^r H^1(k_p, T\otimes\Lambda) \cong \varprojlim_n \bigwedge^r H^1((k_n)_p, T) \xrightarrow{\phi_\infty} \varprojlim_n \mathcal{L}_n = \mathbb{L}_\infty.$$

3.4 Kolyvagin systems for the $\mathbb{L}_\infty$-modified Selmer triple: II

For notational simplicity, write $\mathbb{T} := T\otimes\Lambda$ and, for a fixed topological generator γ of $\Gamma = \mathrm{Gal}(k_\infty/k)$, set $\gamma_n = \gamma^{p^n}$. Let $\mathcal{M}$ denote the maximal ideal of Λ. Fix a finite set S as in § 3.1 which does not contain any non-archimedean prime that splits completely in L/k. Throughout this section, we assume (A1)–(A3) as well as the Rubin–Stark conjecture [Rub96, Conjecture B′] for S and for every $K\in\mathcal{K}$.

In § 2.5, we proved under the hypotheses (A1)–(A3) that:

(i) the Λ-module $\overline{\mathbf{KS}}(\mathbb{T}, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$ is free of rank one;

(ii) the $\mathbb{Z}_p$-module $\overline{\mathbf{KS}}(T, \mathcal{F}_{\mathcal{L}}, \mathcal{P})$ is free of rank one;

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

In [Buy09], a particular generator $\kappa^{\Phi_0} \in \overline{\mathbf{KS}}(T, \mathcal{F}_{\mathcal{L}}, \mathcal{P})$ was constructed using the Rubin–Stark elements. The main goal of this section is to 'lift' κ^{Φ_0} to a Λ-adic Kolyvagin system $\boldsymbol{\kappa}^{\Phi_0^{(\infty)}} \in \overline{\mathbf{KS}}(\mathbb{T}, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$, so that $\boldsymbol{\kappa}^{\Phi_0^{(\infty)}}$ maps to κ^{Φ_0} under the surjection of (iii) above.

Definition 3.20. For $\mathbb{F} = \mathcal{F}_\Lambda$ or $\mathcal{F}_{\mathbb{L}_\infty}$, we set

$$\overline{\mathbf{KS}}'(\mathbb{T}, \mathbb{F}, \mathcal{P}) := \varprojlim_{m,n} \varinjlim_{j} \mathbf{KS}(\mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T}, \mathbb{F}, \mathcal{P}_j),$$

where $\mathbf{KS}(\mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T}, \mathbb{F}, \mathcal{P}_j)$ is the $\Lambda/(p^m, \gamma_n - 1)$-module of Kolyvagin systems (in the sense of [MR04, Definition 3.1.3]) for the propagated Selmer structure $\mathbb{F}$ on the quotient $\mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T}$.

Remark 3.21. We introduced the module $\overline{\mathbf{KS}}'(\mathbb{T}, \mathbb{F}, \mathcal{P})$ because, after applying Kolyvagin's descent procedure [Rub00, § IV] (modified appropriately in [MR04, Appendix A]), one obtains elements of $\overline{\mathbf{KS}}'(\mathbb{T}, \mathcal{F}_\Lambda, \mathcal{P})$. On the other hand, it is not hard to see that the module $\overline{\mathbf{KS}}'(\mathbb{T}, \mathbb{F}, \mathcal{P})$ defined above is naturally isomorphic to the module $\overline{\mathbf{KS}}(\mathbb{T}, \mathbb{F}, \mathcal{P})$ of Definition 2.18(ii), using the fact that each of the collections $\{p^m, \gamma_n - 1\}_{m,n}$ and $\{p^m, \mathbf{X}^n\}_{m,n}$ forms a base of neighborhoods at zero. Furthermore, using the fact that the collection $\{\mathcal{M}^\alpha\}_{\alpha\in\mathbb{Z}^+}$ also forms a base of neighborhoods at zero, one may identify these two modules of Kolyvagin systems with the generalized module of Kolyvagin systems defined in [MR04, Definition 3.1.6]. With a slight abuse of notation, we will write $\overline{\mathbf{KS}}(\mathbb{T}, \mathbb{F}, \mathcal{P})$ for any of the three modules of Kolyvagin systems given by three different definitions (i.e. Definition 2.18 and Definition 3.20 here, and [MR04, Definition 3.1.6]). For the current section, we will use Definition 3.20 to define this module.

Let $\mathbf{ES}(T)$ denote the collection of Euler systems for T, in the sense of [Rub00]. The *Euler system to Kolyvagin system map* of [MR04, Theorem 5.3.3] gives a map

$$\mathbf{ES}(T) \longrightarrow \overline{\mathbf{KS}}(\mathbb{T}, \mathcal{F}_\Lambda, \mathcal{P}).$$

Fix an arbitrary $\{\phi_n^\tau\}_{n,\tau} = \Phi \in \bigwedge^{r-1} \mathbf{Hom}(\mathbb{V}, \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]])$ which satisfies $\mathrm{H}_{\mathbb{L}}$, and let $\boldsymbol{\kappa}^\Phi = \{\{\kappa_\tau^\Phi(m,n)\}_{\tau\in\mathcal{N}}\}_{m,n}$ be the image of the Euler system $\{\varepsilon^\chi_{k_n(\tau),\Phi}\}_{n,\tau}$ of Proposition 3.14.

Thanks to [MR04, Theorem 5.3.3], we know the following relationships.

$$\begin{array}{ccc} \kappa_1^{\Phi} \overset{\text{def}}{=\!=} \varprojlim_{m,n} \kappa_1^{\Phi}(m,n) \in \varprojlim_{m,n} H^1(k, \mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T}) = H^1(k, \mathbb{T}) \\ \| \\ \{\varepsilon^{\chi}_{k_n,\Phi}\}_n \overset{\text{def}}{=\!=\!=\!=} \{\phi_n(\varepsilon^{\chi}_{k_n})\}_n \in \varprojlim_n H^1(k_n, T) = H^1(k, \mathbb{T}) \end{array}$$

Remark 3.22. For every (rational) prime ℓ, Shapiro's lemma shows that

$$H^1(k(\tau), \mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T}) \cong H^1(k_n(\tau), T/p^m T), \tag{16}$$

$$H^1(k(\tau)_\ell, \mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T}) \cong H^1(k_n(\tau)_\ell, T/p^m T). \tag{17}$$

See [MR04, Lemma 5.3.1] for the first isomorphism and [Rub00, Appendix B.5] for its semi-local version. Thus, we may talk about the propagation of a local condition $H^1_{\mathcal{F}}(k_\ell, \mathbb{T}) \subset H^1(k_\ell, \mathbb{T})$ at ℓ to a local condition

$$H^1_{\mathcal{F}}((k_n)_\ell, T/p^m T) \subset H^1((k_n)_\ell, T/p^m T) \cong H^1(k_\ell, \mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T}),$$

i.e. we define $H^1_{\mathcal{F}}((k_n)_\ell, T/p^m T)$ to be the isomorphic copy of $H^1_{\mathcal{F}}(k_\ell, \mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T})$ under the isomorphism (17) of Shapiro's lemma.

Theorem 3.23. *For any $\Phi \in \bigwedge^{r-1} \mathbf{Hom}(\mathbb{V}, \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]])$ which satisfies* $\mathrm{H}_{\mathbb{L}}$,

$$\boldsymbol{\kappa}^{\Phi} := \{\{\kappa^{\Phi}_{\tau}(m,n)\}_{\tau \in \mathcal{N}}\}_{m,n} \in \overline{\mathbf{KS}}(\mathbb{T}, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P}).$$

For the rest of this section, the integers m and n will be fixed, and we will write the element $\kappa^{\Phi}_{\tau}(m,n) \in H^1(k, \mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T})$ simply as κ^{Φ}_{τ}. Theorem 3.23 claims that for each $\tau \in \mathcal{N}_{m+n}$, $\kappa^{\Phi}_{\tau} \in H^1_{\mathcal{F}_{\mathbb{L}_\infty}(\tau)}(k, \mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T})$, where $\mathcal{F}_{\mathbb{L}_\infty}(\tau)$ is the modified Selmer structure defined in [MR04, Example 2.1.8]. Here we merely remark that the Selmer structures $\mathcal{F}_{\mathbb{L}_\infty}$ and $\mathcal{F}_{\mathbb{L}_\infty}(\tau)$ determine the same local conditions away from τ; in particular, they agree at p. On the other hand, [MR04, Theorem 5.3.3] already shows that $\kappa^{\Phi}_{\tau} \in H^1_{\mathcal{F}_{\Lambda}(\tau)}(k, \mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T})$. Since $\mathcal{F}_{\mathbb{L}_\infty}$ and $\mathcal{F}_{\Lambda}$ determine the same local conditions away from p, Theorem 3.23 follows from the next proposition.

Proposition 3.24. *Let*

$$\begin{array}{rccc} \mathrm{loc}_p: & H^1(k, \mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T}) & \longrightarrow & H^1(k_p, \mathbb{T}/(p^m, \gamma_n - 1)\mathbb{T}) \\ & \downarrow \cong & & \downarrow \cong \\ & H^1(k_n, T/p^m T) & \longrightarrow & H^1((k_n)_p, T/p^m T) \end{array}$$

be the localization map into the semi-local cohomology at p (where the vertical isomorphisms follow from Remark 3.22). Then,

$$\mathrm{loc}_p(\kappa^{\Phi}_{\tau}) \in \mathcal{L}_n/p^m\mathcal{L}_n \subset H^1((k_n)_p, T/p^m T).$$

Proposition 3.24 will be proved below. We first remark that

$$\mathcal{L}_n/p^m\mathcal{L}_n = H^1_{\mathcal{F}_{\mathbb{L}_\infty}}((k_n)_p, T/p^m T),$$

i.e. $\mathcal{L}_n/p^m\mathcal{L}_n$ is the propagation of the local condition

$$H^1_{\mathcal{F}_{\mathbb{L}_\infty}}((k_n)_p, T) = H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k_p, \mathbb{T}/(\gamma_n - 1)\mathbb{T}) = \mathcal{L}_n \tag{18}$$

at p. We note that the first equality in (18) is explained in Remark 3.22.

Let

$$\{\tilde{\kappa}_\tau^\Phi(m,n) \in H^1((k_n)_p, T/p^mT)\}_{\tau\in\mathcal{N}_{m+n}}$$

be the collection that Rubin associates (in [Rub00, Definition IV.4.10]) to the Euler system $\{\varepsilon^\chi_{k_n(\tau),\Phi}\}_{n,\tau}$. Here we write $\tilde{\kappa}_\tau^\Phi(m,n)$ for the class which was denoted by $\kappa_{[k_n,\tau,m]}$ in [Rub00]. Since we have already fixed m and n, we can safely drop m and n from the notation and write $\tilde{\kappa}_\tau^\Phi(m,n)$ as $\tilde{\kappa}_\tau^\Phi$ when there is no danger of confusion. Note that [MR04, Appendix A, Equation (33)] relates the class $\tilde{\kappa}_\tau^\Phi$ to the class κ_τ^Φ.

Lemma 3.25. *If $\mathrm{loc}_p(\tilde{\kappa}_\tau^\Phi) \in \mathcal{L}_n/p^m\mathcal{L}_n$, then $\mathrm{loc}_p(\kappa_\tau^\Phi) \in \mathcal{L}_n/p^m\mathcal{L}_n$ as well.*

Proof. This is an obvious consequence of using [MR04, Appendix A, Equation (33)]. □

Let D_τ denote the derivative operator, defined as in [Rub00, Definition IV.4.1]. In [Rub00, Definition IV.4.10 and Remark IV.4.3], Rubin defines the class $\tilde{\kappa}_\tau^\Phi$ as the inverse image of $D_\tau\varepsilon^\chi_{k_n(\tau),\Phi} \pmod{p^m}$ under the restriction map[6]

$$H^1(k_n, T/p^mT) \longrightarrow H^1(k_n(\tau), T/p^mT)^{G^\tau}.$$

Therefore, $\mathrm{loc}_p(\tilde{\kappa}_\tau^\Phi)$ maps to $\mathrm{loc}_p(D_\tau\varepsilon^\chi_{k_n(\tau),\Phi}) \pmod{p^m}$ under the following map (which is also an isomorphism thanks to [Rub00, Remark 4.4.3, Proposition B.5.1 and Proposition B.4.2]):

$$H^1((k_n)_p, T/p^mT) \longrightarrow H^1(k_n(\tau)_p, T/p^mT)^{G^\tau}.$$

Under this isomorphism, $\mathcal{L}_n/p^m\mathcal{L}_n$ is mapped isomorphically onto the rank-one $\mathbb{Z}/p^m\mathbb{Z}\,[\Gamma_n]$-module $(\mathcal{L}_n^\tau/p^m\mathcal{L}_n^\tau)^{G^\tau}$, by the definition of $\mathcal{L}_n^\tau$ and by the fact that $\mathcal{L}_n^\tau$ is a free $\mathbb{Z}_p[G_n^\tau]$-module. The diagram below summarizes the discussion in this paragraph.

$$\begin{array}{ccc} H^1((k_n)_p, T/p^mT) & \xrightarrow{\sim} & H^1(k_n(\tau)_p, T/p^mT)^{G^\tau} \\ \uparrow & & \uparrow \\ \mathcal{L}_n/p^m\mathcal{L}_n & \xrightarrow{\sim} & (\mathcal{L}_n^\tau/p^m\mathcal{L}_n^\tau)^{G^\tau} \end{array}$$

Proposition 3.26. *If Φ satisfies $\mathrm{H}_\mathbb{L}$, then $\mathrm{loc}_p(\tilde{\kappa}_\tau^\Phi) \in \mathcal{L}_n/p^m\mathcal{L}_n$.*

Proof. Since loc_p is Galois equivariant, $\mathrm{loc}_p(D_\tau\varepsilon^\chi_{k_n(\tau),\Phi}) = D_\tau\mathrm{loc}_p(\varepsilon^\chi_{k_n(\tau),\Phi})$. Furthermore,

$$\mathrm{loc}_p(\varepsilon^\chi_{k_n(\tau),\Phi}) \in \mathcal{L}_n^\tau,$$

since Φ satisfies $\mathrm{H}_\mathbb{L}$. On the other hand, by [Rub00, Lemma 4.4.2], $D_\tau\varepsilon_{k_n(\tau),\Phi} \pmod{p^m}$ is fixed by G^τ, which in turn implies that

$$\mathrm{loc}_p(\varepsilon^\chi_{k_n(\tau),\Phi}) \pmod{p^m} \in (\mathcal{L}_n^\tau/p^m\mathcal{L}_n^\tau)^{G^\tau}.$$

This proves that $\mathrm{loc}_p(\tilde{\kappa}_\tau^\Phi)$ belongs to $\mathcal{L}_n/p^m\mathcal{L}_n$ by the discussion above. □

Proof of Proposition 3.24. This is immediate from Lemma 3.25 and Proposition 3.26. □

By the discussion following the statement of Theorem 3.23, this also completes the proof of Theorem 3.23.

[6] Note that $(\mu_{p^\infty} \otimes \chi^{-1})^{G_{k_n(\tau)}}$ is trivial since, for example, the complex conjugation cannot act by χ on μ_{p^∞}, as χ is an even character. This proves that the restriction map in question is an isomorphism, by [Rub00, Remark 4.4.3].

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press

4. Applications to the main conjectures

Assume throughout this section that the finite set of places S of k does not contain any non-archimedean prime which splits completely in L/k. Suppose that the hypotheses (A1)–(A3) hold, as well as the Rubin–Stark conjecture. In this section we assume, in addition, that Leopoldt's conjecture is true; see Remark 4.1 for a discussion concerning this assumption. Let

$$\{\phi_n^\tau\}_{n,\tau} = \Phi_0^{(\infty)} \in \bigwedge^{r-1} \mathbf{Hom}(\mathbb{V}, \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{M}/k)]])$$

be as in § 3.3 (recall that we write ϕ_n for ϕ_n^τ when $\tau = 1$, and that we set $\phi_\infty = \{\phi_n\}$), and let

$$\boldsymbol{\kappa}^{\Phi_0^{(\infty)}} = \{\kappa_\tau^{\Phi_0^{(\infty)}}\}_\tau \in \overline{\mathbf{KS}}(\mathbb{T}, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P})$$

be the Λ-adic Kolyvagin system of $\Phi_0^{(\infty)}$-Stark elements (introduced in § 3.4).

In [Buy09] an explicit generator was determined, which descends from the Euler systems of Stark elements, for the cyclic $\mathbb{Z}_p$-module of Kolyvagin systems $\overline{\mathbf{KS}}(T, \mathcal{F}_\mathcal{L}, \mathcal{P})$. Following [Buy09], we denote this generator by $\kappa^{\Phi_0} = \{\kappa_\tau^{\Phi_0}\}$, where $\Phi_0 \in \varprojlim_\tau \bigwedge^{r-1} \mathrm{Hom}_{\mathbb{Z}_p[G^\tau]}(H^1(k(\tau)_p, T), \mathbb{Z}_p[G^\tau])$ is a certain element that was used in [Buy09] and which we also recalled in § 3.3.

Remark 4.1.

(i) As in [Buy09, § 3], we use Leopoldt's conjecture to ensure that the Kolyvagin system $\kappa^{\Phi_0} \in \overline{\mathbf{KS}}(T, \mathcal{F}_\mathcal{L}, \mathcal{P})$ is *primitive* (in particular, non-trivial). Aside from Proposition 2.12 and Corollary 2.13, this is our only reason for assuming Leopoldt's conjecture.

(ii) By Remark 3.3 and Theorem 2.19, what we call κ^{Φ_0} here differs from what [Buy09] called κ^{Φ_0} by a unit $u \in \mathbb{Z}_p^\times$, where u is as in Remark 3.3. We remind the reader that this difference is due to the fact that we use Rubin–Stark elements $\{\varepsilon_K^\chi\}_{K\in\mathcal{K}}$ in this paper to construct Euler systems, whereas [Buy09] used the Rubin–Stark elements $\{\tilde{\varepsilon}_K^\chi\}_{K\in\mathcal{K}}$. Since κ^{Φ_0} of [Buy09] is a primitive Kolyvagin system, it follows that the κ^{Φ_0} appearing in this paper is a primitive Kolyvagin system as well.

It is clear from our construction that $\boldsymbol{\kappa}^{\Phi_0^{(\infty)}}$ maps to the element κ^{Φ_0} under the surjective map

$$\overline{\mathbf{KS}}(\mathbb{T}) := \overline{\mathbf{KS}}(\mathbb{T}, \mathcal{F}_{\mathbb{L}_\infty}, \mathcal{P}) \twoheadrightarrow \overline{\mathbf{KS}}(T, \mathcal{F}_\mathcal{L}, \mathcal{P}) =: \overline{\mathbf{KS}}(T).$$

Proposition 4.2. *The Λ-adic Kolyvagin system of $\Phi_0^{(\infty)}$-Stark elements $\kappa^{\Phi_0^{(\infty)}}$ is Λ-primitive, in the sense of [MR04, Definition 5.3.9].*

Proof. Let $\overline{T}$ be the residual representation $\mathbb{T}/\mathcal{M}\mathbb{T} = T/pT$. For $\boldsymbol{\kappa} \in \overline{\mathbf{KS}}(\mathbb{T})$ (respectively, $\kappa \in \overline{\mathbf{KS}}(T)$), let $\overline{\boldsymbol{\kappa}}$ (respectively, $\overline{\kappa}$) denote the image of $\boldsymbol{\kappa}$ (respectively, κ) under the map $\overline{\mathbf{KS}}(\mathbb{T}) \to \mathbf{KS}(\overline{T})$ (respectively, the map $\overline{\mathbf{KS}}(T) \to \mathbf{KS}(\overline{T})$). Since $\boldsymbol{\kappa}^{\Phi_0^{(\infty)}}$ maps to the element κ^{Φ_0} under the map $\overline{\mathbf{KS}}(\mathbb{T}) \to \overline{\mathbf{KS}}(T)$, it is clear that $\overline{\boldsymbol{\kappa}}^{\Phi_0^{(\infty)}} = \overline{\kappa}^{\Phi_0}$, so from now on we shall write $\overline{\kappa}$ for both. Since κ^{Φ_0} is primitive,[7] it follows from [MR04, Definition 4.5.5 and Theorem 5.2.10(ii)] that $\overline{\kappa} \neq 0$. This proves that the image of $\boldsymbol{\kappa}^{\Phi_0^{(\infty)}}$ under the map $\overline{\mathbf{KS}}(\mathbb{T}) \to \overline{\mathbf{KS}}(\mathbb{T}/\mathfrak{p}\mathbb{T})$ is non-zero

[7] We remark that our definition of a primitive Kolyvagin system is *a priori* different from [MR04, Definition 4.5.5] of Mazur and Rubin. However, [MR04, Theorem 5.2.10(ii)] shows that these two definitions are, in fact, equivalent.

for any height-one prime $\mathfrak{p} \subset \Lambda$, since we have a commutative diagram

$$\begin{array}{ccccc} \boldsymbol{\kappa}^{\Phi_0^{(\infty)}} & \in & \overline{\mathbf{KS}}(\mathbb{T}) & \searrow & \\ \big\downarrow & & \big\downarrow & & \overline{\mathbf{KS}}(\mathbb{T}/\mathfrak{p}\mathbb{T}) \\ \overline{\kappa} & \in & \mathbf{KS}(\overline{T}) & \swarrow & \end{array}$$

and $\overline{\kappa} \neq 0$. □

Let $\mathrm{char}(\mathbb{A})$ denote the characteristic ideal of a torsion Λ-module $\mathbb{A}$, and recall that $A^\vee$ denotes the Pontryagin dual of an abelian group A. The main application of the (Λ-primitive) Kolyvagin system $\boldsymbol{\kappa}^{\Phi_0^{(\infty)}}$ is the following.

Theorem 4.3. *We have*

$$\mathrm{char}(H^1_{\mathcal{F}^*_{\mathbb{L}_\infty}}(k, \mathbb{T}^*)^\vee) = \mathrm{char}(H^1_{\mathcal{F}_{\mathbb{L}_\infty}}(k, \mathbb{T})/\Lambda \cdot \kappa_1^{\Phi_0^{(\infty)}})$$

Proof. This follows from Theorem 2.20 and Proposition 4.2. □

Corollary 2.13 and Theorem 4.3 (applied with $c = \kappa_1^{\Phi_0^{(\infty)}}$) imply the following.

Corollary 4.4. *We have*

$$\mathrm{char}(H^1_{\mathcal{F}^*_{\mathrm{str}}}(k, \mathbb{T}^*)^\vee) = \mathrm{char}(\mathbb{L}_\infty/\Lambda \cdot \kappa_1^{\Phi_0^{(\infty)}}).$$

Remark 4.5. We know *a priori* only that

$$\varepsilon^\chi_{k_n(\tau)} \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \bigwedge^r H^1(k_n(\tau), T).$$

Let $\mathrm{loc}_p^{(r)}$ denote the map

$$\bigwedge^r H^1(k_n(\tau), T) \longrightarrow \bigwedge^r H^1((k_n(\tau))_p, T) \cong \bigwedge^r V^\chi_{L_n(\tau)},$$

so that

$$\mathrm{loc}_p^{(r)}(\varepsilon^\chi_{k_n(\tau)}) \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \bigwedge^r V^\chi_{L_n(\tau)}.$$

The defining (integrality) property of the Rubin–Stark elements gives the following.

Consequence. *For any*

$$\psi_1 \wedge \psi_2 \wedge \cdots \wedge \psi_r = \psi \in \bigwedge^r \mathrm{Hom}(V^\chi_{L_n(\tau)}, \mathbb{Z}_p[G^\tau_n]),$$

we have

$$\psi(\mathrm{loc}_p^{(r)}(\varepsilon^\chi_{k_n(\tau)})) \in \mathbb{Z}_p[G^\tau_n],$$

where we still use ψ to denote the map on $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \bigwedge^r V^\chi_{L_n(\tau)}$ induced from ψ.

On the other hand, we know (by Corollary 3.11) that the $\mathbb{Z}_p[G^\tau_n]^\chi$-module $V^\chi_{L_n(\tau)}$ is free of rank r, hence the consequence above implies that $\mathrm{loc}_p^{(r)}(\varepsilon^\chi_{k_n(\tau)}) \in \bigwedge^r V^\chi_{L_n(\tau)}$. (This has already been pointed out in [Rub96, Example 1 following Proposition 1.2].)

Let $\mathbf{c}^{\mathrm{stark}}_{k_\infty} \in \bigwedge^r H^1(k_p, \mathbb{T})$ be the image of the element

$$\{\varepsilon^\chi_{k_n}\}_n \in \varprojlim_n \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \bigwedge^r H^1(k_n, T) \xrightarrow{\mathrm{loc}_p^{(r)}} \varprojlim_n \bigwedge^r H^1((k_n)_p, T) \overset{(3.19)}{\cong} \bigwedge^r H^1(k_p, \mathbb{T})$$

under the localization-at-p map $\mathrm{loc}_p^{(r)}$ composed with the isomorphism from Remark 3.19. This is the element which showed up in the statement of Theorem A in § 1.2.

The homomorphism $\phi_\infty = \{\phi_n\}$ maps $\bigwedge^r H^1(k_p, \mathbb{T})$ isomorphically onto $\mathbb{L}_\infty$ by Remark 3.19, and maps the element $\mathbf{c}_{k_\infty}^{\mathrm{stark}} \in \bigwedge^r H^1(k_p, \mathbb{T})$ to the class $\kappa_1^{\Phi_0^{(\infty)}} \in \mathbb{L}_\infty$ by construction. We therefore conclude that

$$\bigwedge^r H^1(k_p, \mathbb{T})/\Lambda \cdot \mathbf{c}_{k_\infty}^{\mathrm{stark}} \cong \mathbb{L}_\infty/\Lambda \cdot \kappa_1^{\Phi_0^{(\infty)}},$$

which, combined with Corollary 4.4, implies the following.

Corollary 4.6. *We have*

$$\mathrm{char}(H^1_{\mathcal{F}^*_{\mathrm{str}}}(k, \mathbb{T}^*)^\vee) = \mathrm{char}\bigg(\bigwedge^r H^1(k_p, \mathbb{T})/\Lambda \cdot \mathbf{c}_{k_\infty}^{\mathrm{stark}}\bigg).$$

Using the explicit description of the Galois cohomology groups in question (cf. [Rub00, § I.6.3]), one may identify $H^1_{\mathcal{F}^*_{\mathrm{str}}}(k, \mathbb{T}^*)^\vee$ with $\mathrm{Gal}(M_\infty/L_\infty)^\chi$, 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 $\mathcal{L}_k^\chi$ denote (an appropriate normalization of) the Deligne–Ribet [DR80] p-adic L-function attached to the character χ. As a consequence of the work of Wiles [Wil90], we deduce the following.

Theorem 4.7. *The* Λ*-module* $\mathrm{char}(\bigwedge^r H^1(k_p, \mathbb{T})/\Lambda \cdot \mathbf{c}_{k_\infty}^{\mathrm{stark}})$ *is generated by* $\mathcal{L}_k^\chi$.

It would be very desirable to prove Theorem 4.7 without appealing to [Wil90] and, therefore, obtain a proof of the 'main' conjecture. It seems that this is feasible: the statement of Theorem 4.7 is very much in the spirit of [Col98, Per94a, Per94b, Per95]; and when $k = \mathbb{Q}$ (i.e. when $r = 1$), Theorem 4.7 is a classical result of Iwasawa [Iwa64]. Note that the Stark elements are obtained from the cyclotomic units when $k = \mathbb{Q}$. One key observation that we mention here is that the cyclotomic units demonstrate the complex Stark conjecture and the p-adic Stark conjecture (see [Sol02, Sol04] for Solomon's version of the p-adic Stark conjecture) simultaneously. However, it would not be reasonable to expect to prove Theorem 4.7 using *only* the properties of the Rubin–Stark elements (which are solutions to the Rubin–Stark conjecture for the complex L-functions), since Rubin's conjecture only predicts the values of a certain *complex*-valued regulator evaluated at these elements. In fact, it is plausible that one would also need to utilize the solutions to an appropriate p-adic Stark conjecture.

In a sequel to this paper, we hope to discuss the relation between the solutions to the complex and p-adic Stark conjectures via the rigidity offered by Theorem 2.19, and prove Theorem 4.7 without assuming Wiles' work, thus deducing the main conjectures. One big obstacle with which the author is faced is the lack of an *integral* p-adic Stark conjecture (at either $s = 1$ or $s = 0$) along the cyclotomic $\mathbb{Z}_p$-tower.

Nevertheless, Theorem 4.7 is true, and this fact already hints at a relation between the solutions of the complex and p-adic Stark conjectures. This relation should be understood as an analogy to the fact that the cyclotomic units give solutions to both the complex Stark conjecture and the p-adic Stark conjecture (when $k = \mathbb{Q}$).

Acknowledgements

It is a pleasure to thank Karl Rubin, Christian Popescu and David Solomon for their comments, suggestions and encouragement. The author also thanks Qéndrim Gashi and the anonymous referee for suggestions that have helped to improve the exposition.

Appendix A. Local conditions at p over an Iwasawa algebra via the theory of (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 $H^1(k_n(\tau)_p, T)$ in § 3.3. This probably could have been achieved without appealing to the theory of (φ, Γ)-modules; however, this very general approach may be of help in generalizing the methods of this paper for application to many other settings.

Throughout this appendix, let K denote a finite extension of $\mathbb{Q}_p$ and set $\tilde{K}_n := K(\mu_{p^n})$ and $\tilde{K}_\infty := \bigcup_n \tilde{K}_n$. Define the Galois groups $\tilde{H}_K := \mathrm{Gal}(\overline{K}/\tilde{K}_\infty)$ and $\tilde{\Gamma}_K := G_K/\tilde{H}_K = \mathrm{Gal}(\tilde{K}_\infty/K)$. 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 $\mathrm{Gal}(\tilde{K}_\infty/\tilde{K}_n) := \tilde{\Gamma}^{(n)}$ for $n \in \mathbb{Z}^+$, which is chosen in such 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

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

where W is a finite group whose order is prime to p. (In fact, W can be identified with $\mathrm{Gal}(K(\mu_p)/K)$.) 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 introduced the notion of a (φ, Γ)-module over a certain period ring,[8] 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 here a detailed discussion of these objects, and instead refer the reader to [Fon90, A.3.1–3.2] for the definitions and 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 as follows.

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

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

[8] However, one should be cautious, as Fontaine's K_n is our $\tilde{K}_n$, etc. For instance, his Γ_K is our $\tilde{\Gamma}_K$.

Suppose that 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 (see [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[9]

$$\psi : \mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}} \longrightarrow \mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}},$$

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

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

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

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

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

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

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

by the Hochschild–Serre spectral sequence.

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

[9] This definition makes sense because $\mathrm{Tr}_{\widehat{\varepsilon^{\mathrm{nr}}}/\varphi(\widehat{\varepsilon^{\mathrm{nr}}})}(\mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}}) \subset p\mathcal{O}_{\widehat{\varepsilon^{\mathrm{nr}}}}$ and φ is injective.

PROPOSITION A.4. *Define $\tau_n := 1 + \tilde{\gamma}_{n-1} + \cdots + \tilde{\gamma}_{n-1}^{p-1} \in \mathbb{Z}_p[[\tilde{\Gamma}_K]]$. Then there is the following 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. □

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

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

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

Remark A.6. The isomorphism

$$\exp^* : H^1_{\tilde{\mathrm{Iw}}}(K, T) \xrightarrow{\sim} D(T)^{\psi=1}$$

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 that 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

$$0 \longrightarrow D(T)^{\varphi=1} \longrightarrow D(T)^{\psi=1} \xrightarrow{\varphi-1} \mathcal{C}(T) \longrightarrow 0. \tag{A1}$$

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

If we now take the W-invariance of the exact sequence (A1) (making use of 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 obtain the following result.

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press

Theorem A.8 (Cherbonnier and Colmez [CC99]).

(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 D. Benois, *On Iwasawa theory of crystalline representations*, Duke Math. J. **104** (2000), 211–267.

Buy07 K. Büyükboduk, *Λ-adic Kolyvagin systems*, Preprint (2007), http://arxiv.org/abs/0706.0377v1.

Buy08 K. Büyükboduk, *Stickelberger elements and Kolyvagin systems*, Preprint (2008), http://arxiv.org/abs/0808.2588.

Buy09 K. Büyükboduk, *Kolyvagin systems of Stark units*, J. Reine Angew. Math. **631** (2009), 85–107.

CC99 F. Cherbonnier and P. Colmez, *Théorie d'Iwasawa des représentations p-adiques d'un corps local*, J. Amer. Math. Soc. **12** (1999), 241–268.

Col79 R. F. Coleman, *Division values in local fields*, Invent. Math. **53** (1979), 91–116.

Col98 P. Colmez, *Théorie d'Iwasawa des représentations de de Rham d'un corps local*, Ann. of Math. (2) **148** (1998), 485–571.

DR80 P. Deligne and K. A. Ribet, *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. **59** (1980), 227–286.

deS87 E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication: p-adic L functions*, Perspectives in Mathematics, vol. 3 (Academic Press, Boston, MA, 1987).

Fon90 J.-M. Fontaine, *Représentations p-adiques des corps locaux. I*, in *The Grothendieck Festschrift, Vol. II*, Progress in Mathematics, vol. 87 (Birkhäuser, Boston, MA, 1990), 249–309.

Gre94 R. Greenberg, *Trivial zeros of p-adic L-functions*, in *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, Contemporary Mathematics, vol. 165 (American Mathematical Society, Providence, RI, 1994), 149–174.

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

Her01 L. Herr, *Une approche nouvelle de la dualité locale de Tate*, Math. Ann. **320** (2001), 307–337.

Iwa64 K. Iwasawa, *On some modules in the theory of cyclotomic fields*, J. Math. Soc. Japan **16** (1964), 42–82.

Kra39 M. Krasner, *Sur la représentation exponentielle dans les corps relativement galoisiens de nombers* $\mathfrak{p}$*-adiques*, Acta Arith. **3** (1939), 133–173.

Mil86 J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1 (Academic Press, Boston, MA, 1986).

MR04 B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799.

MTT86 B. Mazur, J. Tate and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1–48.

Per94a B. Perrin-Riou, *La fonction L p-adique de Kubota-Leopoldt*, in *Arithmetic geometry (Tempe, AZ, 1993)*, Contemporary Mathematics, vol. 174 (American Mathematical Society, Providence, RI, 1994), 65–93.

Per94b B. Perrin-Riou, *Théorie d'Iwasawa des représentations p-adiques sur un corps local* (With an appendix by Jean-Marc Fontaine), Invent. Math. **115** (1994), 81–161.

Per95 B. Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques*, Astérisque, vol. 229 (Société Mathématique de France, Paris, 1995).

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press

Per98 B. Perrin-Riou, *Systèmes d'Euler p-adiques et théorie d'Iwasawa*, Ann. Inst. Fourier (Grenoble) **48** (1998), 1231–1307.

Rub92 K. Rubin, *Stark units and Kolyvagin's 'Euler systems'*, J. reine angew. Math. **425** (1992), 141–154.

Rub96 K. Rubin, *A Stark conjecture 'over* **Z***' for abelian L-functions with multiple zeros*, Ann. Inst. Fourier (Grenoble) **46** (1996), 33–62.

Rub00 K. Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147 (Princeton University Press, Princeton, NJ, 2000).

Sol02 D. Solomon, *On p-adic abelian Stark conjectures at* $s = 1$, Ann. Inst. Fourier (Grenoble) **52** (2002), 379–417.

Sol04 D. Solomon, *Abelian conjectures of Stark type in* $\mathbb{Z}_p$*-extensions of totally real fields*, in *Stark's conjectures: recent work and new directions*, Contemporary Mathematics, vol. 358 (American Mathematical Society, Providence, RI, 2004), 143–178.

Wil90 A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. (2) **131** (1990), 493–540.

Kâzım Büyükboduk kazim@math.stanford.edu
Department of Mathematics, Stanford University, Stanford, CA 94305, USA

Current address: Institut des Hautes Études Scientifiques Le Bois-Marie, 35 route de Chartres, 91440 Bures-sur-Yvette, France

https://doi.org/10.1112/S0010437X09004163 Published online by Cambridge University Press