TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 370, Number 2, February 2018, Pages 927–966
http://dx.doi.org/10.1090/tran/7029
Article electronically published on August 3, 2017

ON THE IWASAWA THEORY OF CM FIELDS FOR SUPERSINGULAR PRIMES

KÂZIM BÜYÜKBODUK

ABSTRACT. The goal of this article is two-fold: First, to prove a (two-variable) main conjecture for a CM field F without assuming the p-ordinary hypothesis of Katz, making use of what we call the Rubin-Stark $\mathcal{L}$-restricted Kolyvagin systems, which is constructed out of the conjectural Rubin-Stark Euler system of rank g. (We are also able to obtain weaker unconditional results in this direction.) The second objective is to prove the Park-Shahabi plus/minus main conjecture for a CM elliptic curve E defined over a general totally real field again using (a twist of the) Rubin-Stark Kolyvagin system. This latter result has consequences towards the Birch and Swinnerton-Dyer conjecture for E.

CONTENTS

1. INTRODUCTION

Let F be a CM field and suppose $[F : \mathbb{Q}] = 2g$. In the particular case when F is an imaginary quadratic field, the main conjectures of Iwasawa theory over F have been settled in [Rub91] using elliptic units. For a general CM field F, all major work related to Iwasawa's main conjecture utilized congruences of modular forms (and have relied on the CM-form method in [HT93, HT94] or the Eisenstein ideal technique in [Mai08, Hsi12]) as the main tool. That approach required that

Received by the editors December 27, 2013, and, in revised form, October 30, 2014, and May 12, 2016.

2010 *Mathematics Subject Classification.* Primary 11G05, 11G07, 11G40, 11R23, 14G10.

Key words and phrases. Iwasawa theory, Iwasawa's main conjectures, Rubin-Stark elements.

This work was partially supported by Marie Curie IRG grant EC-FP7 230668, TÜBİTAK grant 113F059, EU Horizon 2020 MC-GF Grant CriticalGZ/745691, and the Turkish Academy of Sciences.

the following p-ordinary condition (1.1) of Katz holds true. Fix an embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

(1.1) There exists a CM-type Σ such that the embeddings $\Sigma_p := \{\iota_p \circ \sigma\}_{\sigma\in\Sigma}$ induce exactly half of the places of F over p.

Let $\widetilde{F}_\infty$ denote the maximal $\mathbb{Z}_p$-power extension of F and set $\widetilde{\Gamma} = \mathrm{Gal}(\widetilde{F}_\infty)/F$. Let $\widetilde{\Lambda} = \mathcal{W}[[\widetilde{\Gamma}]]$, where $\mathcal{W}$ is the valuation ring of $\widehat{\overline{\mathbb{Q}}}_p$. Assuming (1.1), the relevant Iwasawa module $\widetilde{\mathfrak{X}}_\Sigma$ is $\widetilde{\Lambda}$-torsion, and Katz in [Kat78] has constructed a p-adic L-function $\mathcal{L}_\Sigma \in \widetilde{\Lambda}$. In this case, Hsieh in [Hsi12] proved that the characteristic ideal of $\widetilde{\mathfrak{X}}_\Sigma$ is generated by $\mathcal{L}_\Sigma$ under a suitable hypothesis, thereby proving the Iwasawa main conjecture for F. The author has also obtained results along these lines in [Büy14] using the conjectural Rubin-Stark elements. The approach in [Büy14] is based on a refinement of the rank-g Euler/Kolyvagin system machinery and relies crucially on the assumption (1.1) for an analysis of the local cohomology groups above p.

All these techniques towards the proof of main conjectures for a general CM field F alluded to above fall apart when the p-ordinary condition (1.1) fails. One difficulty is that in the absence of (1.1), neither the relevant Iwasawa module is $\widetilde{\Lambda}$-torsion nor do we have a p-adic L-function available in this setup (in any case, it is not expected to belong to $\widetilde{\Lambda}$). Beyond the case $g = 1$, nothing substantial along these lines was known; when $g = 1$ Rubin has proved the two-variable main conjecture in [Rub91]. Furthermore (still when $g = 1$), if $A/\mathbb{Q}$ is an elliptic curve that has CM by the ring of integers $\mathcal{O}_F$ of F, Kobayashi in [Kob03] formulated a pair of conjectures which are both equivalent to the cyclotomic main conjectures of Perrin-Riou and Kato [PR93, Kat04] for A. Pollack and Rubin in [PR04] proved Kobayashi's conjectures using Rubin's proof of the two-variable main conjecture in [Rub91] and incorporating Kobayashi's theory of plus/minus Selmer groups with the elliptic unit Euler system.

The goal of this article is to appropriately modify and extend the methods of [Büy14] so as to prove (conditional on some standard conjectures):

- a two-variable main conjecture for a general CM field F in the absence of the hypothesis (1.1) using the (conjectural) Rubin-Stark elements (this is Theorem A below);
- a divisibility in the (one-variable) *cyclotomic* main conjecture for a p-supersingular CM elliptic curve defined over a general totally real field (this is Theorem B below);
- prove that the divisibility in the previous item may be upgraded to an equality using the structure of the module of Λ-adic Kolyvagin systems, as described in [Büy16] (we provide a detailed account of this in Section 4 below).

Notation. Before we explain our results in greater detail, we set some notation. Let E be an elliptic curve defined over a totally real field F^+, which has CM by an order $\mathcal{O}$ of an imaginary quadratic field K. Let $g := [F^+ : K]$ and let $F = F^+K$ be the composite CM field. Fix once and for all an odd prime p that is coprime to the index $[\mathcal{O}_K : \mathcal{O}]$ of $\mathcal{O}$ inside the maximal order $\mathcal{O}_K$ and which is inert in $K/\mathbb{Q}$. We denote the unique prime of K above p also by p and we denote the completion K_p by Φ. We let $\mathfrak{O}$ denote the ring of integers of Φ.

Let K_∞ denote the unique $\mathbb{Z}_p^2$-extension of K and K^{cyc} the cyclotomic $\mathbb{Z}_p$-extension. Let $F_\infty = FK_\infty$ and $F^{\mathrm{cyc}} = FK^{\mathrm{cyc}}$. Let $\Gamma = \mathrm{Gal}(F_\infty/F)$ and $\Gamma_{\mathrm{cyc}} = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$. We define the two-variable (resp., one-variable) Iwasawa algebra $\Lambda := \mathfrak{O}[[\Gamma]]$ (resp., $\Lambda_{\mathrm{cyc}} := \mathfrak{O}[[\Gamma_{\mathrm{cyc}}]]$). For a Dirichlet character $\chi : \mathrm{Gal}(\overline{F}/F) \to \mathfrak{O}^\times$, let L denote the extension of F cut by χ and let $\mathfrak{U}$ denote the inverse limit of the χ-isotypic part of the local units up the tower of finite extensions contained in LF_∞/L. Let $\mathcal{Q}$ denote a certain quotient of $\mathfrak{U}$ (see Definition 2.17) and let $\Lambda \cdot \mathrm{loc}_{/V}(\varepsilon^{\chi}_{F_\infty})$ denote the submodule of $\wedge^g \mathcal{Q}$ generated by the image of the tower of Rubin-Stark elements (defined as in Definition 5.8). Let $\widehat{X}_\infty$ be a certain Iwasawa module (denoted by $H^1_{\mathcal{F}^*_{\mathfrak{tr}}}(F, \mathbb{T}^*)^\vee$ in the main text, which is given as in Definition 2.20). *Assume the truth of Rubin-Stark conjectures and Leopoldt's conjecture for Theorems A, B and C below.* See Remarks 1.1 and 1.2 below for the portion of the results in this article that we are able to prove unconditionally.

Statements of the results. The first main result in this article is the (two-variable)[1] Iwasawa main conjecture for F_∞/F. Let $\mathrm{char}(M)$ denote the characteristic ideal of a finitely generated torsion Λ-module.

Theorem A (See Theorems 5.6 and 5.9). *The Λ-module $\widehat{X}_\infty$ is torsion and* $\mathrm{char}(\widehat{X}_\infty)$ *divides* $\mathrm{char}\left(\wedge^g \mathcal{Q}/\Lambda \cdot \mathrm{loc}_{/V}\left(\varepsilon^{\chi}_{F_\infty}\right)\right)$. *These two ideals are equal if we further assume a strong version of the Rubin-Stark Conjecture (Conjecture* 3.6 *below).*

This statement was proved by Rubin [Rub91, §11] when $F^+ = \mathbb{Q}$, using elliptic units. To obtain the generalization above we make use of the Rubin-Stark elements. To do so, the CM *rank-g Euler/Kolyvagin system machinery* developed by the author in [Büy14] (relying crucially on the p-ordinary hypothesis (1.1)) requires a non-trivial refinement. This is one of the major tasks we carry out in this article.

For the rest of our results, we assume that the prime p splits completely in $F^+/\mathbb{Q}$. This assumption could be removed (but allowing also only weaker results); see Remark 1.3 below. Thanks to this assumption we may adopt the (local) methods of Kobayashi [Kob03] and define the signed Selmer groups $\mathrm{Sel}_p^{\pm}(E/F^{\mathrm{cyc}})$. In this situation, we are led to formulate a (conjectural) explicit reciprocity law for the Rubin-Stark elements; see Conjecture 6.16. This conjecture on one hand proposes a natural extension of the Coates-Wiles explicit reciprocity law and, on the other, it furnishes us with a link between the tower of Rubin-Stark elements and the Park-Shahabi signed p-adic L-functions $L_p^{\pm}(E/F^+)$.

Theorem B gives a proof of the cyclotomic main conjecture for E for a supersingular prime p under our running assumptions.

Theorem B (Theorem 6.26). *Assuming the Explicit Reciprocity Conjecture* 6.16 *for Rubin-Stark elements, the divisibility*

$$\mathrm{char}\left(\mathrm{Sel}^{\pm}(E/F^{\mathrm{cyc}})^\vee\right) \mid L_p^{\pm}(E/F^+)\,\Lambda_{\mathrm{cyc}}$$

in the signed main conjecture holds true, with equality if we assume a strong version of the Rubin-Stark Conjecture (Conjecture 3.6 *below).*

[1] Since our sights are mainly set on the proof of the cyclotomic main conjecture for CM elliptic curves over F^+ (that is, Theorem B below), we content ourselves to prove only a two-variable supersingular main conjecture over F. However, the methods of this article seem flexible enough to treat the more general case and prove a more general main conjecture (e.g., over the maximal $\mathbb{Z}_p$-power extension $\widetilde{F}_\infty/F$).

We remark that we do not descend from the two-variable main conjecture in order to deduce Theorem B (as done so in [PR04]), but instead, we rely further on the author's results on the structure of the module of Λ-adic Kolyvagin systems. This alternative approach has the advantage that we need not worry about pseudo-null submodules of various Iwasawa modules.

Remark 1.1. Although the existence of the Rubin-Stark elements is highly conjectural, one may prove (Theorem 4.1 below) that the Kolyvagin systems that they descend from do exist *unconditionally.* Notice also that the Kolyvagin systems which descend from the conjectural Rubin-Stark elements are non-trivial, since we assumed Leopoldt's conjecture (cf. Proposition 4.9). One may work with these Kolyvagin systems for the most part to prove statements which lead to Theorems A and B (Theorem 4.2 and Proposition 4.4). However, the Reciprocity Conjecture 6.16 that links the Kolyvagin systems we construct with the L-values could be stated most naturally in terms of the conjectural Rubin-Stark elements.

Theorem B has the following important consequence towards the conjecture of Birch and Swinnerton-Dyer for the CM elliptic curve $E_{/F^+}$.

Theorem C (Theorem 6.27 below)**.**

(1) *If* $L(E/F^+, 1) \neq 0$*, then* $E(F^+)$ *is finite.*
(2) *Assuming the strong form of the Rubin-Stark Conjecture as well as that* $L(E/F^+, 1) = 0$*, then* $\mathrm{Sel}_p(E/F^+)$ *is infinite.*

Remark 1.2. It seems very plausible that the methods of this paper would allow us to deduce Theorems A, B and C above *unconditionally* under the additional hypothesis that $F^+(E[p])/K$ is abelian. The idea goes roughly as follows (we hope to provide the details in a future note): Firstly, by the assumption that $F^+(E[p])/K$ is abelian, one may use elliptic units to construct classes in $H^1(F, T_p(E) \otimes \Lambda)$. We may use the main theorem of [Büy11] to lift these classes to a Λ-adic Kolyvagin system (for certain *modified Selmer structures* which are defined in Section 2 below) for the G_F-representation $T_p(E)$, so as to view these classes (obtained from elliptic units) as the initial terms of this Λ-adic Kolyvagin system. Using this Λ-adic Kolyvagin system (whose initial term is explicitly given in terms of elliptic units), one could deduce Theorems A, B and C unconditionally.

Remark 1.3. The first version of this article was circulated among experts back in early 2013, and it later became the main motivation and the groundwork for our forthcoming joint work with Antonio Lei [BL15]. In [BL15], we are able extend some of the results of this paper to treat a CM abelian variety of arbitrary dimension. This work in part relies on the techniques developed here, as well as a general theory of plus/minus Coleman maps we develop in [BL17]. Although in [BL15], the authors are able to lift the hypotheses on Theorems B and C that p splits completely in $F^+/\mathbb{Q}$, they are able to deduce only one of the signed main conjectures (whereas we prove both main conjectures simultaneously here). Note that we could have also formulated 2^g signed main conjectures (as opposed to a single plus/minus main conjecture) here as well by assigning one of the "plus" or "minus local conditions" at each prime lying above p (as opposed to assigning the "plus" or "minus local condition" everywhere above p uniformly) and prove each of them.

One further advantage of the more explicit approach we take here (namely, through Kobayashi's interpretation of signed Coleman maps, which in turn rely on his explicit local elements) is that it allows us to state our explicit reciprocity conjectures in a much more concrete form. We hope that this will allow us to verify the explicit reciprocity conjectures (and therefore deduce our main results here unconditionally) in the situation of Remark 1.2, namely, when $F^+(E[p])/K$ is abelian. For the time being, this does not seem tractable in the rather abstract setup of [BL15].

Overview of the methods and layout of the paper. We briefly outline the basic technical ingredients that go into the proofs of Theorems A, B and C.

In order to prove the two-variable main conjecture (Theorem A) we use the Rubin-Stark element Euler system of rank g. This requires us to refine the *rank-g Euler/Kolyvagin system machinery* in the supersingular setting where the assumption (1.1) is no longer valid. The first step is to introduce various *modified Selmer structures* (Section 2) that produce Selmer groups that compare well with their classical counterparts. We construct and study in Section 4 the Kolyvagin systems associated to these modified Selmer structures. We in fact do this first unconditionally, then in Section 4.1 using the Rubin-Stark elements (recalled briefly in Section 3). These Kolyvagin systems are then used in Section 5 (along with the arguments of Section 2.5 to compare the modified Selmer groups (that we control by the Rubin-Stark Kolyvagin systems) to the classical Selmer groups) to prove the divisibility statement in Theorem A. We then show that this divisibility may be upgraded to an equality by exploiting our results in Section 4 on the structure of Λ-adic Kolyvagin systems.

To deduce Theorem B (the cyclotomic main conjecture for a CM elliptic curve E for a supersingular prime p) we appeal to Kobayashi's local theory, with which we directly apply the Kolyvagin system machinery developed in Section 4. This is one of the main differences with the approach in [PR04], which ultimately relies on various explicit calculations with elliptic units which are not at our disposal. We get around this issue by systematically utilizing our results on the modules of Kolyvagin systems. Kobayashi's plus/minus Selmer groups (and the corresponding pair of p-adic L-functions of Park-Shahabi) are recalled in Sections 6.1 and 6.2. The Explicit Reciprocity Conjecture we formulate in Section 6.3 relates the tower of Rubin-Stark elements (along F_∞) to the special values of (twisted) L-functions attached to E at $s = 1$. This conjecture should be thought of as an extension of Coates-Wiles explicit reciprocity law [CW77, Wil78] for elliptic units, and we believe that Conjecture 6.16 should be of independent interest for future investigation.

The proof of Theorem C follows from Theorem B easily. A key ingredient is a result of [NQĐ84] on the psuedo-null submodules of a natural Iwasawa module.

1.1. **Notation and hypotheses.** For any field k, let $\overline{k}$ denote a fixed separable closure of k and let $G_k = \mathrm{Gal}(\overline{k}/k)$ denote its absolute Galois group.

Throughout we fix a rational odd prime p and embeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ where $\mathbb{C}_p$ is the p-adic completion of $\overline{\mathbb{Q}}_p$. We normalize the valuation val_p and the absolute value $|\cdot|_p$ on $\mathbb{C}_p$ by assuming $\mathrm{val}_p(p) = 1$ and $|p|_p = p^{-1}$. For any positive integer n, let $\boldsymbol{\mu}_n$ denote the nth roots of unity and $\boldsymbol{\mu}_{p^\infty} = \varinjlim \boldsymbol{\mu}_{p^m}$.

Let F be a CM field and let F^+ be its maximal real subfield as in the Introduction. Let $\chi : G_F \to \mathfrak{O}^\times$ be any Dirichlet character whose order is prime to p and which has the property that

$$\chi(\wp) \neq 1 \quad \text{for any prime } \wp \text{ of } F \text{ above } p \tag{1.2}$$

and that

$$\chi \neq \omega, \tag{1.3}$$

where ω is the Teichmüller character giving the action of G_F on $\boldsymbol{\mu}_p$. Later in Section 6, we will work with a particular character χ attached to a CM elliptic curve E. We let $L := \overline{F}^{\ker \chi}$ denote the abelian extension of F cut out by χ.

Let $\mathcal{R}$ be the set of primes of F that does not contain any prime above p nor any prime at which χ is ramified. Define $\mathcal{N}(\mathcal{R})$ to be the square free products of primes chosen from $\mathcal{R}$. For $\ell \in \mathcal{R}$, let $F(\ell)$ be the maximal p-extension inside the ray class field of F modulo ℓ, and for $\eta = \ell_1 \cdots \ell_s \in \mathcal{N}(\mathcal{R})$, set $F(\eta) = F(\ell_1) \cdots F(\ell_s)$. We write $L(\eta) = L \cdot F(\eta)$ for the composite field. We consider the following collections of finite abelian extensions of F (resp., of L):

(i) $\mathfrak{T} = \{F(\eta) : \eta \in \mathcal{N}(\mathcal{R})\}$,
(ii) $\mathfrak{T}_0 = \{L(\eta) : \eta \in \mathcal{N}(\mathcal{R})\}$,
(iii) $\mathfrak{E} = \{M \cdot F(\eta) : \eta \in \mathcal{N}(\mathcal{R}); M \subset F_\infty \text{ is a finite extension of } F\}$,
(iv) $\mathfrak{E}_0 = \{M \cdot L(\eta) : \eta \in \mathcal{N}(\mathcal{R}); M \subset F_\infty \text{ is a finite extension of } F\}$.

Let $K_0(X) = \varinjlim_{N \in X_0} N$ and $K(X) = \varinjlim_{N \in X} N$ for $X = \mathfrak{T}$ or $\mathfrak{E}$. We finally set $\mathfrak{G}(\mathfrak{X}) = \mathrm{Gal}(\mathfrak{X}/F)$ and write $\mathfrak{O}[[\mathfrak{G}(\mathfrak{X})]] := \varprojlim \mathfrak{O}[\mathfrak{G}(\mathfrak{X})/U]$, where the inverse limit is over the open subgroups U of $\mathfrak{G}(\mathfrak{X})$, for the completed group ring of $\mathfrak{G}(\mathfrak{X})$.

For any non-archimedean prime λ of F, fix a decomposition group $\mathcal{D}_\lambda$ and the inertia subgroup $\mathcal{I}_\lambda \subset \mathcal{D}_\lambda$. Let $(-)^\vee = \mathrm{Hom}(-, \mathbb{Q}_p/\mathbb{Z}_p)$ denote the Pontryagin duality functor. Observe that $(-)^\vee \otimes \mathfrak{O} = \mathrm{Hom}(-, \Phi/\mathfrak{O})$. Bearing this relation in mind, we will write $X^\vee$ for $\mathrm{Hom}(X, \Phi/\mathfrak{O})$ *when X is an $\mathfrak{O}$-module.* We let $X^* := \mathrm{Hom}(X, \boldsymbol{\mu}_{p^\infty})$ denote the Cartier dual of X.

Let F_∞ and F^{cyc} be as above. Let F_n denote the unique subextension of F^{cyc}/F which has degree p^n and set $\Gamma_n = \mathrm{Gal}(F_n/F)$.

We let G_F act on Λ (resp., Λ_{cyc}) via the tautological surjection $G_F \to \Gamma$ (resp., $G_F \to \Gamma_{\mathrm{cyc}}$). For an $\mathfrak{O}$-module X of finite type which is endowed with a continuous action of G_F, we let G_F act on the Λ-module $X \otimes_{\mathfrak{O}} \Lambda$ by acting on both factors.

2. Selmer structures and comparing Selmer groups

2.1. **Structure of the semi-local cohomology groups.** Let $M = M_0 \cdot F(\eta)$ be a member of the collection $\mathfrak{E}$, where M_0 is a finite subextension of F_∞/F. Set $\Delta_M = \mathrm{Gal}(M/F)$, $\delta_M = |\Delta_M|$ and $\Lambda_M = \mathfrak{O}[\Delta_M]$.

Let X be any $\mathfrak{O}[[G_F]]$-module which is free of rank d as an $\mathfrak{O}$-module. Suppose in addition that X satisfies the following hypothesis:

(**H.p1**) $H^2(F_\wp, X) = 0 = H^2\left(F_\wp, \mathrm{Hom}_{\mathfrak{O}}(X, \mathfrak{O}(1))\right)$, for any prime $\wp$ of F above p.

Lemma 2.1. *Suppose X is as above. Let $M \in \mathfrak{E}$ be an extension of F and let $\mathfrak{P}$ be a prime of M lying above p. Then*

$$H^2(M_{\mathfrak{P}}, X) = 0 = H^2\left(M_{\mathfrak{P}}, \mathrm{Hom}_{\mathfrak{O}}(X, \mathfrak{O}(1))\right).$$

Proof. Let $\wp$ be the prime of F lying below $\mathfrak{P}$ and set $D_{\mathfrak{P}} = \mathrm{Gal}(M_{\mathfrak{P}}/F_{\wp})$. Then either $D_{\mathfrak{P}}$ is trivial, and in this case Lemma 2.1 follows from (**H.p1**), or otherwise $D_{\mathfrak{P}}$ is a non-trivial p-group. Then,

$$\#H^0(M_{\mathfrak{P}}, X^*[\varpi]) = \#H^0\big(D_{\mathfrak{P}}, (H^0(M_{\mathfrak{P}}, X^*[\varpi]))\big) \equiv \#H^0(F_{\wp}, X^*[\varpi]) \equiv 1 \mod p$$

where the last equality holds thanks to (**H.p1**) and local duality. This shows that $H^0(M_{\mathfrak{P}}, X^*) = 0$ and thus by local duality that $H^2(M_{\mathfrak{P}}, X) = 0$, as desired. The second assertion is proved in an identical manner. □

Definition 2.2. For $j = 0, 1, 2$ define the semi-local cohomology groups

$$H^j(M_p, X) := \bigoplus_{i=1}^{s} \bigoplus_{\mathfrak{q}|p} H^j(M_{\mathfrak{q}}, X),$$

and let

$$\mathrm{loc}_p : H^1(M, X) \longrightarrow H^1(M_p, X)$$

denote the localization map.

Proposition 2.3. *Suppose* (**H.p1**) *holds true.*

(i) *The corestriction map*

$$\mathrm{cor} : H^1(M_p, X) \longrightarrow H^1(F_p, X)$$

is surjective.

(ii) *The Λ_M-module $H^1(M_p, X)$ is free of rank $2g \cdot d$.*

(iii) *The Λ-module $H^1(F_p, X \otimes \Lambda)$ is free of rank $2g \cdot d$.*

(iv) *The $\mathfrak{O}[[\mathfrak{G}(\mathfrak{X})]]$-module $\varprojlim_{M \in \mathfrak{C}} H^1(M_p, X)$ is free of rank $2g \cdot d$, where the inverse limits are with respect to corestriction maps.*

Proof. (iii) and (iv) follow at once from (i) and (ii). Both (i) and (ii) are essentially proved in [Büy14, §2.1]. □

Remark 2.4. Observe that for $T = \mathfrak{O} \otimes \chi^{-1}$, the hypothesis **(H.p1)** is verified for $X = T$ since we assumed (1.2) and (1.3) as well as for $X = T(E)$, the p-adic Tate module of an elliptic curve E/F^+ with supersingular reduction at every prime of F^+ above p. In particular, the conclusions of Proposition 2.3 hold true for both choices of G_F-representations.

2.2. Modified Selmer structures for $\mathbb{G}_m$.

The constructions in this subsection and the next will be needed only for sharpening the divisibility in the cyclotomic main conjecture for the CM elliptic curve E, which we shall prove later. The reader who is content with one divisibility in the main conjecture may skip these two subsections.

Definition 2.5. Let R be any ring and M be any R-module. For any submodule $N \subset M$, the *R-saturation of N in M* is the submodule $N^{\mathrm{sat}} = \phi^{-1}\phi(N) \subset M$, where $\phi : M \to M \otimes \mathrm{Frac}(R)$ is the natural map and $\mathrm{Frac}(R)$ is the total ring of fractions of R.

Lemma 2.6. *The $\mathfrak{O}$-module $\mathcal{O}_L^{\times,\chi}$ is free of rank g.*

Proof. This follows from [NSW08, §8.6.12], along with our assumption that χ is different from the Teichmüller character ω. □

Definition 2.7.

(i) Let $\mathcal{V}_F^+ := \mathrm{loc}_p(\mathcal{O}_L^{\times,\chi})^{\mathrm{sat}}$ be the $\mathfrak{O}$-saturation of $\mathrm{loc}_p(\mathcal{O}_L^{\times,\chi})$ in $H^1(F_p,T)$. Note that the $\mathfrak{O}$-module $\mathcal{V}_F^+$ is a direct summand of the free module $H^1(F_p,T)$. Let the rank of the $\mathfrak{O}$-module $\mathcal{V}_F^+$ be $g-\mathfrak{d}$ with $\mathfrak{d}\geq 0$. Observe that $\mathfrak{d}=0$ if Leopoldt's conjecture holds true for L.

(ii) Let $\mathcal{V}_F^-$ be any free submodule of $H^1(F_p,T)$ which complements $\mathcal{V}_F^+$.

Note that $H^1(F,T)$ may be naturally identified by $L^{\times,\chi}$ by Kummer theory, and this is how we make sense of $\mathrm{loc}_p(\mathcal{O}_L^{\times,\chi})$. Furthermore, if Leopoldt's conjecture holds true for L, then $\mathcal{V}_F^+$ is the unique direct summand of $H^1(F_p,T)$ of rank g, containing $\mathrm{loc}_p(\mathcal{O}_L^{\times,\chi})$.

Definition 2.8.

(i) Let $\mathcal{V}_{K(\mathfrak{T})}^\pm$ be the direct summand of $\varprojlim_{M\in\mathfrak{T}} H^1(M_p,T)$ which maps onto $\mathcal{V}_F^\pm$ under the natural (surjective) corestriction map. Note that such a direct summand exists thanks to Proposition 2.3(i) and Nakayama's lemma. Note further that we have the direct sum decomposition
$$\varprojlim_{M\in\mathfrak{T}} H^1(M_p,T) = \mathcal{V}_{K(\mathfrak{T})}^+ \oplus \mathcal{V}_{K(\mathfrak{T})}^-.$$
.

(ii) For $M\in\mathfrak{T}$, let $\mathcal{V}_M^\pm \subset H^1(M_p,T)$ be the image of $\mathcal{V}_{K(\mathfrak{T})}^\pm$ under the natural projection.

Definition 2.9.

(i) Let $\mathfrak{L}$ be any free, rank one $\mathfrak{O}[[\mathfrak{G}(K(\mathfrak{T}))]]$-direct summand of $\mathcal{V}_{K(\mathfrak{T})}^+$.

(ii) For $M\in\mathfrak{T}$, let $\mathfrak{l}_M \subset \mathcal{V}_M^+$ be the image of $\mathfrak{L}$ under the natural projection $\varprojlim_N H^1(N_p,T) \twoheadrightarrow H^1(M_p,T)$. We write $\mathfrak{l}$ instead of $\mathfrak{l}_F$.

We will make use of the following *Selmer structures* on the G_F-representation T while proving a Gras-style conjecture in Section 5 below.

Definition 2.10. By Kummer theory, we may identify $H^1(F,T)$ with $L^{\times,\chi}$ and similarly for any prime $\mathfrak{q}$ of F, the local cohomology group $H^1(F_\mathfrak{q},T)$ with $(L\otimes_F F_\mathfrak{q})^{\times,\chi} = \left(\bigoplus_{\mathfrak{Q}|\mathfrak{q}} L_\mathfrak{Q}^\times\right)^\chi$.

- The *canonical Selmer structure* $\mathcal{F}_{\mathrm{can}}$ is given by the choice of local conditions
$$H^1_{\mathcal{F}_{\mathrm{can}}}(F_\mathfrak{q},T) = \left(\bigoplus_{\mathfrak{Q}|\mathfrak{q}} \mathcal{O}_{L_\mathfrak{Q}}^\times\right)^\chi \subset H^1(F_\mathfrak{q},T)$$
for all primes $\mathfrak{q}$ of F.
- The *$\mathfrak{L}$-restricted Selmer structure* $\mathcal{F}_\mathfrak{l}$ is given by the local conditions
  - $H^1_{\mathcal{F}_\mathfrak{l}}(F_\mathfrak{q},T) = H^1_{\mathcal{F}_{\mathrm{can}}}(F_\mathfrak{q},T)$ for every prime $\mathfrak{q}\nmid p$, and
  - $H^1_{\mathcal{F}_\mathfrak{l}}(F_p,T) = \mathcal{V}_F^- \oplus \mathfrak{l}$.
- The *p-transversal-Selmer structure* $\mathcal{F}_{\mathrm{tr}}$ is given by the local conditions
  - $H^1_{\mathcal{F}_{\mathrm{tr}}}(F_\mathfrak{q},T) = H^1_{\mathcal{F}_{\mathrm{can}}}(F_\mathfrak{q},T)$ for every prime $\mathfrak{q}\nmid p$, and
  - $H^1_{\mathcal{F}_{\mathrm{tr}}}(F_p,T) = \mathcal{V}_F^-$.

We refer the reader to [MR04, §2.1] for the definition of a Selmer structure in its most general form.

Definition 2.11. Given a Selmer structure $\mathcal{F}$ on T, we define the *dual Selmer structure* $\mathcal{F}^*$ on T^* using local Tate duality (as in [MR04, Definition 2.3.1]).

Recall the finite set Σ of primes of F which consists of all primes that ramify in L/F, all archimedean primes of F and all primes of F above p. Let F_Σ denote the maximal extension of F contained in $\bar{F}$ which is unramified outside Σ, and let G_Σ denote the Galois group $\mathrm{Gal}(F_\Sigma/F)$.

Definition 2.12. For $\mathcal{F} = \mathcal{F}_{\mathrm{can}}$, $\mathcal{F}_{\mathfrak{l}}$, or $\mathcal{F}_{\mathrm{tr}}$, we define the *$\mathcal{F}$-Selmer group* on the quotient T of $\mathbb{T}$ by setting

$$H^1_{\mathcal{F}}(F,T) = \ker\left(H^1(G_\Sigma,T) \longrightarrow \bigoplus_{\mathfrak{q}\in\Sigma} H^1(F_{\mathfrak{q}},T)/H^1_{\mathcal{F}}(F_{\mathfrak{q}},T)\right).$$

Example 2.13. We have $H^1_{\mathcal{F}_{\mathrm{can}}}(F,T) = \mathcal{O}_L^{\times,\chi}$ and $H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,T^*)^\vee \cong \mathrm{Cl}(L)^\chi$. See [MR04, §6.1] for details.

2.3. **Modified Selmer structures for $\mathbb{G}_m$ along $F^{\mathbf{cyc}}$ and F_∞.** We set $\mathbb{T}_{\mathrm{cyc}} := T \otimes \Lambda_{\mathrm{cyc}}$ and $\mathbb{T} = T \otimes \Lambda$ (with diagonal G_F-action). The definitions we give in this section will be used to prove various forms of CM main conjectures, which will in turn be used to turn the divisibilities in the cyclotomic (supersingular) main conjecture for CM elliptic curves into equalities.

Definition 2.14. The *canonical Selmer structure* $\mathcal{F}_{\mathrm{can}}$ on X (where $X = \mathbb{T}_{\mathrm{cyc}}, \mathbb{T}$) is given by the choice of local conditions $H^1_{\mathcal{F}_{\mathrm{can}}}(F_{\mathfrak{q}},X) = H^1_{\mathcal{F}_{\mathrm{can}}}(F_{\mathfrak{q}},X)$, for all primes $\mathfrak{q}$ of F. Note that the associated Selmer group $H^1_{\mathcal{F}_{\mathrm{can}}}(F,X)$ is simply the module $H^1(F,X)$.

Lemma 2.15. *Suppose that the weak Leopoldt conjecture holds true for the number field L. Then the Λ_{cyc}-module $H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T}_{\mathrm{cyc}})$ is free of rank g.*

Proof. A form of weak Leopoldt's conjecture is that the dual (canonical) Selmer group $H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,\mathbb{T}^*_{\mathrm{cyc}})$ is Λ_{cyc}-cotorsion. It follows from the hypothesis (1.2) that the Λ_{cyc}-module $H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T}_{\mathrm{cyc}})$ is torsion-free and by Poitou-Tate global duality that it is of rank g. Let γ be a topological generator of Γ^{cyc}. To see that the module $H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T}_{\mathrm{cyc}})$ is in fact free, observe that the augmentation map induces an injective map

$$H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T}_{\mathrm{cyc}})/(\gamma-1) \hookrightarrow H^1_{\mathcal{F}_{\mathrm{can}}}(F,T)$$

by the discussion in §1.6.C, Proposition B.3.3 along with the proof of Proposition 3.2.6 of [Rub00]. Note that in order to compare local conditions at p, we rely on our assumption (1.2). This and Lemma 2.6 show by Nakamaya's lemma that the Λ_{cyc}-module $H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T}_{\mathrm{cyc}})$ may be generated by at most g elements. If this set of generators satisfied a non-trivial Λ_{cyc}-linear relation, it would follow that the dimension of the $\mathrm{Frac}(\Lambda)$ vector space $H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T}_{\mathrm{cyc}}) \otimes_{\Lambda_{\mathrm{cyc}}} \mathrm{Frac}(\Lambda_{\mathrm{cyc}})$ (where $\mathrm{Frac}(\Lambda_{\mathrm{cyc}})$ is the field of fractions of Λ_{cyc}) is strictly smaller than g, and this would contradict the fact that $H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T}_{\mathrm{cyc}})$ is a Λ_{cyc}-module of rank g. □

Remark 2.16. One may use Nekovář's theory of Selmer complexes to give a more conceptual proof of Lemma 2.15 (in fact, along the way, to prove also that the Λ-module $H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T})$ is free of rank g, which is what we explain in what follows). Let $\widetilde{R\Gamma}_{f,\mathrm{Iw}}(F_\infty/F,T)$ be Nekovář's Selmer complex associated to $\mathbb{T}$, which is given by the Greenberg local conditions determined by the choice $U_v^+ = T$ for every prime v of F above p. As we have assumed (1.2), it follows from [Nek06, Lemma 9.6.3] (and [Nek06, Proposition 8.8.6] used in order to pass to limit) that

$$\widetilde{H}^1_f(F_\Sigma/F_\infty, T) \xrightarrow{\sim} H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T})$$

where $\widetilde{H}^1_f$ denotes the cohomology of the Selmer complex in degree 1. Under the hypothesis (1.2), Nekovář proved that the Selmer complex may be represented by a perfect complex concentrated in degrees 1 and 2. In particular, its cohomology in degree 1 is a projective (hence free) Λ-module. The fact that it is of rank g may also be deduced from Nekovář's control and duality theorems: We have

$$\text{(2.1)} \qquad \mathrm{coker}\left(\widetilde{H}^1_f(F_\Sigma/F_\infty, T) \longrightarrow \widetilde{H}^1_f(F_\Sigma/F^{\mathrm{cyc}}, T)\right) \cong \widetilde{H}^2_f(F_\Sigma/F_\infty, T)[\gamma_* - 1]$$
$$\cong H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, \mathbb{T}^*)^\vee[\gamma_* - 1]$$

where γ_* is a topological generator of $\Gamma/\Gamma^{\mathrm{cyc}}$ and the first isomorphism follows from Nekovář's control theorem [Nek06, 8.10.1]; the second from his duality theorem [Nek06, 8.9.6.2]. One may identify $H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, \mathbb{T}^*)^\vee$ with $\varprojlim_{L \subset M \subset LF_\infty} \mathrm{Cl}(M)^\chi$ and argue using classical Iwasawa theory that the cokernel (2.1) is Λ_{cyc}-torsion and the Λ-module $H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T})$ cannot be generated by less than g elements. On the other hand, the proof of Lemma 2.15 shows that it may be generated by at most g elements as well.

Definition 2.17. Let $\mathcal{V}_F^-$ be as in Definition 2.7 and let $\mathcal{V}_{\mathrm{cyc}}$ be any rank-g direct summand of (the free, rank-$2g$ Λ_{cyc}-module) $H^1(F_p, \mathbb{T}_{\mathrm{cyc}})$ which lifts $\mathcal{V}_F^-$ under the surjection $H^1(F_p, \mathbb{T}_{\mathrm{cyc}}) \twoheadrightarrow H^1(F_p, T)$. Likewise, once $\mathcal{V}_{\mathrm{cyc}}$ is chosen, let $\mathcal{V}$ be any rank-g direct summand of (the free, rank-$2g$ Λ-module) $H^1(F_p, \mathbb{T})$ which lifts $\mathcal{V}_{\mathrm{cyc}}$ under the surjection $H^1(F_p, \mathbb{T}) \twoheadrightarrow H^1(F_p, \mathbb{T}_{\mathrm{cyc}})$. Such lifts exist by Nakayama's lemma. Set $\mathcal{Q} := H^1(F_p, \mathbb{T})/\mathcal{V}$ and similarly define $\mathcal{Q}_{\mathrm{cyc}}$.

Let $\mathcal{L} \subset H^1(F_p, \mathbb{T})$ be any rank-one direct summand of $H^1(F_p, \mathbb{T})$ such that $\mathcal{L} \cap \mathcal{V} = 0$ and $\mathcal{L} + \mathcal{V}$ is a free rank $g+1$ direct summand of $H^1(F_p, \mathbb{T})$. Let $\mathcal{L}_{\mathrm{cyc}}$ be its image in $H^1(F_p, \mathbb{T}_{\mathrm{cyc}})$. The existence of such a direct summand follows once again from Nakayama's lemma. It is also easy to observe that $\mathcal{L}_{\mathrm{cyc}} \cap \mathcal{V}_{\mathrm{cyc}} = 0$ and $\mathcal{L}_{\mathrm{cyc}} + \mathcal{V}_{\mathrm{cyc}}$ is a free rank $g+1$ direct summand of $H^1(F_p, \mathbb{T}_{\mathrm{cyc}})$.

Proposition 2.18. *The intersection of $\mathcal{V}_{\mathrm{cyc}}$ and the image of $H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T}_{\mathrm{cyc}})$ (under the localization map at p) is trivial. Likewise, the intersection of $\mathcal{V}$ and the image of $H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T})$ is trivial as well.*

Proof. Consider the commutative diagram:

$$\begin{tikzcd}
H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T}_{\mathrm{cyc}}) \arrow[r, "\mathrm{Loc}_p"] \arrow[d] & H^1(F_p, \mathbb{T}_{\mathrm{cyc}})/\mathcal{V}_{\mathrm{cyc}} \arrow[d, two heads] \\
H^1_{\mathcal{F}_{\mathrm{can}}}(F, T) \arrow[r, hook, "\mathrm{loc}_p"'] & H^1(F_p, T)/\mathcal{V}_F^-
\end{tikzcd}$$

Suppose for $u \in H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T}_{\mathrm{cyc}})$ we have $\mathrm{Loc}_p(u) = 0$ and let $\bar{u}$ denote its image under the left vertical map. The diagram above shows that $\bar{u} = 0$, thence

$$u \in \ker\left(H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T}_{\mathrm{cyc}}) \to H^1(F, T)\right) = (\gamma - 1)H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T}_{\mathrm{cyc}}),$$

where γ is any topological generator of Γ^{cyc}. Write $u = (\gamma - 1)u_0$. We therefore have $(\gamma-1)\mathrm{Loc}_p(u_0) = 0$ by the choice of u. Since the quotient $H^1(F_p, \mathbb{T}_{\mathrm{cyc}})/\mathcal{V}_{\mathrm{cyc}}$ is Λ_{cyc}-torsion free, it follows that $\mathrm{Loc}_p(u_0) = 0$, and repeating the argument above we conclude that $u = (\gamma - 1)u_1$ with $u_1 \in H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T}_{\mathrm{cyc}})$. On running this procedure k times, we conclude that $u \in (\gamma - 1)^k H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T}_{\mathrm{cyc}})$ for every k and thence $u = 0$ and the map Loc_p is injective, proving the first assertion. The proof of the second follows from the first in a similar manner. □

Definition 2.19.

(i) Let $\mathcal{V}_{K(\mathfrak{C})}$ be the direct summand (of rank g) of $\varprojlim_{M\in\mathfrak{C}} H^1(M_p, T)$ which maps onto $\mathcal{V}$ under the natural (surjective) corestriction map.

(ii) For $M \in \mathfrak{C}$, let $\mathcal{V}_M \subset H^1(M_p, T)$ be the image of $\mathcal{V}_{K(\mathfrak{C})}$ under the natural projection.

(iii) Let $\mathfrak{L}$ be any free, rank-one $\mathfrak{O}[[\mathfrak{G}(K(\mathfrak{C}))]]$-direct summand of $\varprojlim_{M\in\mathfrak{C}} H^1(M_p, T)$ such that
- $\mathfrak{L}$ is not contained in $\mathcal{V}_{K(\mathfrak{C})}$,
- $\mathfrak{L} + \mathcal{V}_{K(\mathfrak{C})}$ is also a direct summand of $\varprojlim_{M\in\mathfrak{C}} H^1(M_p, T)$,
- $\mathfrak{L}$ maps onto $\mathcal{L}$ under the natural projection.

(Such $\mathfrak{L}$ exists thanks to Nakayama's lemma again.)

(iv) For $M \in \mathfrak{C}$, let $\mathcal{L}_M \subset H^1(M_p, T)$ be the image of $\mathfrak{L}$ under the natural projection $\varprojlim_{N} H^1(N_p, T) \twoheadrightarrow H^1(M_p, T)$.

We will make use of the following auxiliary *Selmer structures* on the G_F-representation $\mathbb{T}$ while proving various main conjectures for the field F in Sections 5 and 6 below. These results will in turn be utilized in sharpening the divisibility in the supersingular main conjecture for a CM elliptic curve E.

Definition 2.20.

- The *$\mathfrak{L}$-restricted Selmer structure* $\mathcal{F}_{\mathfrak{L}}$ on $\mathbb{T}$ is given by the local conditions
  - $H^1_{\mathcal{F}_{\mathfrak{L}}}(F_\mathfrak{q}, \mathbb{T}) = H^1_{\mathcal{F}_{\mathrm{can}}}(F_\mathfrak{q}, \mathbb{T})$ for every prime $\mathfrak{q} \nmid p$, and
  - $H^1_{\mathcal{F}_{\mathfrak{L}}}(F_p, \mathbb{T}) = \mathcal{V}_{\mathrm{cyc}} \oplus \mathfrak{L}$.
- The *p-transversal-Selmer structure* $\mathcal{F}_{\mathfrak{tr}}$ is given by the local conditions
  - $H^1_{\mathcal{F}_{\mathfrak{tr}}}(F_\mathfrak{q}, \mathbb{T}) = H^1_{\mathcal{F}_{\mathrm{can}}}(F_\mathfrak{q}, \mathbb{T})$ for every prime $\mathfrak{q} \nmid p$, and
  - $H^1_{\mathcal{F}_{\mathfrak{tr}}}(F_p, \mathbb{T}) = \mathcal{V}$.

As in Definition 2.12, all these Selmer structures give rise to a Selmer group (as well as a dual Selmer group, attached to the dual Selmer structure).

Remark 2.21. Any of the Selmer structures above *propagate* (see [MR04, Example 2.1.7]) to give rise to Selmer structures on any subquotient of $\mathbb{T}$. The propagated Selmer structure will still be denoted by the same symbol $\mathcal{F}$.

Remark 2.22. The Selmer structure $\mathcal{F}_{\mathfrak{tr}}$ on $\mathbb{T}$ propagates to recover the Selmer structure $\mathcal{F}_{\mathrm{tr}}$ on T, given as in Definition 2.10. Likewise, if the rank-1 direct summand $\mathcal{L}$ is chosen to lift $\mathfrak{l}$ (which was given in Definition 2.9), then the Selmer structure $\mathcal{F}_{\mathcal{L}}$ on $\mathbb{T}$ propagates to recover the Selmer structure $\mathcal{F}_{\mathfrak{l}}$ on T.

2.4. Modified Selmer structures for E.

We set $\mathbb{T}(E) = T(E) \otimes \Lambda$ and $\mathbb{T}_{\text{cyc}}(E) = T(E) \otimes \Lambda_{\text{cyc}}$. The goal in this section is to define various Selmer structures for these representations, which we shall study with the aid of the (conjectural) Rubin-Stark elements. Note that in order to do so, we will exploit the fact that $\mathbb{T}(E)$ is closely related to the representation $\mathbb{T}$ for an appropriately chosen Dirichlet character χ.

2.4.1. *Preliminaries.* As above, let E be an elliptic curve defined over F^+ which has CM by K. We shall assume that p is inert in $K/\mathbb{Q}$. We denote the unique prime of K above p also by p and the completion K_p by Φ. By slight abuse, we let $\mathfrak{O}$ denote the ring of integers of Φ and let

$$\rho : G_F \longrightarrow \text{Aut}(E[p^\infty]) \cong \mathfrak{O}^\times$$

be the associated p-adic Hecke character. For any G_F-module Y, we define its twist by ρ by setting $Y(\rho) := Y \otimes \text{Hom}(E[p^\infty], \Phi/\mathfrak{O})$. Theory of complex multiplication allows one to identify $T_p(E)$ with $\mathfrak{O}(\rho)$, the free $\mathfrak{O}$-module of rank 1 on which G_F acts via ρ. We will implicitly identify the Cartier dual $T_p(E)^*$ with $E[p^\infty]$ via the Weil pairing.

Definition 2.23. Let $\omega_E : G_F \to \mathfrak{O}^\times$ denote the character which gives the action of G_F on $E[p]$ and let $\langle\rho\rangle := \rho \otimes \omega_E^{-1}$. Note then that the character $\langle\rho\rangle$ factors through Γ.

Throughout this section we will set the character $\chi = \omega_E$ so that $T = \mathfrak{O}(1) \otimes \omega_E^{-1}$.

Definition 2.24. Let $\text{tw} : T \to T(E)$ (the *twisting map*) denote the compositum of the maps

$$T \longrightarrow T \otimes \langle\rho\rangle^{-1} \xrightarrow{\mathcal{W}} T(E)$$

where $\mathcal{W}$ is induced from Weil pairing. The twisting map induces isomorphisms

$$\text{tw} : \ H^1(F, \mathbb{T}) \xrightarrow{\sim} H^1(F, \mathbb{T}(E)),$$

and for every place v of F,

$$\text{tw} : \ H^1(F_v, \mathbb{T}) \xrightarrow{\sim} H^1(F_v, \mathbb{T}(E)) \ .$$

2.4.2. *Selmer structures.* We set $\mathcal{M} = \text{tw}\left(\text{loc}_p\left(H^1_{\mathcal{F}_{\text{can}}}(F, \mathbb{T})\right)\right) \subset H^1(F_p, \mathbb{T}(E))$ and let $\mathcal{M}_{\text{cyc}} \subset H^1(F_p, \mathbb{T}_{\text{cyc}}(E))$ be its projection. Note that $\mathcal{M}$ is a free Λ-module and $\mathcal{M}_{\text{cyc}}$ a free Λ_{cyc}-module, and both have rank g.

Lemma 2.25. *If the Λ_{cyc}-module $H^1_{\mathcal{F}^*_{\text{can}}}(F, \mathbb{T}_{\text{cyc}}(E)^*)^\vee$ is torsion, then so is the quotient*

$$\text{loc}_p\left(H^1(F, \mathbb{T}_{\text{cyc}}(E))\right)/\mathcal{M}_{\text{cyc}} \, .$$

Remark 2.26. The statement that $H^1_{\mathcal{F}^*_{\text{can}}}(F, \mathbb{T}_{\text{cyc}}(E)^*)^\vee$ is Λ_{cyc}-torsion is a form of the weak Leopoldt conjecture for the elliptic curve E. See Corollary 4.3 and Theorem 6.22 below, where we verify the weak Leopoldt conjecture for E (at primes p which split completely in F^+/F) assuming the Explicit Reciprocity Conjecture 6.16 for the Rubin-Stark elements.

Proof of Lemma 2.25. Let γ_* be any lift of a topological generator of $\Gamma/\Gamma^{\text{cyc}}$. Proof follows, as in the discussion of Remark 2.16 (particularly, using Nekovář's control theorem as in (2.1)), once we verify that

$$\text{coker}\left(\widetilde{H}^1_f(F_\Sigma/F_\infty, T(E)) \longrightarrow \widetilde{H}^1_f(F_\Sigma/F^{\text{cyc}}, T(E))\right) \cong \widetilde{H}^2_f(F_\Sigma/F_\infty, \mathbb{T}(E))[\gamma_* - 1]$$

is Λ_{cyc}-torsion. (This is because the quotient $\mathrm{loc}_p\left(H^1(F,\mathbb{T}_{\mathrm{cyc}}(E))\right)/\mathcal{M}_{\mathrm{cyc}}$ is a homomorphic image of the quotient

$$H^1(F,\mathbb{T}_{\mathrm{cyc}}(E))/\mathrm{im}\left(H^1(F,\mathbb{T}(E))\right) \cong \widetilde{H}^1_f(F_\Sigma/F_{\mathrm{cyc}},T)/\mathrm{im}\left(\widetilde{H}^1_f\left(F_\Sigma/F_\infty,T\right)\right) .)$$

Note that we have

$$\widetilde{H}^2_f(F_\Sigma/F_\infty,\mathbb{T}(E)) \cong H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,\mathbb{T}(E)^*)^\vee$$

by [Nek06, 8.9.6.2]. Furthermore,

$$H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,\mathbb{T}(E)^*)^\vee/(\gamma_*-1) \cong \left(H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,\mathbb{T}(E)^*)[\gamma_*-1]\right)^\vee \cong H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,\mathbb{T}_{\mathrm{cyc}}(E)^*)^\vee$$

where the second isomorphism is by [MR04, Lemma 3.5.3], and hence we conclude thanks to our assumption that $H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,\mathbb{T}(E)^*)^\vee/(\gamma_*-1)$ is Λ_{cyc}-torsion.

We now conclude by [PR84, Lemme I.3.4(ii)] that

$$H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,\mathbb{T}(E)^*)^\vee[\gamma_*-1] \cong \widetilde{H}^2_f(F_\Sigma/F_\infty,\mathbb{T}(E))[\gamma_*-1]$$

is Λ_{cyc}-torsion as well. □

Definition 2.27. Let $\mathbb{V}_E^{\mathrm{cyc}} \subset H^1(F_p,\mathbb{T}_{\mathrm{cyc}}(E))$ be a free rank-g direct summand with the property that $\mathbb{V}_E^{\mathrm{cyc}} \cap \mathcal{M}_{\mathrm{cyc}} = 0$. Note that such a direct summand exists by rank considerations. Let $\mathbb{V}_E \subset H^1(F_p,\mathbb{T}(E))$ be any rank-g direct summand which maps onto $\mathbb{V}_E^{\mathrm{cyc}}$ under the surjection $H^1(F_p,\mathbb{T}(E)) \to H^1(F_p,\mathbb{T}_{\mathrm{cyc}}(E))$.

See Remark 6.19 below for a natural choice of $\mathbb{V}_E^{\mathrm{cyc}}$ under the additional hypothesis that p splits completely in $F^+/\mathbb{Q}$, using Kobayashi's plus/minus Iwasawa theory. We will use these choices in order to prove the main theorems of this article.

Remark 2.28. The proof of Proposition 2.18 may be modified to prove that $\mathbb{V}_E \cap \mathcal{M} = 0$ as well.

Definition 2.29. Let $\mathbb{V} := \mathrm{tw}^{-1}(\mathbb{V}_E) \subset H^1(F_p,\mathbb{T})$. Let $\mathbb{L} \subset H^1(F_p,\mathbb{T})$ be a rank-one direct summand of $H^1(F_p,\mathbb{T})$ such that $\mathbb{L}\cap\mathbb{V} = 0$ and $\mathbb{L}+\mathbb{V}$ is a free rank $g+1$ direct summand of $H^1(F_p,\mathbb{T})$. As before, the existence of such a direct summand follows from Nakayama's lemma. Let $\mathbb{L}_E \subset H^1(F_p,\mathbb{T}(E))$ denote its isomorphic image and $\mathbb{L}_E^{\mathrm{cyc}}$ its image under the projection map to $H^1(F_p,\mathbb{T}_{\mathrm{cyc}}(E))$.

Note that $\mathbb{V} \cap \mathrm{loc}_p\left(H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T})\right) = 0$ by the observation in Remark 2.28.

Definition 2.30.

- The *canonical Selmer structure* $\mathcal{F}_{\mathrm{can}}$ is given by the choice of local conditions $H^1_{\mathcal{F}_{\mathrm{can}}}(F_\mathfrak{q},\mathbb{T}(E)) = H^1(F_\mathfrak{q},\mathbb{T}(E))$, for all primes $\mathfrak{q}$ of F.
- The $\mathbb{L}$*-restricted Selmer structure* is given by the local conditions
  - $H^1_{\mathcal{F}_\mathbb{L}}(F_\mathfrak{q},\mathbb{T}(E)) = H^1_{\mathcal{F}_{\mathrm{can}}}(F_\mathfrak{q},\mathbb{T}(E))$ for every prime $\mathfrak{q}\nmid p$, and
  - $H^1_{\mathcal{F}_\mathbb{L}}(F_p,\mathbb{T}(E)) = \mathbb{V}_E \oplus \mathbb{L}_E$.
- The *Kobayashi Selmer structure* $\mathcal{F}_{\mathrm{Kob}}$ is given by the local conditions
  - $H^1_{\mathcal{F}_{\mathrm{Kob}}}(F_\mathfrak{q},\mathbb{T}(E)) = H^1_{\mathcal{F}_{\mathrm{can}}}(F_\mathfrak{q},\mathbb{T}(E))$ for every prime $\mathfrak{q}\nmid p$, and
  - $H^1_{\mathcal{F}_{\mathrm{Kob}}}(F_p,\mathbb{T}(E)) = \mathbb{V}_E$.

Given a Selmer structure $\mathcal{F}$ on $\mathbb{T}(E)$, we can talk about the *dual Selmer structure* $\mathcal{F}^*$ on $\mathbb{T}^*$, the Selmer group attached to it and its propagations to the various subquotients of $\mathbb{T}(E)$ (most important of which are $\mathbb{T}_{\mathrm{cyc}}(E)$ and $T(E)$ for our purposes), as we have done so previously. Via the twisting isomorphism tw, we also obtain a Selmer structure (by a slight abuse, which we still denote by $\mathcal{F}_{\mathbb{L}}$ or $\mathcal{F}_{\mathrm{Kob}}$) on $\mathbb{T}$ (and on its various subquotients).

2.5. **Global duality and comparison of Selmer groups.** Let R be a complete local noetherian domain with maximal ideal $\mathfrak{M}$. Let X be an R-module of finite type. We will write $\overline{X} := X \otimes_R R/\mathfrak{M}$ for its reduction modulo the maximal ideal of R. Note that

$$\overline{\mathbb{T}} = \overline{\mathbb{T}}_{\mathrm{cyc}} = \overline{T} = \boldsymbol{\mu}_p \otimes \chi^{-1}$$

and

$$\overline{\mathbb{T}}(E) = \overline{\mathbb{T}}_{\mathrm{cyc}}(E) = \overline{T(E)} = E[p]$$

as G_F-representations. In particular, when χ is chosen to be ω_E^{-1}, it follows thanks to the Weil pairing that all the six residual representations we consider above agree.

Let k denote the residue field of $\mathfrak{O}$.

Lemma 2.31. *Assume the truth of Leopoldt's conjecture for the number field L. We have*

$$\dim_k H^1_{\mathcal{F}}(F,\overline{T}) = \dim_k H^1_{\mathcal{F}^*}(F,\overline{T}^*)$$

for $\mathcal{F} = \mathcal{F}_{\mathrm{tr}}, \mathcal{F}_{\mathfrak{tr}}$ *or* $\mathcal{F}_{\mathrm{Kob}}$ *and*

$$\dim_k H^1_{\mathcal{G}}(F,\overline{T}) = \dim_k H^1_{\mathcal{G}^*}(F,\overline{T}^*) + 1$$

for $\mathcal{G} = \mathcal{F}_{\mathfrak{l}}, \mathcal{F}_{\mathcal{L}}$ *or* $\mathcal{F}_{\mathbb{L}}$. (*Note that when* $\mathcal{F} = \mathcal{F}_{\mathrm{Kob}}$ *or* $\mathcal{G} = \mathcal{F}_{\mathbb{L}}$ *we only consider the case* $\chi = \omega_E$.)

Proof. As explained in Example 2.13 we have $H^1_{\mathcal{F}_{\mathrm{can}}}(F,T) \cong \mathcal{O}_{L_\chi}^{\times,\chi}$, and hence Lemma 2.6 shows that the $\mathfrak{O}$-module $H^1_{\mathcal{F}_{\mathrm{can}}}(F,T)$ is free of rank g under the running assumptions. On the other hand, $H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,T^*) \cong \mathrm{CL}(L)^\chi$ is finite, and it follows from the discussion in Section 5.2 of [MR04] that

$$\begin{aligned}\dim_k H^1_{\mathcal{F}_{\mathrm{can}}}(F,\overline{T}) &- \dim_k H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,\overline{T}^*)\\ &= \mathrm{rank}_{\mathfrak{O}} H^1_{\mathcal{F}_{\mathrm{can}}}(F,T) - \mathrm{corank}_{\mathfrak{O}} H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,T^*) = g.\end{aligned} \tag{2.2}$$

Observe that we have by the choices we have made that

$$\dim_k H^1_{\mathcal{F}_{\mathrm{can}}}(F_p,\overline{T}) - \dim_k H^1_{\mathcal{F}}(F_p,\overline{T}) = g$$

for $\mathcal{F} = \mathcal{F}_{\mathrm{tr}}, \mathcal{F}_{\mathfrak{tr}}$ or $\mathcal{F}_{\mathrm{Kob}}$ and

$$\dim_k H^1_{\mathcal{F}_{\mathrm{can}}}(F_p,\overline{T}) - \dim_k H^1_{\mathcal{G}}(F_p,\overline{T}) = g-1$$

for $\mathcal{G} = \mathcal{F}_{\mathfrak{l}}, \mathcal{F}_{\mathcal{L}}$ or $\mathcal{F}_{\mathbb{L}}$. Proposition 1.6 of [Wil95] shows that

$$\begin{aligned}\Big(\dim_k H^1_{\mathcal{F}_{\mathrm{can}}}(F,\overline{T}) - \dim_k H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,\overline{T}^*)\Big) - \Big(\dim_k H^1_{\mathcal{F}}(F,\overline{T}) - \dim_k H^1_{\mathcal{F}^*}(F,\overline{T}^*)\Big)&\\ = \dim_k H^1_{\mathcal{F}_{\mathrm{can}}}(F_p,\overline{T}) - \dim_k H^1_{\mathcal{F}}(F_p,\overline{T})&\\ = g\,.&\end{aligned}$$

The first part of the proposition follows from (2.2), and the second part may also be deduced by replacing $\mathcal{F}$'s by $\mathcal{G}$'s. □

Remark 2.32. Throughout this paragraph, $\mathcal{F}$ will stand for any of $\mathcal{F}_{\mathfrak{l}}, \mathcal{F}_{\mathcal{L}}$ or $\mathcal{F}_{\mathbb{L}}$, with the convention that if $\mathcal{F} = \mathcal{F}_{\mathbb{L}}$ the $\chi = \omega_E$. Corollary 4.5.2 of [MR04] asserts that the module of Kolyvagin systems $\mathbf{KS}(\mathcal{F},\overline{T})$ is a k-vector space of dimension one, thanks to the second part of Lemma 2.31. On the other hand, it follows from the main theorem of [Büy16] that these *residual* Kolyvagin systems deform to X

(where $X = \mathbb{T}, \mathbb{T}(E), \mathbb{T}_{\mathrm{cyc}}$ or $\mathbb{T}_{\mathrm{cyc}}(E)$) and that the module $\overline{\mathbf{KS}}(\mathcal{F}, X)$ is free of rank one over the corresponding coefficient ring. The elements of these modules (namely, Kolyvagin systems) are used to bound the characteristic ideal of $H^1_{\mathcal{F}^*}(F, X)^\vee$. The generators of the module of Kolyvagin systems are characterized by the property that the bounds they give on the characteristic ideal of $H^1_{\mathcal{F}^*}(F, X)^\vee$ are sharp.

We will later use the (conjectural) Rubin-Stark elements to construct these Kolyvagin systems and exploit facts recalled above in order to verify the sharpness of the bounds we shall obtain on the Kobayashi Selmer groups for the CM elliptic curve E.

Proposition 2.33. *Assume that Leopoldt's conjecture holds for L. Then,*

$$H^1_{\mathcal{F}_{\mathrm{tr}}}(F, T) = H^1_{\mathcal{F}_{\mathfrak{tr}}}(F, \mathbb{T}_{\mathrm{cyc}}) = H^1_{\mathcal{F}_{\mathfrak{tr}}}(F, \mathbb{T}) = 0,$$

and if $H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, \mathbb{T}_{\mathrm{cyc}}(E)^*)^\vee$ is Λ_{cyc}-torsion, then

$$H^1_{\mathcal{F}_{\mathrm{Kob}}}(F, \mathbb{T}_{\mathrm{cyc}}(E)) = H^1_{\mathcal{F}_{\mathrm{Kob}}}(F, \mathbb{T}(E)) = 0.$$

Proof. The first group of assertions follows from the definitions. Let $\mathcal{M}_{\mathrm{cyc}}$ be as at the start of Section 2.4.2. The quotient $\mathrm{loc}_p\left(H^1(F, \mathbb{T}_{\mathrm{cyc}}(E))\right)/\mathcal{M}_{\mathrm{cyc}}$ is a torsion Λ_{cyc}-module by Lemma 2.25 (under our assumption of the weak Leopoldt conjecture for $T(E)$). Since $\mathcal{M}_{\mathrm{cyc}} \cap \mathbb{V}_E^{\mathrm{cyc}} = 0$ by our very choice of $\mathbb{V}_E^{\mathrm{cyc}}$ and since $H^1(F_p, \mathbb{T}_{\mathrm{cyc}})/\mathbb{V}_E^{\mathrm{cyc}}$ is torsion free, it follows that $\mathrm{loc}_p\left(H^1(F, \mathbb{T}_{\mathrm{cyc}}(E))\right) \cap \mathbb{V}_E^{\mathrm{cyc}} = 0$. This means

$$H^1_{\mathcal{F}_{\mathrm{Kob}}}(F, \mathbb{T}_{\mathrm{cyc}}(E)) := \ker\left(H^1(F, \mathbb{T}_{\mathrm{cyc}}(E)) \xrightarrow{\mathrm{loc}_p} \mathbb{V}_E^{\mathrm{cyc}}\right) = 0\,.$$

Let $\gamma_* \in \Gamma$ be any lift of a topological generator of $\Gamma/\Gamma^{\mathrm{cyc}}$. The exact sequence

$$0 \longrightarrow \mathbb{T} \xrightarrow{\gamma_*-1} \mathbb{T} \longrightarrow \mathbb{T}_{\mathrm{cyc}} \longrightarrow 0$$

yields an injection

$$H^1_{\mathcal{F}_{\mathrm{Kob}}}(F, \mathbb{T})\big/(\gamma_* - 1) \hookrightarrow H^1_{\mathcal{F}_{\mathrm{Kob}}}(F, \mathbb{T}_{\mathrm{cyc}}) = 0,$$

and we conclude by Nakayama's lemma that $H^1_{\mathcal{F}_{\mathrm{Kob}}}(F, \mathbb{T}) = 0$ as well. □

Proposition 2.34. *Assume that Leopoldt's conjecture holds for L and the weak Leopoldt conjecture for $T(E)$. Let $(\mathcal{F}, \mathcal{G}, \mathfrak{D}, X)$ be any of the following quadruples:*

$$\{(\mathcal{F}_{\mathrm{tr}}, \mathcal{F}_{\mathfrak{l}}, \mathfrak{l}, T), (\mathcal{F}_{\mathfrak{tr}}, \mathcal{F}_{\mathcal{L}}, \mathcal{L}_{\mathrm{cyc}}, \mathbb{T}_{\mathrm{cyc}}), (\mathcal{F}_{\mathfrak{tr}}, \mathcal{F}_{\mathcal{L}}, \mathcal{L}, \mathbb{T}),$$
$$(\mathcal{F}_{\mathrm{Kob}}, \mathcal{F}_{\mathbb{L}}, \mathbb{L}_{\mathrm{cyc}}, \mathbb{T}_{\mathrm{cyc}}(E)), (\mathcal{F}_{\mathrm{Kob}}, \mathcal{F}_{\mathbb{L}}, \mathbb{L}, \mathbb{T})\}.$$

Then the following sequence is exact:

$$0 \longrightarrow H^1_{\mathcal{G}}(F, X) \xrightarrow{\mathrm{loc}_p} \mathfrak{D} \longrightarrow H^1_{\mathcal{F}^*}(F, X^*)^\vee \longrightarrow H^1_{\mathcal{G}^*}(F, X^*)^\vee \longrightarrow 0.$$

Proof. This follows from Poitou-Tate global duality, used with Proposition 2.33. □

3. Rubin-Stark Euler system of rank r

We review Rubin's [Rub96] integral refinement of Stark's conjectures, which we will later use to construct Kolyvagin systems for the modified Selmer structure $\mathcal{F}_{\mathcal{L}}$ on $\mathbb{T}$. For the rest of this paper, we assume that the Rubin-Stark Conjecture [Rub96, Conjecture B′] holds true for the fields which appear in this article.

Let χ, f_χ and L be as above, and recall the definitions of the collections of extensions $\mathfrak{E}_0$ and $\mathfrak{E}$ from §1.1. Fix forever a finite set S of places of F that does *not* contain any prime above p, but contains the set of infinite places S_∞ and all primes $\lambda \nmid p$ at which χ is ramified. Assume that $|S| \geq g+1$. For each $\mathcal{M} \in \mathfrak{E}_0$, let

$$S_{\mathcal{M}} = \{\text{places of } \mathcal{M} \text{ lying above the places in } S\} \cup \{\text{places of } \mathcal{M} \text{ at which } \mathcal{M}/F \text{ is ramified}\}$$

be a set of places of $\mathcal{M}$. Let $\mathcal{O}^\times_{\mathcal{M},S_{\mathcal{M}}}$ denote the $S_{\mathcal{M}}$-units of $\mathcal{M}$, and $\Delta_{\mathcal{M}}$ (resp., $\delta_{\mathcal{M}}$) denote $\mathrm{Gal}(\mathcal{M}/F)$ (resp., $|\mathrm{Gal}(\mathcal{M}/F)|$).

Definition 3.1. Let G be any finite group and let X be any $\mathfrak{O}[G]$-module which is of finite type over $\mathfrak{O}$. Following [Rub96], we define for any integer $r \geq 0$ the submodule $\bigwedge_0^r X \subset \Phi \otimes \bigwedge^r X$ by setting

$$\bigwedge_0^r X = \left\{ x \in \Phi \otimes \bigwedge^r X : (\varphi_1 \wedge \cdots \wedge \varphi_r)(x) \in \mathfrak{O}[G] \right. \\ \left. \text{for every } \varphi_1, \cdots, \varphi_r \in \mathrm{Hom}(X, \mathfrak{O}[G]) \right\}.$$

We also let $\overline{\bigwedge^r X}$ denote the isomorphic image of $\bigwedge^r X$ under the map $j : \bigwedge^r X \to \Phi \otimes \bigwedge^r X$.

Example 3.2. If X is a free $\mathfrak{O}[G]$-module, then $\bigwedge_0^r X = \overline{\bigwedge^r X}$. In general, $|G| \cdot \bigwedge_0^r X \subset \overline{\bigwedge^r X}$.

Rubin in [Rub96, Conjecture B$'$] predicts the existence of certain elements

$$\tilde{\varepsilon}_{\mathcal{M},S_{\mathcal{M}}} \in \bigwedge_0^g \mathcal{O}^\times_{\mathcal{M},S_{\mathcal{M}}}$$

linked via a regulator map to the value of the corresponding Artin L-function at $s = 0$.

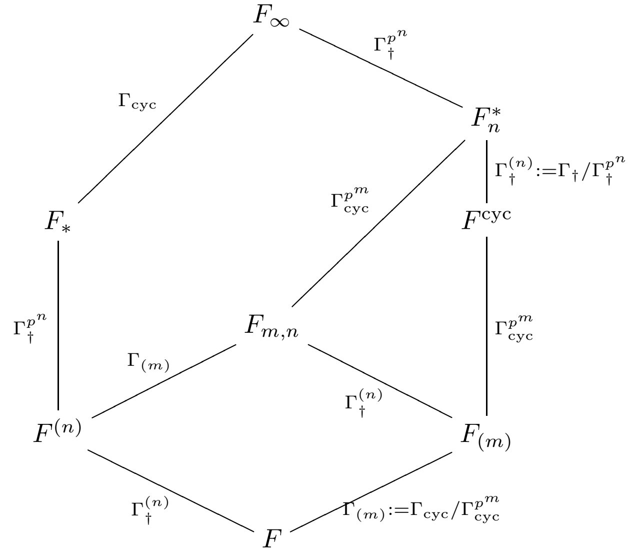
Remark 3.3. Rubin's conjecture predicts that the elements $\tilde{\varepsilon}_{\mathcal{M},S_{\mathcal{M}}}$ should in fact lie inside the module $\bigwedge_0^g \mathcal{O}^\times_{\mathcal{M},S_{\mathcal{M}},\mathcal{T}}$ where $\mathcal{T}$ is a finite set of primes disjoint from $S_{\mathcal{M}}$, chosen in a way that the group $\mathcal{O}^\times_{\mathcal{M},S_{\mathcal{M}},\mathcal{T}}$ of $S_{\mathcal{M}}$-units which are congruent to 1 modulo all the primes in $\mathcal{T}$ is torsion-free. As explained in [Büy09b, Remark 3.1], one can safely ignore $\mathcal{T}$ as far as we are concerned in this paper.

As further explained in [Büy14, §3.1], the Rubin-Stark elements may be used to construct an *Euler system of rank g* for T (in the sense of [PR98], as appropriately generalized in [Büy10] so as to allow denominators). We omit the details here and refer the reader to [Büy14]. This Euler system of rank g is a collection $\mathcal{C}^{(g)}_{\text{R-S}} = \{\varepsilon^\chi_{\mathcal{K}}\}_{\mathcal{K}\in\mathfrak{E}}$ where $\varepsilon^\chi_{\mathcal{K}} \in \bigwedge_0^g H^1(\mathcal{K},T)$. The collection $\mathcal{C}^{(g)}_{\text{R-S}}$ will be called the *Rubin-Stark Euler system of rank g* for T.

3.1. **Strong Rubin-Stark conjectures.**

Let $F_\dagger \subset F_\infty$ be any $\mathbb{Z}_p$-extension of F disjoint from F^{cyc} over F and let $\Gamma_\dagger = \mathrm{Gal}(F_\dagger/F)$ so that we have $\Gamma = \Gamma_\dagger \times \Gamma_{\mathrm{cyc}}$. Let $\gamma_\dagger$ be a topological generator of $\Gamma_\dagger$ and let γ_{cyc} denote a fixed topological generator of Γ^{cyc}.

Given positive integers m, n we let $F_{\mathrm{cyc}} \subset F_n^\dagger \subset F_\infty$ denote the fixed field of $\Gamma_\dagger^{p^n}$ (so that we have $\mathrm{Gal}(F_n^\dagger/F) = \Gamma_{\mathrm{cyc}} \times \Gamma_\dagger^{(n)}$ with $\Gamma_\dagger^{(n)} = \Gamma_\dagger/\Gamma_\dagger^{p^n}$) and let $F \subset F_{m,n} \subset F_n^\dagger$ be the fixed field of $\Gamma_{\mathrm{cyc}}^{p^m}$ (so that $\mathrm{Gal}(F_{m,n}/F) = \Gamma_{(m)} \times \Gamma^{(n)}$ with $\Gamma_{(m)} = \Gamma_{\mathrm{cyc}}/\Gamma_{\mathrm{cyc}}^{p^m}$). We write $F_{(m)} = F_{m,0} \subset F^{\mathrm{cyc}}$ and $F^{(n)} = F_{0,n} \subset F_\dagger$. Observe that $F_{m,n}$ is the joint of $F_{(m)}$ and $F^{(n)}$. The following diagram summarizes the definitions in this subsection:



Proposition 3.4. *Let m, n be arbitrary positive integers. Then:*

(i) $\operatorname{coker}\big(H^1(F, \mathbb{T}_{\mathrm{cyc}}) \to H^1_{\mathcal{F}_{\mathrm{can}}}(F_{(m)}, T)\big)$ *is finite.*

(ii) *The $\mathfrak{O}[\Gamma_{(m)}]$-module $H^1_{\mathcal{F}_{\mathrm{can}}}(F_{(m)}, T)$ is free of rank g.*

(iii) *The $\mathfrak{O}[\Gamma_{(m)} \times \Gamma^{(n)}]$-module $H^1_{\mathcal{F}_{\mathrm{can}}}(F_{(m,n)}, T)$ is free of rank g.*

Proof. We argue as in Remark 2.16. By Nekovář's control theorem

$$\operatorname{coker}\big(H^1(F, \mathbb{T}_{\mathrm{cyc}}) \to H^1_{\mathcal{F}_{\mathrm{can}}}(F_{(m)}, T)\big) \cong \widetilde{H}^2_f(F_\Sigma/F, T)[\gamma_{\mathrm{cyc}}^{p^m} - 1]$$

and $\widetilde{H}^2_f(F_\Sigma/F_{(m)}, T) \cong H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, \mathbb{T}^*_{\mathrm{cyc}})^\vee$. Since

$$H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, \mathbb{T}^*_{\mathrm{cyc}})^\vee / (\gamma_{\mathrm{cyc}}^{p^m} - 1) \cong H^1_{\mathcal{F}^*_{\mathrm{can}}}(F_{(m)}, T^*)^\vee \cong \mathrm{Cl}(LF_{(m)})^\chi$$

is finite, the characteristic ideal of the torsion Λ_{cyc}-module $H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, \mathbb{T}^*_{\mathrm{cyc}})^\vee$ is prime to $\gamma_{\mathrm{cyc}}^{p^m} - 1$, and by the structure theorem for finitely generated Λ_{cyc}-modules we see that $H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, \mathbb{T}^*_{\mathrm{cyc}})^\vee[\gamma_{\mathrm{cyc}}^{p^m} - 1]$ is finite, concluding the proof of (i).

This argument may be used to prove that $\operatorname{coker}\big(H^1(F, \mathbb{T}_{\mathrm{cyc}}) \to H^1_{\mathcal{F}_{\mathrm{can}}}(F, T)\big)$ is finite, which in turn implies that $\operatorname{coker}\Big(H^1(F_{(m)}, T) \xrightarrow{\mathrm{pr}} H^1_{\mathcal{F}_{\mathrm{can}}}(F, T)\Big)$ is finite as well. Thence the image of the map pr (induced by projection modulo $\gamma_{\mathrm{cyc}} - 1$) is a free $\mathfrak{O}$-module of rank g. It follows by Nakayama's lemma that the $\mathfrak{O}[\Gamma_{(m)}]$-module $H^1(F_{(m)}, T)$ may be generated by at most g elements, say by $\{v_1, \cdots, v_g\}$. On the other hand, it follows from the first part that $H^1(F_{(m)}, T)$ contains a free $\mathfrak{O}[\Gamma_{(m)}]$-module of rank g (isomorphic image of the free module $H^1(F, \mathbb{T}_{\mathrm{cyc}})/(\gamma_{\mathrm{cyc}}^{p^m} - 1)$), say with basis $\{y_1, \cdots, y_g\}$. One may easily verify that any non-trivial $\mathfrak{O}[\Gamma_{(m)}]$-linear relation $\{v_1, \cdots, v_g\}$ would yield a non-trivial $\mathfrak{O}[\Gamma_{(m)}]$-linear relation of $\{y_1, \cdots, y_g\}$, which is impossible. This shows that $\{v_1, \cdots, v_g\}$ is indeed a basis and (ii) follows.

The proof of (iii) follows similarly. We indicate the main steps. First, we verify that the $\mathfrak{O}[[\Gamma_{(m)} \times \Gamma_\dagger]]$-module $H^1_{\mathcal{F}_{\mathrm{can}}}(F_{(m)}, T \otimes \Lambda_\dagger)$ is free of rank g. Next, we check that the map $H^1_{\mathcal{F}_{\mathrm{can}}}(F_{(m)}, T\otimes\Lambda_\dagger) \to H^1_{\mathcal{F}_{\mathrm{can}}}(F_{m,n}, T)$ has finite cokernel, thence $H^1_{\mathcal{F}_{\mathrm{can}}}(F_{m,n}, T)$ contains a free $\mathfrak{O}[\Gamma_{(m)}\times\Gamma^{(n)}]$-module of rank g (with finite index in $H^1_{\mathcal{F}_{\mathrm{can}}}(F_{m,n}, T)$), say again with basis $\{y_1,\cdots,y_g\}$. Furthermore, it follows by Nakayama's lemma that $H^1_{\mathcal{F}_{\mathrm{can}}}(F_{m,n}, T)$ may be generated by at most g elements, say by $\{v_1,\cdots,v_g\}$. It is easy to check as above that a non-trivial linear relation of $\{v_1,\cdots,v_g\}$ would yield a non-trivial relation among $\{y_1,\cdots,y_g\}$, concluding the proof that $\{v_1,\cdots,v_g\}$ is a basis of $H^1_{\mathcal{F}_{\mathrm{can}}}(F_{m,n}, T)$. □

Remark 3.5. By Proposition 3.4(iii) it follows that

$$\varepsilon^\chi_{F_{m,n}} \in \bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(F_{m,n}, T)\,,$$

since we have $\bigwedge_0^g H^1_{\mathcal{F}_{\mathrm{can}}}(F_{m,n}, T) = \bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(F_{m,n}, T)$ by Example 3.2.

Inspired by [PR98, Definition 1.2.2], we propose the following strengthening (along the tower F_∞/F) of the Rubin-Stark conjectures:

Conjecture 3.6 (Strong Rubin-Stark Conjecture). *There exists an element*

$$\mathfrak{S}_\infty = \mathfrak{S}_{\infty,1}\wedge\cdots\wedge\mathfrak{S}_{\infty,g} \in \bigwedge^g H^1(F,\mathbb{T})$$

(where the exterior product is evaluated in the category of Λ-modules) such that for every subextension $F\subset M = F_{m,n}\subset F_\infty$ as above, the image of $\mathfrak{S}_\infty$ under the natural projection to $\bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(M,T)$ is ε^χ_M, the χ-isotypic component of the Rubin-Stark element.

Assuming the truth of the Strong Rubin-Stark Conjecture, we set

$$\mathfrak{S}_{\mathrm{cyc}} = \mathfrak{S}_{\mathrm{cyc},1}\wedge\cdots\wedge\mathfrak{S}_{\mathrm{cyc},g} \in \bigwedge^g H^1(F,\mathbb{T}_{\mathrm{cyc}})$$

to denote the image of $\mathfrak{S}_\infty$.

Remark 3.7. If we knew that neither the Λ-module $\varprojlim_{L\subset M\subset LF_\infty}\mathrm{Cl}(M)^\chi$ nor the Λ_{cyc}-module $\varprojlim_{L\subset M\subset LF^{\mathrm{cyc}}}\mathrm{Cl}(M)^\chi$ has pseudo-null submodules, the Strong Rubin-Stark Conjecture would have been trivial. Indeed in that case, it follows that the maps

$$H^1_{\mathcal{F}_{\mathrm{can}}}(F_{m,n}, T) \longrightarrow H^1_{\mathcal{F}_{\mathrm{can}}}(F_{m',n'}, T)$$

(for positive integers $m\geq m'$ and $n\geq n'$) are surjective and using Proposition 3.4 that

$$\varprojlim \bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(F_{m,n}, T) = \bigwedge^g \varprojlim H^1_{\mathcal{F}_{\mathrm{can}}}(F_{m,n}, T) = \bigwedge^g H^1(F,\mathbb{T})\,.$$

4. Kolyvagin systems for $\mathbb{G}_m$ and E

Until the end of this paper, we assume the truth of Leopoldt's conjecture for L. This in particular shows that $\mathfrak{d}=0$. Let $\mathcal{P}$ be the set of all primes of F that complements the set of primes F at which T is ramified and the set of primes above p. Let

$$\overline{\mathbf{KS}}(\mathbb{T},\mathcal{F}_{\mathcal{L}},\mathcal{P}) := \varprojlim_{k,\bar\alpha}\left(\varinjlim_{\substack{k'\geq k,\\ \bar\beta\succ\bar\alpha}} \mathbf{KS}(\mathbb{T}_{k,\bar\alpha},\mathcal{F}_{\mathcal{L}},\mathcal{P}_{k',\bar\beta})\right)$$

denote the module of $\mathcal{L}$-restricted Kolyvagin systems for the triple $(\mathbb{T}, \mathcal{F}_{\mathcal{L}}, \mathcal{P})$. Here we borrowed notation from [Büy14, Appendix A]; we note for the convenience of the reader that

- we have $r = 3$ in this portion of the current article,
- $\bar{\alpha}$ and $\bar{\beta}$ stand for triples of positive integers, and
- our $\mathcal{F}_{\mathcal{L}}$ corresponds to $\mathcal{F}_{\mathcal{L}_\infty}$ in [Büy14].

We similarly define the modules $\overline{\mathbf{KS}}(X, \mathcal{F}, \mathcal{P})$ where $(X, \mathcal{F})$ is one of the pairs $(\mathbb{T}_{\mathrm{cyc}}, \mathcal{F}_{\mathcal{L}})$, $(T, \mathcal{F}_{\mathcal{L}})$, $(\mathbb{T}(E), \mathcal{F}_{\mathbb{L}})$ or $(\mathbb{T}_{\mathrm{cyc}}(E), \mathcal{F}_{\mathbb{L}})$.

It follows from [MR04, Theorem 5.1.1] and Lemma 2.31 that the k-vector space $\mathbf{KS}(\overline{T}, \mathcal{F}, \mathcal{P})$ has dimension one ($\mathcal{F} = \mathcal{F}_{\mathcal{L}}$ or $\mathcal{F}_{\mathbb{L}}$). The following theorem asserts that these Kolyvagin systems may be lifted to various deformations of $\overline{T}$.

Theorem 4.1.

(i) *Both Λ-modules of $\overline{\mathbf{KS}}(\mathbb{T}, \mathcal{F}_{\mathcal{L}}, \mathcal{P})$ and $\overline{\mathbf{KS}}(\mathbb{T}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P})$, as well as the Λ_{cyc}-modules $\overline{\mathbf{KS}}(\mathbb{T}, \mathcal{F}_{\mathcal{L}}, \mathcal{P})$ and $\overline{\mathbf{KS}}(\mathbb{T}_{\mathrm{cyc}}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P})$ and the $\mathfrak{O}$-module $\overline{\mathbf{KS}}(T, \mathcal{F}_{\mathcal{L}}, \mathcal{P})$ are free of rank one.*

(ii) *All five free modules in* (i) *are generated by a **primitive** Kolyvagin system $\boldsymbol{\kappa}$, namely by a Kolyvagin system whose image $\bar{\boldsymbol{\kappa}} \in \mathbf{KS}(\overline{T}, \mathcal{F}, \mathcal{P})$ (where $\mathcal{F} = \mathcal{F}_{\mathcal{L}}$ or $\mathcal{F}_{\mathbb{L}}$ depending on which module of Kolyvagin systems we are talking about) is non-zero.*

Proof. The assertions in (i) and (ii) over $\mathfrak{O}$ are [MR04, Theorem 5.2.10], and over Λ or Λ_{cyc}, they both follow from [Büy14, Theorem A.14]. □

The following theorem summarizes the main applications of the Kolyvagin systems, whose existence is guaranteed by the previous theorem. Let $(R, X, \mathcal{F})$ be any one of the five triples $(\mathfrak{O}, T, \mathcal{F}_{\mathcal{L}})$, $(\Lambda_{\mathrm{cyc}}, \mathbb{T}_{\mathrm{cyc}}, \mathcal{F}_{\mathcal{L}})$, $(\Lambda, \mathbb{T}, \mathcal{F}_{\mathcal{L}})$, $(\Lambda_{\mathrm{cyc}}, \mathbb{T}_{\mathrm{cyc}}(E), \mathcal{F}_{\mathbb{L}})$ or $(\Lambda, \mathbb{T}(E), \mathcal{F}_{\mathbb{L}})$.

Theorem 4.2. *Suppose that $\boldsymbol{\kappa} \in \overline{\mathbf{KS}}(X, \mathcal{F}, \mathcal{P})$ is a Kolyvagin system whose initial term $\kappa_1 \in H^1_{\mathcal{F}}(F, X)$ is non-zero.*

(i) *The R-module $H^1_{\mathcal{F}^*}(F, X^*)^\vee$ is R-torsion, and the R-module $H^1_{\mathcal{F}}(F, X)$ has rank one.*

(ii) *If $R = \mathfrak{O}$, then $\# H^1_{\mathcal{F}^*}(F, X^*)^\vee \mid \# \left(H^1_{\mathcal{F}}(F, X)/R \cdot \kappa_1\right)$. If $R = \Lambda$ or Λ_{cyc}, then*
$$\mathrm{char}\left(H^1_{\mathcal{F}^*}(F, X^*)^\vee\right) \mid \mathrm{char}\left(H^1_{\mathcal{F}}(F, X)/R \cdot \kappa_1\right) .$$

(iii) *When $R = \mathfrak{O}$ or $R = \Lambda_{\mathrm{cyc}}$, we have equality in the divisibilities of* (ii) *if and only if the Kolyvagin system $\boldsymbol{\kappa}$ is primitive.*

Proof. When $R = \mathfrak{O}$ all assertions follow from [MR04, §5.2]. The arguments of [MR04, §5.3] essentially verify all three assertions when $R = \Lambda_{\mathrm{cyc}}$ as well. Here we provide a sketch of their proof in that case.

For (i), we may choose a height one prime ideal $\wp = (\gamma_{\mathrm{cyc}} - 1 + p^N)$ of Λ_{cyc} (where $N \in \mathbb{Z}^+$) such that

- $\Lambda_{\mathrm{cyc}}/(\gamma_{\mathrm{cyc}} - 1) \cong \Lambda_{\mathrm{cyc}}/\wp$,
- the image $\kappa_1^\wp \in H^1_{\mathcal{F}}(F, X \otimes \Lambda/\wp)$ of κ_1 is non-zero.

Note that $\kappa_1^\wp$ is the initial term of the Kolyvagin system $\boldsymbol{\kappa}^\wp \in \overline{\mathbf{KS}}(X \otimes \Lambda/\mathfrak{P}, \mathcal{F}, \mathcal{P})$ and it follows from (i) applied with $R = \Lambda/\wp \cong \mathfrak{O}$ that the $\Lambda/\wp$-module
$$H^1_{\mathcal{F}^*}\left(F, (X \otimes \Lambda/\wp)^*\right)^\vee = H^1_{\mathcal{F}^*}\left(F, X^*[\wp]\right)^\vee \cong H^1_{\mathcal{F}^*}\left(F, X^*\right)^\vee / \wp H^1_{\mathcal{F}^*}\left(F, X^*\right)^\vee$$

is finite. This shows by the structure theorem for finitely generated Λ_{cyc}-modules that the Λ_{cyc}-module $H^1_{\mathcal{F}^*}(F, X^*)^\vee$ is torsion. Since the module

$$H^1_{\mathcal{F}^*}\left(F, (X \otimes \Lambda/\wp)^*\right)^\vee$$

is finite, it follows from Lemma 2.31 that $H^1_{\mathcal{F}}(F, X \otimes \Lambda/\wp)$ has $\Lambda/\wp$-rank one. Furthermore, as we have a natural injection

$$H^1_{\mathcal{F}}(F, X)/\wp H^1_{\mathcal{F}}(F, X) \hookrightarrow H^1_{\mathcal{F}}(F, X \otimes \Lambda/\wp)\ ,$$

it follows by Nakayama's lemma that the Λ_{cyc}-module $H^1_{\mathcal{F}}(F, X)$ is cyclic. On the other hand, since κ_1 is a non-zero element of the Λ_{cyc}-torsion free module $H^1_{\mathcal{F}}(F, X)$, it follows that $H^1_{\mathcal{F}}(F, X)$ has positive Λ_{cyc}-rank. This concludes the proof of (i) when $R = \Lambda_{\mathrm{cyc}}$.

We next sketch a proof of (ii) when $R = \Lambda_{\mathrm{cyc}}$. Fix a pseudo-isomorphism

$$H^1_{\mathcal{F}^*}(F, X^*)^\vee \longrightarrow \bigoplus_i \Lambda_{\mathrm{cyc}}/\mathfrak{P}^{m_i} \oplus \left(\bigoplus_j \Lambda_{\mathrm{cyc}}/f_j\Lambda_{\mathrm{cyc}}\right)$$

where $\mathfrak{P}$ is any height one prime dividing $\mathrm{char}\left(H^1_{\mathcal{F}^*}(F, X^*)^\vee\right)$ and where each f_j is prime to $\mathfrak{P}$. We are content to prove that

$$\sum_i m_i \leq \mathrm{ord}_{\mathfrak{P}}\,\mathrm{char}\left(H^1_{\mathcal{F}}(F, X)/\Lambda_{\mathrm{cyc}} \cdot \kappa_1\right)\ , \tag{4.1}$$

from which (ii) follows. We will assume that $p \notin \mathfrak{P}$ and therefore $\mathfrak{P}$ is generated by a distinguished polynomial $P \in \Lambda_{\mathrm{cyc}} = \mathfrak{O}[[\gamma_{\mathrm{cyc}} - 1]]$. For a general height one prime $\mathfrak{Q}$ of Λ_{cyc} , let $S_{\mathfrak{Q}}$ denote the integral closure of $\Lambda_{\mathrm{cyc}}/\mathfrak{Q}$. Note that $[S_{\mathfrak{Q}} : \Lambda_{\mathrm{cyc}}/\mathfrak{Q}]$ is finite. Set $\mathfrak{P}_N = (P + \pi^N)$, where N is a positive integer (chosen sufficiently large to ensure that $\mathfrak{P}_N$ is a prime ideal). Write $X_N = (X \otimes \Lambda_{\mathrm{cyc}}/\mathfrak{P}) \otimes S_{\mathfrak{P}_N}$. It follows from our assumption (1.2) that we have injections

$$\iota : H^1(G_\Sigma, X \otimes \Lambda_{\mathrm{cyc}}/\mathfrak{P}_N) \hookrightarrow H^1(G_\Sigma, X_N)$$

and

$$\iota_p : H^1(F_p, X \otimes \Lambda_{\mathrm{cyc}}/\mathfrak{P}_N) \hookrightarrow H^1(F_p, X_N)$$

with finite cokernels (whose size depends only on $[S_{\mathfrak{P}} : \Lambda_{\mathrm{cyc}}/\mathfrak{P}]$). Define the Selmer structure $\mathcal{F}$ on X_N by setting

$$H^1_{\mathcal{F}}(F_\lambda, X_N) = \ker\left(H^1(F_\lambda, X_N) \longrightarrow H^1(F_\lambda^{\mathrm{ur}}, X_N \otimes \mathbb{Q}_p)\right)$$

for $\lambda \nmid p$ (this would be the local condition denoted by $H^1_{\mathcal{F}_{\mathrm{can}}}(F_\lambda, X_N)$ in the notation of [MR04]) and by defining $H^1_{\mathcal{F}}(F_p, X_N)$ as the $S_{\mathfrak{P}_N}$-saturation of

$$\iota_p\left(H^1_{\mathcal{F}}(F_p, X \otimes \Lambda_{\mathrm{cyc}}/\mathfrak{P}_N)\right).$$

As explained in the proof of Theorem 5.3.10 of [MR04], for every sufficiently large positive integer N we have:

1. $\Lambda_{\mathrm{cyc}}/\mathfrak{P}_N \cong \Lambda_{\mathrm{cyc}}/\mathfrak{P}$,
2. the image $\kappa_1^{\mathfrak{P}_N} \in H^1_{\mathcal{F}}(F, X_N)$ of κ_1 is non-zero,
3. $\mathrm{coker}\left(H^1_{\mathcal{F}}(F, X)/\mathfrak{P}_N H^1_{\mathcal{F}}(F, X) \hookrightarrow H^1_{\mathcal{F}}(F, X_N)\right)$ is finite with order bounded by a constant independent of N,
4. $\mathfrak{P}_N$ is prime to f_j for every j.

Only the verification of (3) requires a slight enhancement of [MR04, Proposition 5.3.14] (so as to apply with the Selmer structure $\mathcal{F}$ in place of the Selmer structure $\mathcal{F}_\Lambda$ in [MR04]). This shows, proceeding as in the proof of Theorem 5.3.10 of [MR04] (essentially, by only making use of the Kolyvagin system $\boldsymbol{\kappa}^{\mathfrak{P}_N} \in \overline{\mathbf{KS}}(X_N, \mathcal{F}, \mathcal{P})$ over the one-dimensional ring $S_{\mathfrak{P}_N}$) that

$$\begin{aligned} Nr\sum_i m_i + O(1) &= \mathrm{length}_{\mathbb{Z}_p} H^1_{\mathcal{F}^*}(F, X^*)[\mathfrak{P}_N] = \mathrm{length}_{\mathbb{Z}_p} H^1_{\mathcal{F}^*}\left(F, (X/\mathfrak{P}_N)^*\right) \\ &\leq \mathrm{length}_{\mathbb{Z}_p} H^1_{\mathcal{F}^*}(F, X_N^*) + O(1) \\ &\leq \mathrm{length}_{\mathbb{Z}_p} \left(H^1_{\mathcal{F}}(F, X_N)/S_{\mathfrak{P}_N} \cdot \kappa_1^{\mathfrak{P}_N}\right) + O(1) \\ &= \mathrm{length}_{\mathbb{Z}_p} \left(\left(H^1_{\mathcal{F}}(F, X)/\Lambda_{\mathrm{cyc}} \cdot \kappa_1\right) \otimes \Lambda_{\mathrm{cyc}}/\mathfrak{P}_N\right) + O(1) \\ &= Nr \,\mathrm{ord}_{\mathfrak{P}}\, \mathrm{char}\left(H^1_{\mathcal{F}}(F, X)/\Lambda_{\mathrm{cyc}} \cdot \kappa_1\right) + O(1) \end{aligned}$$

where $r = \mathrm{rank}_{\mathbb{Z}_p} S_{\mathfrak{P}}$. (4.1) now follows (for characteristic zero primes $\mathfrak{P}$) taking N sufficiently large in the inequality above. In case $p \in \mathfrak{P}$, we proceed by considering the ideals $\mathfrak{P}_N = (\pi + (\gamma_{\mathrm{cyc}} - 1)^N)$ and conclude the proof.

When $R = \Lambda$, we may make use of the arguments of Ochiai in [Och05, §3] in order to reduce the assertions in (i) and (ii) to the case of a dimension-two regular ring. As details pertaining to this point will soon be available (in much greater generality) as part of our forthcoming joint work with T. Ochiai, we indicate here only the key points. We follow the terminology of [Och05, §3]. First of all, our argument above when $R = \Lambda_{\mathrm{cyc}}$ shows that for all but finitely many *linear elements* $l \in \Lambda$, we have (i) and (ii) for the $\Lambda/(l)$-module $\mathbb{T} \otimes \Lambda/(l)$. As the second step, one makes use of this input together with control theorems for the $\mathcal{F}_{\mathcal{L}}$-Selmer groups (which are in fact easier than those relevant to considerations in [Och05], due to the fact that $\mathbb{T} = T \otimes \Lambda$ is a rather simple Galois deformation) as well [Och05, Proposition 3.6] (which characterizes the characteristic ideal of a torsion Λ-module M in terms of the characteristic ideals of the quotients M/lM as $\Lambda/(l)$-modules) to finish the proof. □

Corollary 4.3. *Suppose $\boldsymbol{\kappa} \in \overline{\mathbf{KS}}(\mathbb{T}_{\mathrm{cyc}}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P})$ is a Kolyvagin system with non-vanishing initial term $\kappa_1 \in H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T}_{\mathrm{cyc}}(E))$. Then $H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, \mathbb{T}_{\mathrm{cyc}}(E)^*)^\vee$ is a torsion Λ_{cyc}-module, and the weak Leopoldt conjecture for E holds true.*

Proof. This follows from Theorem 4.2(i) and the obvious injection

$$H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, \mathbb{T}_{\mathrm{cyc}}(E)^*) \hookrightarrow H^1_{\mathcal{F}^*_{\mathbb{L}}}(F, \mathbb{T}_{\mathrm{cyc}}(E)^*) \,.$$

□

Proposition 4.4. *Let $\boldsymbol{\kappa} \in \overline{\mathbf{KS}}(\mathbb{T}, \mathcal{F}_{\mathbb{L}}, \mathcal{P})$ be a Kolyvagin system with initial term $0 \neq \kappa_1 \in H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T})$ and let $\widetilde{\boldsymbol{\kappa}} \in \overline{\mathbf{KS}}(\mathbb{T}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P})$ with initial term* $\mathrm{tw}(\kappa_1) \in$ *$H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T}(E))$. Suppose that*

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

Then,

(i) $\mathrm{char}\left(H^1_{\mathcal{F}^*_{\mathbb{L}}}(F, \mathbb{T}(E)^*)^\vee\right) = \mathrm{char}\left(H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T}(E))/\Lambda \cdot \mathrm{tw}\,(\kappa_1)\right).$

(ii) *The Kolyvagin system $\widetilde{\boldsymbol{\kappa}}$ and its image $\pi_{\mathrm{cyc}}\,(\widetilde{\boldsymbol{\kappa}}) \in \overline{\mathbf{KS}}(\mathbb{T}_{\mathrm{cyc}}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P})$ are both primitive.*

(iii) *Let* $\mathfrak{K}_1 \in H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T}_{\mathrm{cyc}}(E))$ *be the initial term of the Kolyvagin system* $\pi_{\mathrm{cyc}}(\widetilde{\boldsymbol{\kappa}})$*. Then*

$$\mathrm{char}\left(H^1_{\mathcal{F}^*_{\mathbb{L}}}(F, \mathbb{T}_{\mathrm{cyc}}(E)^*)^\vee\right) = \mathrm{char}\left(H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T}_{\mathrm{cyc}}(E))/\Lambda_{\mathrm{cyc}} \cdot \mathfrak{K}_1\right).$$

Proof. (i) follows using a formal twisting argument; cf. Lemma VI.1.2 and Theorem VI.4.1 of [Rub00].

Let $\mathfrak{g} \in \overline{\mathbf{KS}}(\mathbb{T}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P})$ be a generator and let g_1 be its initial term. Write $\widetilde{\boldsymbol{\kappa}} = r \cdot \mathfrak{g}$ (where $r \in \Lambda$) so that $\mathrm{tw}\,(\kappa_1) = r \cdot g_1$. It follows from (i) and Theorem 4.2(ii) that

$$\begin{aligned}\mathrm{char}\left(H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T}(E))/\Lambda \cdot rg_1\right) &= \mathrm{char}\left(H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T}(E))/\Lambda \cdot \mathrm{tw}\,(\kappa_1)\right)\\ &\mid \mathrm{char}\left(H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T}(E))/\Lambda \cdot g_1\right),\end{aligned}$$

which shows that $r \in \Lambda^\times$, proving the first assertion in (ii). It now follows from Theorem 4.1(ii) that the image $\overline{\boldsymbol{\kappa}} \in \mathbf{KS}(\overline{T}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P})$ of $\widetilde{\boldsymbol{\kappa}}$ is non-zero, and the second assertion in (ii) holds true by the commutative diagram

$$\begin{tikzcd}
\overline{\mathbf{KS}}(\mathbb{T}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P}) \arrow[rr, "\pi_{\mathrm{cyc}}"] \arrow[dr] & & \overline{\mathbf{KS}}(\mathbb{T}_{\mathrm{cyc}}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P}) \arrow[dl] \\
& \mathbf{KS}(\overline{T}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P}) &
\end{tikzcd}$$

and by Theorem 4.1(ii). The final portion of the proposition follows now from (ii) and Theorem 4.2(iii). □

4.1. **Rubin-Stark $\mathcal{L}$-restricted Kolyvagin systems.** The purpose of this section is to construct the $\mathcal{L}$-restricted Kolyvagin systems $\mathbb{T}$ (we proved they exist unconditionally in the previous section) out of the Rubin-Stark elements. In order to do so, we will first construct an Euler system of rank one (namely, an Euler system in the sense of [Rub00]) that enjoys additional local properties at p. We will then apply Kolyvagin's descent on this Euler system.

Definition 4.5.

(i) For $X = T$ or $T(E)$, let $\mathrm{ES}(X) = \mathrm{ES}(X, \mathfrak{E})$ denote the collection of Euler systems for X in the sense of [Rub00, §2].

(ii) Let $\mathfrak{L} \subset \mathcal{V}^+_{K(\mathfrak{E})}$ be a $\mathfrak{O}[[\mathfrak{G}(K(\mathfrak{E}))]]$-direct summand as in Definition 2.9. An Euler system $\mathbf{c} = \{c_{\mathcal{K}}\} \in \mathrm{ES}(T)$ is called an $\mathfrak{L}$*-restricted Euler system* if

$$\mathrm{loc}_p(c_{\mathcal{K}}) \in \mathcal{V}^-_{\mathcal{K}} \oplus \mathfrak{l}_{\mathcal{K}}$$

for every $\mathcal{K} \in \mathfrak{E}$. The module of $\mathfrak{L}$-restricted Euler systems for T is denoted by $\mathrm{ES}_{\mathfrak{L}}(T)$. We similarly define the module of $\mathbb{L}$-restricted Euler systems $\mathrm{ES}_{\mathbb{L}}(T(E))$ for $T(E)$.

Theorem 4.6 (Mazur-Rubin)**.** *For $X = T$ or $T(E)$, there is a canonical map*

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

with the property that if $\mathbf{c} = \{c_{\mathcal{K}}\}_{\mathcal{K} \in \mathfrak{E}} \in \mathrm{ES}(X)$ *maps to* $\boldsymbol{\kappa} \in \overline{\mathbf{KS}}(X \otimes \Lambda, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$*, then*

$$\kappa_1 = \{c_M\} \in \varprojlim_M H^1(M, X) = H^1(F, X \otimes \Lambda),$$

where the inverse limit is over the finite subextensions M of F_∞/F.

For any field $\mathcal{K} \in \mathfrak{E}$, recall that $\Delta_{\mathcal{K}} := \mathrm{Gal}(\mathcal{K}/F)$ and write $\delta_{\mathcal{K}} = |\Delta_{\mathcal{K}}|$. Let $\varPhi = \{\varphi_{\mathcal{K}}\}$ be any element of $\varprojlim_{\mathcal{K}\in\mathfrak{E}} \bigwedge^{r-1} \mathrm{Hom}_{\mathfrak{O}[\Delta_{\mathcal{K}}]}\left(H^1(\mathcal{K},T), \mathfrak{O}[\Delta_K]\right)$. As explained in [Rub96, §1.2], there is a natural map

$$\bigwedge^{r-1} \mathrm{Hom}_{\mathfrak{O}[\Delta_{\mathcal{K}}]}\left(H^1(\mathcal{K},T), \mathfrak{O}[\Delta_K]\right) \longrightarrow \mathrm{Hom}_{\mathfrak{O}[\Delta_{\mathcal{K}}]}\left(\bigwedge^{g} H^1(\mathcal{K},T), H^1(\mathcal{K},T)\right).$$

We denote the image of $\varphi_{\mathcal{K}}$ under this map still by $\varphi_{\mathcal{K}}$. Given a collection $\varPhi = \{\varphi_{\mathcal{K}}\}$ as above, we obtain an element $\varphi_{\mathcal{K}}(\varepsilon_{\mathcal{K}}^{\chi}) \in H^1(\mathcal{K},T)$ by the defining (integrality) property of the elements $\varepsilon_{\mathcal{K}}^{\chi} \in \frac{1}{\delta_{\mathcal{K}}} \bigwedge^g H^1(\mathcal{K},T)$. In other words, the denominators $\delta_{\mathcal{K}}$ disappear once we apply the homomorphisms $\varphi_{\mathcal{K}}$.

Theorem 4.7 (Perrin-Riou, Rubin). *$c_{\varPhi}^{\chi} := \{\varphi_{\mathcal{K}}(\varepsilon_{\mathcal{K}}^{\chi})\} \in \mathrm{ES}(T)$.*

Proof. This is proved in [PR98, §1.2.3]; see also [Rub96, §6]. □

Localization followed by projection to $\mathcal{V}_{\mathcal{K}}^{+}$ induces a canonical homomorphism

(4.2)
$$\varprojlim_{\mathcal{K}\in\mathfrak{E}} \bigwedge^{r-1} \mathrm{Hom}_{\mathfrak{O}[\Delta_{\mathcal{K}}]}\left(\mathcal{V}_{\mathcal{K}}^{+}, \mathfrak{O}[\Delta_{\mathcal{K}}]\right) \longrightarrow \varprojlim_{\mathcal{K}\in\mathfrak{E}} \bigwedge^{r-1} \mathrm{Hom}_{\mathfrak{O}[\Delta_{\mathcal{K}}]}\left(H^1(\mathcal{K},T_{\chi}), \mathfrak{O}[\Delta_{\mathcal{K}}]\right).$$

If $\varPhi$ is an element of the left side of (4.2), its image under this homomorphism will still be denoted by the same symbol.

The following theorem tells us how to obtain $\mathfrak{L}$-restricted Euler systems (and $\mathcal{L}$-restricted Kolyvagin systems) starting with the Rubin-Stark Euler system $\mathcal{C}_{\text{R-S}}^{(g)}$ of rank g.

Theorem 4.8. *Recall the quotients $\mathcal{Q} = H^1(F_p,\mathbb{T})/\mathcal{V}$, $\mathcal{Q}_{\mathrm{cyc}} = H^1(F_p,\mathbb{T}_{\mathrm{cyc}})/\mathcal{V}_{\mathrm{cyc}}$.*

- (i) *There exists an element $\Psi = \{\psi_{\mathcal{K}}\} \in \varprojlim_{\mathcal{K}\in\mathfrak{E}} \bigwedge^{r-1} \mathrm{Hom}_{\mathfrak{O}[\Delta_{\mathcal{K}}]}\left(\mathcal{V}_{K}^{+}, \mathfrak{O}[\Delta_{\mathcal{K}}]\right)$ such that $\psi_{\mathcal{K}}$ maps $\bigwedge^g \mathcal{V}_{\mathcal{K}}^{+}$ isomorphically onto $\mathcal{L}_{\mathcal{K}}$ (likewise, $\bigwedge^g \mathcal{Q}_{\mathrm{cyc}}$ to $\mathcal{L}_{\mathrm{cyc}}$ and $\bigwedge^g \mathcal{Q}$ to $\mathcal{L}$).*
- (ii) *For Ψ as in* (i)*, $\boldsymbol{c}_{\Psi}^{\chi} := \{\psi_{\mathcal{K}}(\varepsilon_{\mathcal{K}}^{\chi})\} \in \mathrm{ES}_{\mathfrak{L}}(T)$.*
- (iii) *Let $\boldsymbol{\kappa}^{\text{R-S}} \in \overline{\mathbf{KS}}(\mathbb{T}, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ be the image of $\boldsymbol{c}_{\Psi}^{\chi}$ under the Euler systems to the Kolyvagin systems map of Theorem* 4.6*. Then $\boldsymbol{\kappa}^{\text{R-S}} \in \overline{\mathbf{KS}}(\mathbb{T}, \mathcal{F}_{\mathcal{L}}, \mathcal{P})$; i.e., $\boldsymbol{\kappa}^{\text{R-S}}$ is an $\mathcal{L}$-restricted Kolyvagin system.*

Proof. (i) may be proved mimicking the arguments of [Büy10, §3.3.1]. To prove (ii) and (iii), one makes use of Proposition 2.3 and adapts (completely formally) the proof of Theorem 3.25 of [Büy10]. □

Let $c_{F,\Psi}^{\chi} := \psi_F(\varepsilon_F^{\chi}) \in H^1_{\mathcal{F}_{\mathfrak{L}}}(F,T)$ denote the initial term of the $\mathfrak{L}$-restricted Euler system $\mathbf{c}_{\Psi}^{\chi}$. Similarly, define $c_{F_{\mathrm{cyc}},\Psi}^{\chi} = \{c_{M,\Psi}^{\chi}\} \in \varprojlim_{M\subset F_{\mathrm{cyc}}} H^1(M,T) = H^1(F,\mathbb{T}_{\mathrm{cyc}})$ and $c_{F_{\infty},\Psi}^{\chi} = \{c_{M,\Psi}^{\chi}\} \in \varprojlim_{M\subset F_{\infty}} H^1(M,T) = H^1(F,\mathbb{T})$, where the inverse limit is over the finite subextensions M of F_{∞}/F.

Proposition 4.9. *$c_{F,\Psi}^{\chi} \neq 0$.*

Proof. This follows from the proof of Proposition 6.6 in [Rub96] since we assumed Leopoldt's conjecture. □

Remark 4.10. Definition VI.3.1 [Rub00] equips us with a *twisting morphism* $\mathrm{ES}(T) \to \mathrm{ES}(T(E))$, which then evidently restricts to a map $\mathrm{ES}_{\mathbb{L}}(T) \to \mathrm{ES}_{\mathbb{L}}(T(E))$ on the $\mathbb{L}$-restricted Euler systems. Let $\mathbf{c}_\Psi(E)\in \mathrm{ES}_{\mathbb{L}}(T(E))$ denote the image of $\mathbf{c}_\Psi^\chi$. Then the image $\boldsymbol{\kappa}^{\text{R-S}}(E)$ of $\mathbf{c}_\Psi(E)$ under the map of Theorem 4.6 (applied with $X=T(E)$) lies in $\overline{\mathbf{KS}}(\mathbb{T}(E),\mathcal{F}_{\mathbb{L}},\mathcal{P})$. The initial term $\kappa_1^E\in H^1_{\mathcal{F}_{\mathbb{L}}}(F,\mathbb{T}(E))$ of the Kolyvagin system $\boldsymbol{\kappa}^{\text{R-S}}(E)$ may be explicitly described: $\kappa_1^E=\mathrm{tw}\left(c^\chi_{F_\infty,\Psi}\right)$. In particular, it follows from Proposition 4.9 that $\kappa_1^E\neq 0$.

5. Gras' conjecture and CM main conjectures over F

Although our sights are set ultimately on the arithmetic of CM elliptic curves defined over F^+, we present the following results for $\mathbb{G}_m$, first of which may be thought of as a generalization of Gras' conjecture and second and third as the one- and two-variable main conjectures for the CM field F. We will later use these results to promote all inequalities we shall obtain using the Rubin-Stark Euler/Kolyvagin systems for $T(E)$ of Remark 4.10 into equalities.

We assume until the end of this article that the following hypothesis on S holds true (recall as well that we assume the truth of the Rubin-Stark conjectures and Leopoldt's conjecture for L):

(**H.S**) The set S that appears in the definition of Rubin-Stark elements (see the start of Section 3) contains no non-archimedean prime of F that splits in L/F.

Definition 5.1. Let $\mathcal{A}^\chi_{\mathrm{cyc}}=\varprojlim_{M\subset LF_{\mathrm{cyc}}}\mathrm{Cl}(M)^\chi$ and similarly $\mathcal{A}^\chi_\infty=\varprojlim_{M\subset LF_\infty}\mathrm{Cl}(M)^\chi$. We have the identifications (by class field theory)

$$\mathcal{A}^\chi_{\mathrm{cyc}}=H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,\mathbb{T}^*_{\mathrm{cyc}})^\vee \quad\text{and}\quad \mathcal{A}^\chi_\infty=H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,\mathbb{T}^*)^\vee\,.$$

Theorem 5.2.

(i) $\#\,\mathrm{Cl}(L)^\chi=[\bigwedge^g\mathcal{O}_L^{\times,\chi}:\mathfrak{O}\cdot\varepsilon_F^\chi]$, *and the Rubin-Stark $\mathcal{L}$-restricted Kolyvagin system $\boldsymbol{\kappa}^{\text{R-S}}\in\overline{\mathbf{KS}}(\mathbb{T},\mathcal{F}_{\mathcal{L}},\mathcal{P})$ is primitive.*

If in addition the Strong Rubin-Stark Conjecture holds true, then

(ii) $\mathrm{char}\left(\mathcal{A}^\chi_{\mathrm{cyc}}\right)=\mathrm{char}\left(\bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T}_{\mathrm{cyc}})/\Lambda_{\mathrm{cyc}}\cdot\mathfrak{S}_{\mathrm{cyc}}\right)$.

(iii) $\mathrm{char}\left(\mathcal{A}^\chi_\infty\right)=\mathrm{char}\left(\bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T})/\Lambda\cdot\mathfrak{S}_\infty\right)$.

Proof. It follows from Theorem 4.2(i) and Proposition 4.9 that $H^1_{\mathcal{F}^*_{\mathcal{L}}}(F,T^*)$ is finite, the Λ_{cyc}-module $H^1_{\mathcal{F}^*_{\mathcal{L}}}(F,\mathbb{T}^*_{\mathrm{cyc}})^\vee$ and the Λ-module $H^1_{\mathcal{F}^*_{\mathcal{L}}}(F,\mathbb{T}^*)^\vee$ are torsion. Furthermore, by Theorem 4.2(ii) we have

$$\mathrm{Fitt}(H^1_{\mathcal{F}^*_{\mathcal{L}}}(F,T^*)^\vee)\mid\mathrm{Fitt}(H^1_{\mathcal{F}_{\mathcal{L}}}(F,T)/\mathfrak{O}\cdot c^\chi_{F,\Psi})\,,$$

$$\mathrm{char}\left(H^1_{\mathcal{F}^*_{\mathcal{L}}}(F,\mathbb{T}^*_{\mathrm{cyc}})^\vee\right)\mid\mathrm{char}\left(H^1_{\mathcal{F}_{\mathcal{L}}}(F,\mathbb{T}_{\mathrm{cyc}})/R\cdot c^\chi_{F_{\mathrm{cyc}},\Psi}\right)\,, \tag{5.1}$$

$$\mathrm{char}\left(H^1_{\mathcal{F}^*_{\mathcal{L}}}(F,\mathbb{T}^*)^\vee\right)\mid\mathrm{char}\left(H^1_{\mathcal{F}_{\mathcal{L}}}(F,\mathbb{T})/\Lambda\cdot c^\chi_{F_\infty,\Psi}\right)\,.$$

It is these divisibilities we shall upgrade to equalities (and conclude with the proof of the theorem) with the aid of an analytic class number formula. In order to save space, we shall do this simultaneously. To that end, let R denote any of the coefficient rings $\mathfrak{O},\Lambda_{\mathrm{cyc}}$ or Λ. Correspondingly, let X stand for one of the representations $T,\mathbb{T}_{\mathrm{cyc}}$ or $\mathbb{T}$; V for one of the submodules $\mathcal{V}^+_F,\mathcal{V}_{\mathrm{cyc}}$, or $\mathcal{V}$ (of $H^1(F_p,X)$); D for one of the R-lines $\mathfrak{l},\mathcal{L}_{\mathrm{cyc}}$ or $\mathcal{L}$; c for one of the elements $c^\chi_{F,\Psi},c^\chi_{F_{\mathrm{cyc}},\Psi}$ or $c^\chi_{F_\infty,\Psi}$ and ε for ε^χ_F (when we assume the Strong Rubin-Stark Conjecture, for one of $\mathfrak{S}_{\mathrm{cyc}}$ and

$\mathfrak{G}_\infty$ as well). Let $Q = H^1(F_p, X)/V$, a free R-module of rank g. Define the map $\mathrm{loc}_{/V}$ to be the compositum of the maps

$$\mathrm{loc}_{/V} : H^1_{\mathcal{F}_{\mathrm{can}}}(F, X) \longrightarrow H^1(F_p, X) \longrightarrow Q\,.$$

Note that this map is injective by our choice of U. By slight abuse, we denote the isomorphic image of D inside Q also by D. Note with this convention that the map $\mathrm{loc}_{/V}$ induces an injection $\mathrm{loc}_{/V} : H^1_{\mathcal{F}_{\mathcal{L}}}(F, X) \to D$. Henceforth, whenever the element ε is used with a coefficient ring R other than $\mathfrak{O}$, we implicitly assume the Strong Rubin-Stark Conjecture. When $R = \mathfrak{O}$, we mean by the characteristic ideal of a torsion R-module its initial Fitting ideal.

As we have indicated in the statement of Theorem 4.8, Ψ induces an isomorphism $\Psi : \bigwedge^g Q \to D$ and furthermore verifies that $\mathrm{loc}_{/V}(c) = \Psi(\mathrm{loc}_{/V}(\varepsilon))$ (in fact by its very choice). We therefore have

$$(5.2)\quad R\cdot \mathrm{loc}_{/V}(c) = \mathrm{Fitt}\left(\bigwedge^g Q/R\cdot \mathrm{loc}_{/V}(\varepsilon)\right) D = \mathrm{char}\left(\bigwedge^g Q/R\cdot \mathrm{loc}_{/V}(\varepsilon)\right) D.$$

Furthermore, the following sequences are exact:

$$0 \longrightarrow H^1_{\mathcal{F}_{\mathcal{L}}}(F, X) \longrightarrow H^1_{\mathcal{F}_{\mathrm{can}}}(F, X) \overset{\mathrm{loc}_{/V}}{\longrightarrow} Q/D,$$

$$0 \longrightarrow H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, X^*) \longrightarrow H^1_{\mathcal{F}^*_{\mathcal{L}}}(F, X^*) \overset{\mathrm{loc}^*_{/V}}{\longrightarrow} H^1_{\mathcal{F}^*_{\mathcal{L}}}(F_p, X^*)/H^1_{\mathcal{F}^*_{\mathrm{can}}}(F_p, X^*).$$

Global duality states that the images of $\mathrm{loc}_{/V}$ and $\mathrm{loc}^*_{/V}$ are orthogonal complements. Hence

(5.3)
$$\mathrm{char}\left(\frac{H^1_{\mathcal{F}^*_{\mathcal{L}}}(F, X^*)^\vee}{H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, X^*)^\vee}\right) = \mathrm{char}(\mathrm{coker}(\mathrm{loc}_{/V})) = \mathrm{char}\left(\frac{Q}{D + \mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F, T))}\right).$$

Observe further that

$$\begin{aligned}\frac{Q}{D + \mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F, T))} &\cong \frac{Q/\mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F, T))}{(D + \mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F, T)))/\mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F, T))}\\ &\cong \frac{Q/\mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F, T))}{D/\big(\mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F, T)) \cap D\big)}\\ &\cong \frac{Q/\mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F, T))}{D/\mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathcal{L}}}(F, T))}\ .\end{aligned}$$

This together with (5.3) and (5.1) proves that

$$\begin{aligned}\mathrm{char}(H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, X^*)^\vee) &= \mathrm{char}(H^1_{\mathcal{F}^*_{\mathcal{L}}}(F, X^*)^\vee)\cdot \frac{\mathrm{char}\left(D/\mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathcal{L}}}(F, X))\right)}{\mathrm{char}\left(Q/\mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F, X))\right)}\\ (5.4)\qquad &\Big|\ \mathrm{char}\left(H^1_{\mathcal{F}_{\mathcal{L}}}(F, T)/R\cdot c\right)\cdot \frac{\mathrm{char}\left(D/\mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathcal{L}}}(F, X))\right)}{\mathrm{char}\left(Q/\mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F, X))\right)}\\ &= \frac{\mathrm{char}\left(D/R\cdot \mathrm{loc}_{/V}(c)\right)}{\mathrm{char}\left(Q/\mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F, X))\right)}\ ,\end{aligned}$$

where the final equality is because $\mathrm{loc}_{/V}$ is injective. (5.2) shows further that

$$\begin{aligned}\mathrm{char}(H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,X^*)^\vee) \mid \frac{\mathrm{char}\left(\bigwedge^g Q/R\cdot \mathrm{loc}_{/V}(\varepsilon)\right)}{\mathrm{char}\left(Q/\mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F,X))\right)} &\\ = \frac{\mathrm{char}\left(\bigwedge^g Q/R\cdot \mathrm{loc}_{/V}(\varepsilon)\right)}{\mathrm{char}\left(\bigwedge^g Q/\bigwedge^g \mathrm{loc}_{/V}(H^1_{\mathcal{F}_{\mathrm{can}}}(F,X))\right)} &\\ = \mathrm{char}\left(\bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(F,X)/R\cdot\varepsilon\right). & \qquad (5.5)\end{aligned}$$

This concludes when $R=\mathfrak{O}$ so that $\#\,\mathrm{Cl}(L)^\chi = [\bigwedge^g \mathcal{O}_L^{\times,\chi} : \mathfrak{O}\cdot\varepsilon_F^\chi]$. Choosing the auxiliary set of primes $\mathcal{T}$ that appears in the definition of Rubin-Stark elements carefully (as in [Büy09a, §2.1]; see also the discussion preceding Theorem 3.11 in [Büy09a]), one may use the analytic class number formula (together with an inclusion-exclusion argument) for all fields between L and F to convert the inequality of Theorem 5.2(i) into an equality, concluding the proof of the first assertion in (i). See [Rub92, §5], [Rub96, Corollary 5.4] and [Pop04, §4.2] for details. Tracing back the inequalities above, we see that we in fact have an equality in the divisibility

$$\mathrm{Fitt}(H^1_{\mathcal{F}^*_{\mathcal{L}}}(F,T^*)^\vee) \mid \mathrm{Fitt}(H^1_{\mathcal{F}_{\mathcal{L}}}(F,T)/\mathfrak{O}\cdot c^\chi_{F,\Psi})$$

of (5.1), and it follows from Theorem 4.2(iii) that the Kolyvagin system $\boldsymbol{\kappa}^{\text{R-S}}(T)\in\overline{\mathbf{KS}}(T,\mathcal{F}_{\mathcal{L}},\mathcal{P})$ (which is the image of $\boldsymbol{\kappa}^{\text{R-S}}$) is primitive. The second assertion in (i) now follows from Theorem 4.1(ii).

Theorem 4.1(ii) shows that the image $\boldsymbol{\kappa}^{\text{R-S}}(\mathbb{T}_{\mathrm{cyc}})\in\overline{\mathbf{KS}}(\mathbb{T}_{\mathrm{cyc}},\mathcal{F}_{\mathcal{L}},\mathcal{P})$ of $\boldsymbol{\kappa}^{\text{R-S}}$ is primitive as well. Hence we have equality in the divisibility

$$\mathrm{char}\left(H^1_{\mathcal{F}^*_{\mathcal{L}}}(F,\mathbb{T}^*_{\mathrm{cyc}})^\vee\right) \mid \mathrm{char}\left(H^1_{\mathcal{F}_{\mathcal{L}}}(F,\mathbb{T}_{\mathrm{cyc}})/R\cdot c^\chi_{F_{\mathrm{cyc}},\Psi}\right)$$

of (5.1) and therefore also in (5.5) when $R=\Lambda_{\mathrm{cyc}}$. This is exactly the statement of (ii).

When $R=\Lambda$, the divisibility (5.5) reads

$$\mathrm{char}(\mathcal{A}^\chi_\infty) \mid \mathrm{char}\left(\bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T})/\Lambda\cdot\mathfrak{S}_\infty\right). \qquad (5.6)$$

Let $\pi_{\mathrm{cyc}}:\Lambda\twoheadrightarrow\Lambda_{\mathrm{cyc}}$ denote the obvious projection. We will check below in Lemma 5.4 that

$$\pi_{\mathrm{cyc}}(\mathrm{char}_\Lambda(\mathcal{A}^\chi_\infty)) = \mathrm{char}_{\Lambda_{\mathrm{cyc}}}(\mathcal{A}^\chi_{\mathrm{cyc}}) \neq 0$$

and in Lemma 5.5 that

$$\pi_{\mathrm{cyc}}(\mathrm{char}\left(\bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T})/\Lambda\cdot\mathfrak{S}_\infty\right)) = \mathrm{char}\left(\bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T}_{\mathrm{cyc}})/\Lambda\cdot\mathfrak{S}_{\mathrm{cyc}}\right).$$

All this shows (along with (5.6) and (ii)) that there are generators f (resp., g) of $\mathrm{char}_\Lambda(\mathcal{A}^\chi_\infty)$ (resp., of $\mathrm{char}\left(\bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T})/\Lambda\cdot\varepsilon^\chi_{F_\infty}\right)$) such that $f\notin\ker\pi_{\mathrm{cyc}}$, $f-g\in\ker\pi_{\mathrm{cyc}}$ and f divides g. We conclude using Lemma 5.3 that $g/f\in\Lambda^\times$, concluding the proof of (iii). □

Lemma 5.3. *Suppose $f,g\in\Lambda$ are such that $f\mid g$, $f-g\in\ker\pi_{\mathrm{cyc}}$ and $f\notin\ker\pi_{\mathrm{cyc}}$. Then $g/f\in\Lambda^\times$.*

Proof. Write $g = f \cdot h$ with $h \in \Lambda$, so that $f - g = f(1-h) \in \ker \pi_{\mathrm{cyc}}$. Since $f \notin \ker \pi_{\mathrm{cyc}}$, it follows that $1 - h \in \ker \pi_{\mathrm{cyc}} \subset \mathfrak{m}_\Lambda$, where $\mathfrak{m}_\Lambda$ is the maximal ideal. Hence h is indeed a unit. □

Lemma 5.4. $\pi_{\mathrm{cyc}}(\mathrm{char}_\Lambda(\mathcal{A}_\infty^\chi)) = \mathrm{char}_{\Lambda_{\mathrm{cyc}}}(\mathcal{A}_{\mathrm{cyc}}^\chi) \neq 0\,.$

Proof. Observe that $\ker \pi_{\mathrm{cyc}} = (\gamma_* - 1)\Lambda$ where $\gamma_* \in \Gamma$ is any lift of a topological generator of $\Gamma/\Gamma_{\mathrm{cyc}}$. By the control theorem,

$$\mathcal{A}_\infty^\chi/(\gamma^* - 1) = H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, \mathbb{T}^*)^\vee/(\gamma_* - 1) \cong H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, \mathbb{T}^*_{\mathrm{cyc}})^\vee = \mathcal{A}^\chi_{\mathrm{cyc}}\,.$$

As the Λ_{cyc}-module $\mathcal{A}^\chi_{\mathrm{cyc}}$ is torsion, it follows from Lemme 4 of [PR84, §1.1.3] that $\mathrm{char}_\Lambda(\mathcal{A}^\chi_\infty)$ is prime to $(\gamma_* - 1)$ and $\pi_{\mathrm{cyc}}\left(\mathrm{char}_\Lambda(\mathcal{A}^\chi_\infty)\right) = \mathrm{char}_{\Lambda_{\mathrm{cyc}}}(\mathcal{A}^\chi_{\mathrm{cyc}})$, as desired. □

Lemma 5.5.

$$\pi_{\mathrm{cyc}}(\mathrm{char}\left(\bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T})/\Lambda \cdot \mathfrak{S}_\infty\right)) = \mathrm{char}\left(\bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T}_{\mathrm{cyc}})/\Lambda \cdot \mathfrak{S}_{\mathrm{cyc}}\right).$$

Proof. It suffices to verify that the Λ_{cyc}-module

$$\mathrm{coker}(H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T}) \xrightarrow{\pi_{\mathrm{cyc}}} H^1_{\mathcal{F}_{\mathrm{can}}}(F, \mathbb{T}_{\mathrm{cyc}}))$$

is pseudo-null. It follows from Nekovář's control theorem (as used in Remark 2.16) that $\mathrm{coker}(\pi_{\mathrm{cyc}}) \cong \mathcal{A}^\chi_\infty[\gamma_* - 1]$. This module is pseudo-null by Lemme 4 of [PR84, §1.1.3]. □

5.1. **A two-variable CM main conjecture.** The goal in this section is to prove a somewhat less precise version of Theorem 5.2(iii) assuming only the Rubin-Stark Conjecture (but not the Strong Rubin-Stark Conjecture). Hypotheses from the previous section are in effect. Recall the map $\mathrm{loc}_{/V}$ defined as in the proof of Theorem 5.2.

Theorem 5.6. *We have*

$$\mathrm{char}\left(\mathcal{L}/\Lambda \cdot \mathrm{loc}_{/V}\left(c^\chi_{F_\infty,\Psi}\right)\right) \subseteq \mathrm{char}\left(H^1_{\mathcal{F}^*_{\mathfrak{tr}}}(F, \mathbb{T}^*)^\vee\right). \tag{5.7}$$

In particular, the module $H^1_{\mathcal{F}^*_{\mathfrak{tr}}}(F, \mathbb{T}^*)$ is Λ-cotorsion. Furthermore, the containment in (5.7) *may be promoted to an equality if the Strong Rubin-Stark Conjecture holds true.*

Proof. The first part may be deduced from Proposition 2.34 (used with $\mathcal{F} = \mathcal{F}_{\mathfrak{tr}}$ and $\mathcal{G} = \mathcal{F}_\mathcal{L}$) and Theorem 4.2(ii) (used with $\mathcal{F}_\mathcal{L}$). The second assertion follows from Proposition 4.9, the fact that $\mathrm{loc}_{/V}$ is injective (see the proof of Theorem 5.2) and the containment (5.7). Finally, the third portion follows from the proof of Theorem 5.2. □

Remark 5.7. Let $\mathcal{K}$ be any field contained in the collection $\mathfrak{C}$. The defining property of the Rubin-Stark elements and Example 3.2 show that $\mathrm{loc}_{/V}(\varepsilon^\chi_\mathcal{K}) \in \overline{\bigwedge^g Q_\mathcal{K}}$ where $Q_\mathcal{K} := H^1(\mathcal{K}_p, T)/\mathcal{V}^-_\mathcal{K}$ and the exterior product is taken in the category of $\mathfrak{O}[\mathrm{Gal}(\mathcal{K}/F)]$-modules. We will simply write $\mathrm{loc}_{/V}(\varepsilon^\chi_\mathcal{K})$ in place of $j^{-1}(\mathrm{loc}_{/V}(\varepsilon^\chi_\mathcal{K})) \in \bigwedge^g Q_\mathcal{K}$.

Definition 5.8. Recall the free-module $\mathcal{Q} = H^1(F_p, \mathbb{T})/\mathcal{V}$ of rank g. Define

$$\mathrm{loc}_{/V}(\varepsilon^{\chi}_{F_\infty}) = \{\mathrm{loc}_{/V}(\varepsilon^{\chi}_{M})\} \in \varprojlim \bigwedge^{g} Q_M = \bigwedge^{g} \varprojlim Q_M = \bigwedge^{g} \mathcal{Q}$$

to be the tower of Rubin-Stark elements along F_∞. Here the inverse limit is taken over all finite subextensions of F_∞/F, and the second equality holds thanks to the fact that each module Q_M is free as an $\mathfrak{O}[\mathrm{Gal}(M/F)]$-module and the transition maps $Q_M \to Q_{M'}$ $(F \subset M' \subset M \subset F_\infty)$ are all surjective (because all the maps $\mathcal{Q} \to Q_M$ are).

Theorem 5.9. *The ideal* $\mathrm{char}\left(H^1_{\mathcal{F}^*_{\mathfrak{tr}}}(F, \mathbb{T}^*)^\vee\right)$ *divides* $\mathrm{char}\left(\bigwedge^g \mathcal{Q}/\Lambda \cdot \mathrm{loc}_{/V}(\varepsilon^{\chi}_{F_\infty})\right)$, *with equality if we further assume the Strong Rubin-Stark Conjecture.*

Proof. Thanks to our choice of Ψ we have

$$\mathrm{char}\left(\mathcal{L}/\Lambda \cdot \mathrm{loc}_p\left(c^{\chi}_{F_\infty,\Psi}\right)\right) = \mathrm{char}\left(\bigwedge^{g} Q/\Lambda \cdot \mathrm{loc}_{/V}\left(\varepsilon^{\chi}_{F_\infty}\right)\right),$$

and the proof follows from Theorem 5.6. □

Remark 5.10. The Iwasawa module $H^1_{\mathcal{F}^*_{\mathfrak{tr}}}(F, \mathbb{T}^*)^\vee$ should be compared to the module $\hat{X}$ of [Rub91, §11] and Theorems 5.2 and 5.9 to Rubin's main conjecture [Rub91, Theorem 4.1(ii)], generalized to the setting where the base field F is now a general CM field.

6. The cyclotomic (supersingular) main conjecture for CM elliptic curves

The goal of this section is to apply results from Section 4 to study the cyclotomic Iwasawa theory of a CM elliptic curve at a supersingular prime.

Recall that $F^{\mathrm{cyc}} \subset F_\infty$ denotes the cyclotomic $\mathbb{Z}_p$-extension of F and F_n its nth layer. Further notation from Section 2.4.1 is also still in effect. In particular, recall the characters ρ, $\langle\rho\rangle$ and ω_E. Also until the end, the Dirichlet character χ is chosen to be ω_E.

Throughout Section 6 *we assume that* p *splits completely in* $F^+/\mathbb{Q}$. As before, let $T(E) = T_p(E)$ denote the p-adic Tate module of E. Let $S_p = \{\wp_1, \cdots, \wp_g\}$ denote the set of primes of F^+ lying above p. Note that each $\wp_i$ remains inert in the quadratic extension F/F^+. We denote the unique prime of F above $\wp_i$ by $\mathfrak{p}_i$. By a slight abuse, we denote the unique prime of F_n (and of F^{cyc}) above $\mathfrak{p}_i$ by the same symbol $\mathfrak{p}_i$.

6.1. **Preliminaries.**

In this subsection we recall some classical results (due mostly to Coates and Wiles) in the Iwasawa theory of CM elliptic curves. We shall initially record them being faithful to the original notions and notation, and later in Remark 6.5 we explain which objects we have introduced in the previous sections they correspond to.

Let $\mathfrak{M}$ be the maximal abelian pro-p extension of $\mathfrak{F} := F(E[p^\infty])$ unramified outside primes above p. Set $\mathfrak{X} := \mathrm{Gal}(\mathfrak{M}/\mathfrak{F})$ and $\Lambda_{\mathfrak{F}} := \mathfrak{O}[[\mathrm{Gal}(\mathfrak{F}/F)]]$. For any extension M of F (finite or infinite), consider the *relaxed* Selmer group

$$\mathrm{Sel}'_p(E/M) = \ker\left(H^1(M, E[p^\infty]) \longrightarrow \prod_{v \nmid p} \frac{H^1(M_v, E[p^\infty])}{E(M_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right).$$

Lemma 6.1 (Rubin). *For any infinite extension M_∞ of F contained in $\mathfrak{F}$,*

$$\mathrm{Sel}'_p(E/M_\infty) = \mathrm{Sel}_p(E/M_\infty).$$

Proof. This follows from [Rub85, Lemma 2.2]. □

Definition 6.2. Given a $\Lambda_{\mathfrak{F}}$-module Y and a continuous character $\psi : \mathrm{Gal}(\mathfrak{F}/F) \to \mathfrak{O}^\times$, we define $Y(\psi) := Y \otimes \mathfrak{O}_{\psi^{-1}}$ where $\mathfrak{O}_{\psi^{-1}}$ is the cyclic $\mathfrak{O}$-module on which $\mathrm{Gal}(\mathfrak{F}/F)$ acts via ψ^{-1}.

Definition 6.3. Given a $\Lambda_{\mathfrak{F}}$-module Y, we define $Y^\rho_\infty := Y(\rho^{-1}) \otimes_{\Lambda_{\mathfrak{F}}} \Lambda$ (resp., $Y^\rho_{\mathrm{cyc}} := Y(\rho^{-1}) \otimes_{\Lambda_{\mathfrak{F}}} \Lambda_{\mathrm{cyc}}$), the F_∞-coinvariants (resp., F^{cyc}-coinvariants) of $Y(\rho^{-1})$.

Lemma 6.4.

(i) $\mathrm{Sel}'_p(E/\mathfrak{F}) \cong \mathrm{Hom}_{\mathfrak{O}}(\mathfrak{X}, E[p^\infty])$.

(ii) $\mathrm{Sel}_p(E/F_\infty)^\vee \cong \mathfrak{X}^\rho_\infty$ *and* $\mathrm{Sel}_p(E/F^{\mathrm{cyc}})^\vee \cong \mathfrak{X}^\rho_{\mathrm{cyc}}$.

Proof. Proof of (i) is essentially due to Coates and Wiles and follows from the criterion of Néron-Ogg-Shafarevich utilized as in the proof of [CW77, Theorem 2]. Proposition 1.2 of [Rub85] shows (for $M_\infty = F^{\mathrm{cyc}}$ or F_∞) that

$$\mathrm{Sel}'_p(E/M_\infty) = \mathrm{Sel}'_p(E/\mathfrak{F})^{\mathrm{Gal}(\mathfrak{F}/M_\infty)}.$$

(In fact, the case $M_\infty = F_\infty$ is a straightforward consequence of the inflation restriction sequence, as $p \nmid [\mathfrak{F} : F_\infty]$.) It follows from Lemma 6.1 and (i) that

$$\begin{aligned}\mathrm{Sel}_p(E/M_\infty) &\cong \mathrm{Hom}_{\mathfrak{O}}\left(\mathfrak{X}, E[p^\infty]\right)^{\mathrm{Gal}(\mathfrak{F}/M_\infty)}\\ &\cong \mathrm{Hom}_{\mathfrak{O}}\left(\mathfrak{X}(\rho^{-1}), \Phi/\mathfrak{O}\right)^{\mathrm{Gal}(\mathfrak{F}/M_\infty)} \cong \mathrm{Hom}_{\mathfrak{O}}\left(\mathfrak{X}^\rho_?, \Phi/\mathfrak{O}\right)\end{aligned}$$

where ? = cyc or ∞ (depending on whether $M_\infty = F^{\mathrm{cyc}}$ or F_∞). □

For every prime $\mathfrak{p}_i$ of F above p, we denote the prime of $\mathfrak{F}$ above $\mathfrak{p}_i$ also by the symbol $\mathfrak{p}_i$. Let $\mathfrak{U}_i = \varprojlim \mathfrak{U}_M$ be the inverse limit (with respect to norm maps) of the local units (at $\mathfrak{p}_i$), where M varies over finite subextensions of $\mathfrak{F}_{\mathfrak{p}_i}/F_{\mathfrak{p}_i}$. The compositum of the maps

$$E(\mathfrak{F}_{\mathfrak{p}_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Hom}(G_{\mathfrak{F}_{\mathfrak{p}_i}}, E[p^\infty]) \to \mathrm{Hom}(\mathfrak{U}_i, E[p^\infty]) \xrightarrow{\sim} \mathrm{Hom}_{\mathfrak{O}}(\mathfrak{U}_i(\rho^{-1}), \Phi/\mathfrak{O})$$

(where the first map comes from the identification

$$H^1(\mathfrak{F}_{\mathfrak{p}_i}, E[p^\infty]) \xrightarrow{\sim} \mathrm{Hom}(G_{\mathfrak{F}_{\mathfrak{p}_i}}, E[p^\infty])$$

and the second map by the inclusion $\mathfrak{U}_i \hookrightarrow G_{\mathfrak{F}_{\mathfrak{p}_i}}$ of local class field theory) induces a non-degenerate (cf. [Rub87, Prop. 5.2]), $\mathfrak{O}$-linear *Kummer pairing*

$$\langle\, ,\, \rangle : \left(E(F^{\mathrm{cyc}}_{\mathfrak{p}_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right) \times \mathfrak{U}^\rho_{i,\mathrm{cyc}} \longrightarrow \Phi/\mathfrak{O}.$$

Remark 6.5. Let $\mathcal{F}_{\mathrm{str}}$ denote the *strict Selmer structure* on Z (where $Z = \mathbb{T}$ or $\mathbb{T}(E)$) given by the local conditions:

- $H^1_{\mathcal{F}_{\mathrm{str}}}(F_{\mathfrak{q}}, Z) = H^1_{\mathcal{F}_{\mathrm{can}}}(F_{\mathfrak{q}}, Z)$ for every prime $\mathfrak{q} \nmid p$,
- $H^1_{\mathcal{F}_{\mathrm{str}}}(F_p, Z) = 0$.

It follows easily using the inflation-restriction sequence that

$$H^1_{\mathcal{F}^*_{\mathrm{str}}}(F, \mathbb{T}^*)^\vee = \mathfrak{X}(\omega_E^{-1}) \otimes_{\Lambda_{\mathfrak{F}}} \Lambda =: \mathfrak{X}^{\omega_E}_\infty. \tag{6.1}$$

By Lemma 6.4, we conclude that

$$\text{(6.2)}\qquad \begin{aligned} 5\mathrm{Sel}_p(E/F_\infty)^\vee &= \mathfrak{X}_\infty^\rho = \mathfrak{X}(\rho^{-1}) \otimes_{\Lambda_{\mathfrak{F}}} \Lambda \\ &= H^1_{\mathcal{F}^*_{\mathrm{str}}}(F, \mathbb{T}^*)^\vee \otimes \langle \rho \rangle \cong H^1_{\mathcal{F}^*_{\mathrm{str}}}(F, \mathbb{T}(E)^*)^\vee, \end{aligned}$$

and on tensoring with Λ_{cyc} (and using once again the perfect control theorem)

$$\text{(6.3)}\qquad \begin{aligned} \mathrm{Sel}_p(E/F_{\mathrm{cyc}})^\vee &= \mathfrak{X}_{\mathrm{cyc}}^\rho = \mathfrak{X}_\infty^\rho \otimes_\Lambda \Lambda_{\mathrm{cyc}} \\ &\cong H^1_{\mathcal{F}^*_{\mathrm{str}}}(F, \mathbb{T}_{\mathrm{cyc}}(E)^*)^\vee. \end{aligned}$$

Furthermore, we have

$$\text{(6.4)}\qquad H^1(F_{\mathfrak{p}_i}, \mathbb{T}(E)) \underset{\mathrm{tw}}{\overset{\sim}{\longleftarrow}} H^1(F_{\mathfrak{p}_i}, \mathbb{T}) \otimes \langle \rho^{-1} \rangle = \mathfrak{U}^\rho_{i,\infty}\ ,$$

and on applying $\bigotimes_\Lambda \Lambda_{\mathrm{cyc}}$ to both sides,

$$H^1(F_{\mathfrak{p}_i}, \mathbb{T}_{\mathrm{cyc}}(E)) \overset{\sim}{\longleftarrow} \mathfrak{U}^\rho_{i,\mathrm{cyc}}\,.$$

Here tw : $H^1(F_{\mathfrak{p}_i}, \mathbb{T}) \to H^1(F_{\mathfrak{p}_i}, \mathbb{T}(E))$ is the twisting morphism which factors through the Λ-isomorphism (that we still denote by tw)

$$H^1(F_{\mathfrak{p}_i}, \mathbb{T}) \otimes \langle \rho^{-1} \rangle \overset{\sim}{\longrightarrow} H^1(F_{\mathfrak{p}_i}, \mathbb{T}(E))\,.$$

6.2. **Plus/minus Selmer groups and p-adic L-functions.** Following [Kob03] (see also [IP06]), we define the ±-subgroups as follows:

Definition 6.6. For every positive integer n, set

$$E^+(F_{n,\mathfrak{p}_i}) := \{x \in E(F_{n,\mathfrak{p}_i}) : \mathrm{Tr}_{n/m}(x) \in E(F_{m-1,\mathfrak{p}_i}) \text{ for } 0 < m \le n, m: \text{ odd}\},$$

$$E^-(F_{n,\mathfrak{p}_i}) := \{x \in E(F_{n,\mathfrak{p}_i}) : \mathrm{Tr}_{n/m}(x) \in E(F_{m-1,\mathfrak{p}_i}) \text{ for } 0 < m \le n, m: \text{ even}\},$$

where $\mathrm{Tr}_{n/m}(x) : E(F_{n,\mathfrak{p}_i}) \longrightarrow E(F_{m,\mathfrak{p}_i})$ is the trace map. We also set

$$E^\pm(F^{\mathrm{cyc}}_{\mathfrak{p}_i}) = \varinjlim E^\pm(F_{n,\mathfrak{p}_i}).$$

Definition 6.7. Let $\mathrm{Sel}_p(E/F_n)$ denote the classical Selmer group attached to E and set $\mathrm{Sel}_p(E/F^{\mathrm{cyc}}) = \varinjlim \mathrm{Sel}_p(E/F_n)$. Define the ±-Selmer groups by setting

$$\mathrm{Sel}_p^\pm(E/F_n) := \ker\left(\mathrm{Sel}_p(E/F_n) \longrightarrow \bigoplus_{i=1}^{g} \frac{H^1(F_{n,\mathfrak{p}_i}, E[p^\infty])}{\mathfrak{Kum}_i\,(E^\pm(F_{n,\mathfrak{p}_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)}\right).$$

Let $\mathrm{Sel}_p^\pm(E/F^{\mathrm{cyc}}) = \varinjlim \mathrm{Sel}_p^\pm(E/F_n)$.

We note that these two Selmer groups actually correspond to the cases $(+, \cdots, +)$ and $(-, \cdots, -)$-Selmer groups among 2^g possible options.

Definition 6.8. For a fixed topological generator γ of Γ_{cyc} and $n \ge 1$, we define the element $\nu_n = \sum_{i=0}^{p-1} \gamma^{ip^{n-1}} \in \Lambda_{\mathrm{cyc}}$ and set

$$\omega_n^+ = \prod_{\substack{1 \le i \le n \\ i:\ \text{even}}} \nu_i\ , \quad \omega_n^- = \prod_{\substack{1 \le i \le n \\ i:\ \text{odd}}} \nu_i\,.$$

At the analytic end of things, Park and Shahabi [PS11] have constructed a pair of signed (bounded) p-adic L-functions $L_p^\pm(E/F^+) \in \Lambda_{\mathrm{cyc}} \otimes \mathbb{Q}_p$ whose basic properties are outlined in the following theorem. For each prime $\mathfrak{P}$ of F^+ above p, we let $\alpha = \alpha(\mathfrak{P})$ denote a distinguished roof of the Hecke polynomial for E at $\mathfrak{P}$. As the prime $\mathfrak{P}$ is inert in F/F^+, it follows that $\alpha(\mathfrak{P})^2 = -p$, and our convention is that we always pick the same square root α of $-p$ (other choices would alter the bounded p-adic L-functions of Park and Shahabi by only ±1).

Theorem 6.9 (Park-Shahabi)**.** *There exists a pair of elements $L_p^+(E/F^+)$, $L_p^-(E/F^+) \in \Lambda_{\mathrm{cyc}} \otimes \mathbb{Q}_p$ which are characterized by the following interpolation properties: For every non-trivial character χ of Γ^{cyc} of finite order p^n,*

- *for odd n, we have*

$$\chi\left(L_p^+(E/F^+)\right) = (-1)^{\frac{n+1}{2}g} p^{\frac{n+1}{2}(g-1)} \frac{\tau(\chi)}{\chi(\omega_n^+)} \frac{L(E,\overline{\chi},1)}{\Omega_E(F^+)},$$

- *for even n, we have*

$$\chi\left(L_p^-(E/F^+)\right) = (-1)^{g\cdot(\frac{n}{2}+1)} p^{n/2(g-1)} \frac{\tau(\chi)}{\chi(\omega_n^-)} \frac{L(E,\overline{\chi},1)}{\Omega_E(F^+)}.$$

Furthermore, their value at the trivial character is given by

$$\mathbf{1}\left(L_p^+(E/F^+)\right) = u_1 \cdot \frac{L(E,1)}{\Omega_E(F^+)} \quad , \quad \mathbf{1}\left(L_p^-(E/F^+)\right) = u_2 \cdot \frac{L(E,1)}{\Omega_E(F^+)}$$

where $u_1, u_2 \in \overline{\mathbb{Q}}^\times$ (whose precise values we need not know).

Here, the period $\Omega_E(F^+)$ corresponds to the quantity $\Omega(\epsilon_0, f_E) D_{F^+}^{-1}(\sqrt{-1})^{-g}$ in [PS11], where f_E is the Hilbert modular form of parallel weight two that one associates (via the Weil-Jacquet-Langlands correspondence) to our CM elliptic curve E and D_{F^+} is the discriminant of F^+.

Proof. This is an immediate consequence of the interpolation formula [PS11, Theorem 2.3] and the factorization [PS11, Theorem 2.7], used together with [Pol03, Lemma 4.7]. □

The following is the signed-main conjecture that Park and Shahabi posed in this context.

Conjecture 6.10 (Park-Shahabi)**.**

(i) *Both modules* $\mathrm{Sel}_p^+(E/F^{\mathrm{cyc}})$ *and* $\mathrm{Sel}_p^-(E/F^{\mathrm{cyc}})$ *are Λ_{cyc}-cotorsion.*

(ii) *Any generator of the ideal* $\mathrm{char}\left(\mathrm{Sel}_p^\pm(E/F^{\mathrm{cyc}})^\vee\right)$ *also generates the ideal $L_p^\pm(E/F^+)(\Lambda_{\mathrm{cyc}} \otimes \mathbb{Q}_p)$.*

Definition 6.11. Let $V_i^\pm \subset \mathfrak{U}_{i,\mathrm{cyc}}^\rho$ denote the orthogonal complement of $E^\pm(F_{\mathfrak{p}_i}^{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ under the Kummer pairing defined as above. Via the identifications in Remark 6.5, we view $V_i^\pm$ as a submodule of $H^1(F_{\mathfrak{p}_i}, \mathbb{T}_{\mathrm{cyc}}(E))$.

Set $\mathfrak{U} = \bigoplus_{i=1}^g \mathfrak{U}_i$ and $\mathbb{V}_{E,\mathrm{cyc}}^\pm = \bigoplus_{i=1}^g V_i^\pm$. Define $\mathfrak{U}_\infty^\rho$ and $\mathfrak{U}_{\mathrm{cyc}}^\rho$ in a similar manner. Let $\alpha : \mathfrak{U} \to \mathfrak{X}$ be the Artin map of global class field theory (and likewise the compositum

$$\mathfrak{a} : \mathfrak{U}_{\mathrm{cyc}}^\rho \xrightarrow{\sim} H^1(F_p, \mathbb{T}(E)) \longrightarrow H^1_{\mathcal{F}_{\mathrm{str}}^*}(F, \mathbb{T}_{\mathrm{cyc}}(E)^*)^\vee$$

be the map obtained by the Poitou-Tate global duality). The following properties of the submodules $\mathbb{V}_{E,\mathrm{cyc}}^\pm$ may be obtained as in [PR04, Theorem 4.3 and Proposition 4.4] (and using the comparisons of Remark 6.5 wherever necessary).

Proposition 6.12 (Pollack-Rubin). *For every $1 \le i \le g$ we have:*

(i) *the Λ-module $\mathfrak{U}^{\rho}_{i,\infty} \cong H^1(F_{\mathfrak{p}_i}, \mathbb{T}(E))$ and the Λ_{cyc}-module $\mathfrak{U}^{\rho}_{i,\mathrm{cyc}} \cong H^1(F_{\mathfrak{p}_i}, \mathbb{T}_{\mathrm{cyc}}(E))$ are free of rank two,*

(ii) *the Λ_{cyc}-modules $V_i^{\pm}$ and $H^1(F_{\mathfrak{p}_i}, \mathbb{T}_{\mathrm{cyc}}(E))/V_i^{\pm}$ are both free of rank one,*

(iii) *there is a (non-canonical) submodule $\mathbf{V}_i^{\pm} \subset H^1(F_{\mathfrak{p}_i}, \mathbb{T}(E))$ whose image under the natural map*

$$\pi_{\mathrm{cyc}} : H^1(F_{\mathfrak{p}_i}, \mathbb{T}(E)) \longrightarrow H^1(F_{\mathfrak{p}_i}, \mathbb{T}_{\mathrm{cyc}}(E))$$

is the module $V_i^{\pm}$ and is such that both $\mathbf{V}_i^{\pm}$ and $H^1(F_{\mathfrak{p}_i}, \mathbb{T}(E))/\mathbf{V}_i^{\pm}$ are free of rank one over Λ,

(iv) $\mathrm{Sel}_p^{\pm}(E/F^{\mathrm{cyc}})^{\vee} = \mathfrak{X}^{\rho}_{\mathrm{cyc}}/\alpha(\mathbb{V}^{\pm}_{E,\mathrm{cyc}}) \cong H^1_{\mathcal{F}^*_{\mathrm{str}}}(F, \mathbb{T}_{\mathrm{cyc}}(E)^*)^{\vee}/\mathfrak{a}(\mathbb{V}^{\pm}_{E,\mathrm{cyc}})$.

6.3. **An explicit reciprocity conjecture for Rubin-Stark elements.** As we have assumed that the prime p splits completely in $F^+/\mathbb{Q}$, we may identify $F^+_{\wp_i}$ with $\mathbb{Q}_p$, and the constructions of Kobayashi [Kob03, §4] for a supersingular elliptic curve defined over $\mathbb{Q}_p$ carry over.

Definition 6.13. Given positive integers n and $1 \le i \le g$, let $E_1(F_{n,\mathfrak{p}_i}) \subset E(F_{n,\mathfrak{p}_i})$ denote the kernel of the reduction map modulo $\mathfrak{p}_i$. Then $E_1(F_{n,\mathfrak{p}_i})$ is the pro-p part of $E(F_{n,\mathfrak{p}_i})$, and we define the logarithm map λ_E to be the compositum

$$\lambda_E : E(F_{n,\mathfrak{p}_i}) \twoheadrightarrow E_1(F_{n,\mathfrak{p}_i}) \xrightarrow{\sim} \hat{E}(\mathfrak{p}_i) \longrightarrow F_{n,\mathfrak{p}_i},$$

where $\hat{E}$ is the formal group of $E/F_{\mathfrak{p}_i}$.

We consider Kobayashi's trace-compatible sequence of points $d_{n,i} \in E(F^+_{n,\wp_i})$; we refer the reader to [PR04, §3] for basic properties of these points and their comparison with Kobayshi's original construction. Using the complex multiplication map $E(F^+_{n,\wp_i}) \otimes \mathfrak{O} \to E(F_{n,\mathfrak{p}_i})$, we define the element $\mathfrak{d}_{n,i} \in E(F_{n,\mathfrak{p}_i})$ as the image of $d_{n,i}$. Key properties of the elements $\mathfrak{d}_{n,i}$ are outlined in the following proposition.

Proposition 6.14 (Kobayashi). *Let $\Gamma_n := \mathrm{Gal}(F_n/F)$. For every positive integer n and $1 \le i \le g$,*

(i) $\sum_{\sigma \in \Gamma_n} \chi(\sigma)\lambda_E(\mathfrak{d}^{\sigma}_{n,i}) = (-1)^{[n/2]}\tau(\chi)$, *where $\tau(\chi)$ is the Gauss sum,*

(ii) *if ϵ is the sign of $(-1)^n$, then $E^{\epsilon}(F_{n,\wp_i}) = \mathfrak{O}[\Gamma_n]\mathfrak{d}_{n,i}$ and $E^{-\epsilon}(F_{n,\wp_i}) = \mathfrak{O}[\Gamma_n]\mathfrak{d}_{n-1,i}$. Moreover, we have $E^{\epsilon}(F_{n,\wp_i}) + E^{-\epsilon}(F_{n,\wp_i}) = E(F_{n,\wp_i})$.*

Proof. This is a restatement of [PR04, Theorem 3.2]. □

Definition 6.15. Let $\mathcal{S}_{\infty} \subset \varprojlim_{M \subset F_{\infty}} \bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(M, T)$ denote the cyclic Λ-module generated by the tower of Rubin-Stark elements $\{\varepsilon^{\chi}_M\}$ and let $\mathcal{S}^{E,p}_{\infty}$ be the image of $\mathcal{S}_{\infty}$ under the compositum of maps

$$\varprojlim_{M \subset F_{\infty}} \bigwedge^g H^1_{\mathcal{F}_{\mathrm{can}}}(M, T) \to \varprojlim_{M \subset F_{\infty}} \bigwedge^g H^1(M_p, T) \xrightarrow{\sim} \bigwedge^g H^1(F_p, \mathbb{T})$$
$$\xrightarrow[\mathrm{tw}]{\sim} \bigwedge^g H^1(F_p, \mathbb{T}(E)).$$

We write $\mathrm{pr}_i : H^1(F_p, \mathbb{T}) \to H^1(F_{\mathfrak{p}_i}, \mathbb{T})$ for the obvious projection map (similarly, for the map defined on $H^1(M_p, T)$ for any M as above).

Conjecture 6.16.

(i) *There exists a generator* $\Xi_1 \wedge \cdots \wedge \Xi_g$ *of the cyclic* Λ*-module* $\mathcal{S}_\infty^{E,p}$ *such that for every* $n \in \mathbb{Z}^+$*, for every primitive character* $\chi : \mathrm{Gal}(F_n/F) \to \boldsymbol{\mu}_{p^\infty}$ *and for every positive integer* k*,*

$$\det\left(\sum_{\sigma\in\Gamma_n} \chi^{-1}(\sigma)\langle \mathfrak{d}_{n,i}^{\sigma} \otimes p^{-k}, \mathfrak{u}_{i,j}\rangle\right)$$
$$= p^{-kg}(-1)^{[n/2]g}\tau(\chi)\chi(\omega_n^{\epsilon})^{g-1}p^{\left[\frac{n+1}{2}\right](g-1)}\frac{L(E/F^+,\chi,1)}{\Omega_E(F^+)}$$

where $\mathfrak{u}_{i,j} := \mathrm{pr}_i(\Xi_j) \in H^1(F_{\mathfrak{p}_i}, \mathbb{T}(E)) \overset{\mathrm{tw}}{=} \mathfrak{U}_\infty^{\rho}$, $L(E/F^+,\chi,s)$ *is the* L*-series twisted by the character* χ *and* ϵ *is the sign of* $(-1)^n$*.*

(ii) *For all but finitely many characters* χ *of* Γ_{cyc}*, we have* $L(E/F^+,\chi,1) \neq 0$*.*

Remark 6.17. The first part of Conjecture 6.16 is a natural (but partial, in that it only concerns the plus/minus subgroups of the local cohomology groups) generalization of Coates and Wiles' reciprocity law [CW77, Wil78]. The second part proposes an extension of Rohrlich's [Roh84] non-vanishing theorem in the special case $F^+ = \mathbb{Q}$; see also [Roh89] for a result in this direction (which proves the weaker statement that (ii) holds true for infinitely many characters χ).

Recall the lift $\mathbf{V}_i^{\pm} \subset \mathfrak{U}_{i,\infty}^{\rho} \overset{\mathrm{tw}}{=} H^1(F_{\mathfrak{p}_i}, \mathbb{T}(E))$ of $V_i^{\pm}$ and set

$$\mathbb{V}_E^{\pm} := \bigoplus_{i=1}^{g} \mathbf{V}_i^{\pm} \subset H^1(F_p, \mathbb{T}(E)).$$

Let $\mathbb{V}^{\pm} \subset H^1(F_p, \mathbb{T})$ be the inverse image of $\mathbb{V}_E^{\pm}$ under the twisting isomorphism tw.

Recall the modules $\mathcal{M}$ and $\mathcal{M}_{\mathrm{cyc}}$ from Section 2.4.2.

Theorem 6.18. *If Conjecture* 6.16 *holds true, then* $\mathcal{M}_{\mathrm{cyc}} \cap \mathbb{V}_{E,\mathrm{cyc}}^{\pm} = 0 = \mathcal{M} \cap \mathbb{V}_E^{\pm}$.

Proof. Let Ξ denote the Λ-submodule of $H^1(F_p, \mathbb{T}(E))$ generated by $S = \{\Xi_1, \cdots, \Xi_g\}$ and Ξ_{cyc} its image inside $H^1(F_p, \mathbb{T}_{\mathrm{cyc}}(E))$ generated by $S_{\mathrm{cyc}} = \{\Xi_1^{\mathrm{cyc}}, \cdots, \Xi_g^{\mathrm{cyc}}\}$ where $\Xi_j^{\mathrm{cyc}} \in H^1(F_p, \mathbb{T}_{\mathrm{cyc}}(E))$ is the image of Ξ_j. First, notice that S is linearly independent over Λ and S_{cyc} is linearly independent over Λ_{cyc}. Indeed, if $a_1 \cdot \Xi_1^{\mathrm{cyc}} + \cdots + a_g \cdot \Xi_g^{\mathrm{cyc}} = 0$ for some $a_1, \cdots, a_g \in \Lambda_{\mathrm{cyc}}$, then this would imply that

$$\overline{a}_1 \cdot \mathrm{col}_1 + \cdots + \overline{a}_g \cdot \mathrm{col}_g = 0,$$

where col_j denotes the jth column of the matrix $\left[\sum_{\sigma\in\Gamma_n} \chi^{-1}(\sigma)\langle \mathfrak{d}_{n,i}^{\sigma} \otimes p^{-k}, \mathfrak{u}_{i,j}\rangle\right]_{i,j}$ and $\overline{a} \in \mathfrak{O}$ is the image of $a \in \Lambda_{\mathrm{cyc}}$ under the augmentation map. The explicit reciprocity conjecture (applied for large enough n) shows that $\overline{a}_i = 0$ for every i, so that $a_i = (\gamma_{\mathrm{cyc}} - 1)b_i$ for some $b_i \in \Lambda_{\mathrm{cyc}}$. As the Λ_{cyc}-module $H^1(F_p, \mathbb{T}_{\mathrm{cyc}}(E))$ is Λ_{cyc}-torsion free, we conclude that

$$b_1 \cdot \Xi_1^{\mathrm{cyc}} + \cdots + b_g \cdot \Xi_g^{\mathrm{cyc}} = 0$$

and in turn that each b_i is divisible by $\gamma_{\mathrm{cyc}} - 1$. Iterating this argument, we conclude that each a_i is divisible by arbitrarily large powers of $\gamma_{\mathrm{cyc}} - 1$, then $a_i = 0$ for every i. This completes the verification that S_{cyc} is Λ_{cyc}-linearly independent. The assertion that the set S is Λ-linearly independent is proved similarly. We therefore conclude that Ξ is a free Λ-module, Ξ_{cyc} is a free Λ_{cyc}-module and both have rank g.

We are now content to prove that $\Xi_{\mathrm{cyc}} \cap \mathbb{V}^{\pm}_{E,\mathrm{cyc}} = 0$. Suppose that $\sum_i a_i \cdot \Xi_i^{\mathrm{cyc}}$ belongs to $\mathbb{V}^{\epsilon}_{E,\mathrm{cyc}}$ (where $\epsilon = +$ or $-$) for some $a_1, \cdots, a_g \in \Lambda_{\mathrm{cyc}}$. Let n be a positive integer chosen so that the sign of $(-1)^n$ is ϵ and $L(E/F^+, \chi, 1) \neq 0$ for some primitive character χ of Γ_n. If $\mathrm{col}_1, \cdots, \mathrm{col}_g$ are the column vectors of $\left[\sum_{\sigma\in\Gamma_n} \chi^{-1}(\sigma)\langle \mathfrak{d}^{\sigma}_{n,i} \otimes p^{-k}, \mathfrak{u}_{i,j}\rangle\right]_{i,j}$ as above, we conclude once again that

$$\overline{a}_1 \cdot \mathrm{col}_1 + \cdots + \overline{a}_g \cdot \mathrm{col}_g = 0$$

and by the explicit reciprocity conjecture that each a_i is divisible by $\gamma_{\mathrm{cyc}} - 1$. Write $a_i = (\gamma_{\mathrm{cyc}} - 1)b_i$ so that we have

$$(\gamma_{\mathrm{cyc}} - 1) \cdot \sum_i b_i \cdot \Xi_i^{\mathrm{cyc}} \in \mathbb{V}^{\epsilon}_{E,\mathrm{cyc}}\,.$$

But according to Proposition 6.12(ii), the Λ_{cyc}-module $H^1(F_p, \mathbb{T}_{\mathrm{cyc}}(E))/\mathbb{V}^{\epsilon}_{E,\mathrm{cyc}}$ is torsion-free and therefore $\sum_i b_i \cdot \Xi_i^{\mathrm{cyc}} \in \mathbb{V}^{\epsilon}_{E,\mathrm{cyc}}$. Repeating the argument s times (for every positive integer s) we conclude that $(\gamma_{\mathrm{cyc}} - 1)^s$ divides each a_i, and therefore that $a_i = 0$, as desired.

It is not hard to see that there is an $r \in \Lambda$ with $\pi_{\mathrm{cyc}}(r) \neq 0$ and $r \cdot \Xi \subset \mathcal{M}$ (hence, we also have $\pi_{\mathrm{cyc}}(r) \cdot \Xi_{\mathrm{cyc}} \subset \mathcal{M}_{\mathrm{cyc}}$). The submodule $\pi_{\mathrm{cyc}}(r) \cdot \Xi_{\mathrm{cyc}}$ has Λ_{cyc}-rank g, and therefore the quotient $\mathcal{M}_{\mathrm{cyc}}/\pi_{\mathrm{cyc}}(r) \cdot \Xi_{\mathrm{cyc}}$ is torsion. This in turn shows that there is a non-zero element $\tilde{r} \in \Lambda_{\mathrm{cyc}}$ with $\tilde{r}\mathcal{M}_{\mathrm{cyc}} \subset \Xi_{\mathrm{cyc}}$. Using this observation, the fact that $H^1(F_p, \mathbb{T}_{\mathrm{cyc}}(E)$ is Λ_{cyc}-torsion free and our conclusion from the previous paragraph that $\Xi_{\mathrm{cyc}} \cap \mathbb{V}^{\pm}_{E,\mathrm{cyc}} = 0$, it follows that $\mathcal{M}_{\mathrm{cyc}} \cap \mathbb{V}^{\pm}_{E,\mathrm{cyc}} = 0$.

It now follows at once from Nakayama's lemma that $\mathcal{M} \cap \mathbb{V}^{\pm}_{E} = 0$ as well. □

Remark 6.19. Theorem 6.18 supplies us with two *natural* choices for the free Λ-module $\mathbb{V}_E$ in Definition 2.27: $\mathbb{V}^{+}_{E}$ or $\mathbb{V}^{-}_{E}$.

6.4. **Rubin-Stark elements and the plus/minus main conjecture.** Throughout this subsection, we assume the truth of the Explicit Reciprocity Conjecture 6.16 (therefore, implicitly the truth of Rubin-Stark conjectures) and of Leopoldt's conjecture for the number field L. Throughout, let ϵ stand for one of $+$ or $-$.

Definition 6.20.

(i) Let $\mathfrak{Q}_{\epsilon,\infty} := H^1(F_p, \mathbb{T}(E))/\mathbb{V}^{\epsilon}_{E}$ and let $\mathrm{loc}^{\epsilon}_{p}$ denote the compositum

$$\mathrm{loc}^{\epsilon}_{p} : H^1(F, \mathbb{T}(E)) \xrightarrow{\mathrm{loc}_p} H^1(F_p, \mathbb{T}(E)) \longrightarrow \mathfrak{D}_{\epsilon,\infty}.$$

(The quotient $\mathfrak{Q}_{\epsilon,\infty}$ is related (via the twisting map tw) to the quotients Q defined as in Section 5 and the map $\mathrm{loc}^{\epsilon}_{p}$ to $\mathrm{loc}_{/V}$.) Observe that $\mathfrak{Q}_{\epsilon,\infty}$ is a free Λ-module of rank g by Proposition 6.12(iii) and the map $\mathrm{loc}^{\epsilon}_{p}$ is injective by Theorem 6.18.

(ii) Let $\mathfrak{u}_{\text{R-S}} = \mathfrak{u}_1 \wedge \cdots \wedge \mathfrak{u}_g \in \bigwedge^g \mathfrak{Q}_{\epsilon,\infty}$ denote the image of the tower of Rubin-Stark elements $\mathrm{loc}^{\epsilon}_{p}(\varepsilon^{\omega_E}_{F_\infty}) \in \bigwedge^g \mathcal{Q}$ (given as in Definition 5.8, with the choice $\mathcal{V} = \mathrm{tw}^{-1}(\mathbb{V}^{\epsilon}_{E})$) under the twisting map $\bigwedge^g \mathcal{Q} \to \bigwedge^g \mathfrak{Q}_{\epsilon,\infty}$.

(iv) Similarly define $\mathfrak{Q}_{\epsilon,\mathrm{cyc}}$ and the map

$$\mathrm{loc}^{\epsilon}_{p} : H^1(F, \mathbb{T}_{\mathrm{cyc}}(E)) \longrightarrow \mathfrak{Q}_{\epsilon,\mathrm{cyc}}\,.$$

Let $\bar{\mathfrak{u}}_{\text{R-S}} = \bar{\mathfrak{u}}_1 \wedge \cdots \wedge \bar{\mathfrak{u}}_g \in \bigwedge^g \mathfrak{Q}_{\epsilon,\mathrm{cyc}}$ be the image of $\mathfrak{u}_{\text{R-S}}$ under the projection map $\bigwedge^g \mathfrak{Q}_{\epsilon,\infty} \to \bigwedge^g \mathfrak{Q}_{\epsilon,\mathrm{cyc}}\,.$

Theorem 6.21. *Any generator of the ideal* $\mathrm{char}\left(\bigwedge^g \mathfrak{Q}_{\epsilon,\mathrm{cyc}}/\Lambda_{\mathrm{cyc}}\cdot\bar{\mathfrak{u}}_{\text{R-S}}\right)$ *generates the cyclic* $(\Lambda_{\mathrm{cyc}}\otimes\mathbb{Q}_p)$*-module* $(\Lambda_{\mathrm{cyc}}\otimes\mathbb{Q}_p)\cdot L_p^{\epsilon}(E/F^+)$.

The proof we shall present below for this theorem is essentially identical to the proof of [PR04, Theorem 7.2] after a number of obvious modifications.

Proof. Let $\mu_i^{\pm}\in\mathrm{Hom}(E^{\pm}(F_{\mathfrak{p}_i}^{\mathrm{cyc}})\otimes\mathbb{Q}_p/\mathbb{Z}_p,\mathbb{Q}_p/\mathbb{Z}_p)$ be the generator which was essentially constructed by Kobayashi [Kob03, Theorem 6.2], whose properties are outlined in [PR04, Theorem 7.1]. Let $\Xi=\xi_1\wedge\cdots\wedge\xi_g\in\bigwedge^g\in\mathfrak{S}_{\infty}^{\rho}$ be as in the statement of Conjecture 6.16, and let $\varphi_{i,j}^{\pm}$ denote the image of ξ_j inside $\mathrm{Hom}(E^{\pm}(F_{\mathfrak{p}_i}^{\mathrm{cyc}})\otimes\mathbb{Q}_p/\mathbb{Z}_p,\mathbb{Q}_p/\mathbb{Z}_p)$. Then

$$\varphi_{i,j}^{\pm}=h_{i,j}^{\pm}\,\mu_i^{\pm}\tag{6.5}$$

for some $h_{i,j}^{\pm}\in\Lambda_{\mathrm{cyc}}$ and

$$\begin{gathered}\bigwedge^g\mathfrak{Q}_{\mathrm{cyc}}^{\pm,\rho}/\Lambda_{\mathrm{cyc}}\cdot\bar{\mathfrak{u}}_{\text{R-S}}\xrightarrow{\sim}\Lambda_{\mathrm{cyc}}/\det\left(h_{i,j}^{\pm}\right),\\ \mathrm{char}\left(\bigwedge^g\mathfrak{Q}_{\mathrm{cyc}}^{\pm,\rho}/\Lambda_{\mathrm{cyc}}\cdot\bar{\mathfrak{u}}_{\text{R-S}}\right)=\det\left(h_{i,j}^{\pm}\right)\Lambda_{\mathrm{cyc}}.\end{gathered}\tag{6.6}$$

Let $\chi:\Gamma_{\mathrm{cyc}}\to\boldsymbol{\mu}_{p^n}$ be any character of order $p^n>1$. It follows from (6.5) that for every $k\geq 1$ and $1\leq i\leq g$,

$$L_{i,j}^{\pm}:=\sum_{\sigma\in\Gamma_n}\chi(\sigma)\varphi_{i,j}^{\pm}(\mathfrak{d}_{n,i}^{\sigma}\otimes p^{-k})=\chi(h_{i,j}^{\pm})\sum_{\sigma\in\Gamma_n}\chi(\sigma)\mu_i^{\pm}(\mathfrak{d}_{n,i}^{\sigma}\otimes p^{-k})=:R_{i,j}^{\pm}.\tag{6.7}$$

A computation of Kobayashi (cf. [PR04, Theorem 7.1]) shows that $R_{i,j}^{\pm}=\chi(h_{i,j}^{\pm})\chi(\omega_n^{\pm})p^{-k}$ so that we have

$$\det\left(R_{i,j}^{\pm}\right)=p^{-kg}\chi\left(\det\left(h_{i,j}^{\pm}\right)\right)\chi(\omega_n^{\pm})^g.\tag{6.8}$$

On the other hand, Conjecture 6.16 (which we assume) together with Proposition 6.14 shows that

$$\det\left(L_{i,j}^{\epsilon}\right)=p^{-kg}(-1)^{[n/2]g}\tau(\chi)\chi(\omega_n^{\epsilon})^{g-1}p^{\left[\frac{n+1}{2}\right](g-1)}\frac{L(E/F^+,\chi,1)}{\Omega_E(F^+)},\tag{6.9}$$

where ϵ is the sign of $(-1)^{n+1}$. It follows from (6.7), (6.8) and (6.9) that

$$\begin{aligned}(-1)^{[n/2]g}\tau(\chi)\chi(\omega_n^{\epsilon})^{g-1}p^{\left[\frac{n+1}{2}\right](g-1)}&\frac{L(E/F^+,\chi,1)}{\Omega_E(F^+)}\\ &\equiv\chi\left(\det\left(h_{i,j}^{\epsilon}\right)\right)\chi(\omega_n^{\epsilon})^g\mod p^{kg}\end{aligned}$$

for every k. The proof follows from Theorem 6.9. □

Theorem 6.22. *The* Λ_{cyc}*-module* $H^1_{\mathcal{F}_{\mathrm{can}}}(F,\mathbb{T}_{\mathrm{cyc}}(E)^*)^{\vee}$ *is torsion.*

This statement is a reformulation of the weak Leopoldt conjecture for our CM elliptic curve E and the cyclotomic $\mathbb{Z}_p$-extension F_{cyc} of F.

Proof. By Corollary 4.3, it suffices to prove the existence of a Kolyvagin system $\boldsymbol{\kappa}\in\overline{\mathbf{KS}}(\mathbb{T}_{\mathrm{cyc}}(E),\mathcal{F}_{\mathbb{L}},\mathcal{P})$ with non-vanishing initial term $\kappa_1\in H^1_{\mathcal{F}_{\mathbb{L}}}(F,\mathbb{T}_{\mathrm{cyc}}(E))$. A suitable modification in Theorem 4.8 (so as to allow the replacement of $\mathbb{T}$ with

$\mathbb{T}(E)$ and $\mathcal{L}$ with $\mathbb{L}_E$, etc.) shows that there is an isomorphism $\Psi : \bigwedge^g \mathfrak{Q}_{\epsilon,\infty} \to \mathbb{L}_E$ and a Kolyvagin system $\boldsymbol{\kappa}(\text{R-S}) \in \overline{\mathbf{KS}}(\mathbb{T}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P})$ with the following properties:

- The initial term $\kappa_1(\text{R-S}) \in H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T}(E))$ of $\boldsymbol{\kappa}(\text{R-S})$ verifies that

$$\mathrm{loc}_p^{\epsilon}(\kappa_1(\text{R-S})) = \Psi(\mathfrak{u}_{\text{R-S}})\,. \tag{6.10}$$

- Let $\boldsymbol{\kappa}^{\text{cyc}}(\text{R-S}) \in \overline{\mathbf{KS}}(\mathbb{T}_{\text{cyc}}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P})$ be the image of $\boldsymbol{\kappa}(\text{R-S})$ and let $\kappa_1^{\text{cyc}}(\text{R-S}) \in H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T}_{\text{cyc}}(E))$ be its initial term. Then

$$\mathrm{loc}_p^{\epsilon}(\kappa_1^{\text{cyc}}(\text{R-S})) = \Psi_{\text{cyc}}(\bar{\mathfrak{u}}_{\text{R-S}})\,, \tag{6.11}$$

  where $\Psi_{\text{cyc}} : \bigwedge^g \mathfrak{Q}_{\epsilon,\text{cyc}} \to \mathbb{L}_E^{\text{cyc}}$ is the isomorphism induced from Ψ by base change.

The proof now follows from (6.11), Theorem 6.21 and the second part of the Explicit Reciprocity Conjecture 6.16 (from which follows that $L_p^{\epsilon}(E/F^+) \in \Lambda_{\text{cyc}} \otimes \mathbb{Q}_p$ is nonzero). □

Definition 6.23. Let $\mathcal{F}_\epsilon$ denote the Selmer structure on $\mathbb{T}$ (and on its subquotients, given by propagation as usual) defined by the local conditions

- $H^1_{\mathcal{F}_\epsilon}(F_\mathfrak{q}, \mathbb{T}(E)) = H^1_{\mathcal{F}_{\text{can}}}(F_\mathfrak{q}, \mathbb{T}(E))$ for every prime $\mathfrak{q} \nmid p$,
- $H^1_{\mathcal{F}_\epsilon}(F_p, \mathbb{T}(E)) = \mathbb{V}_E^{\epsilon}$.

Set $\mathcal{Y}_{\epsilon,\infty} = H^1_{\mathcal{F}_\epsilon^*}(F, \mathbb{T}(E)^*)^\vee$ and $\mathcal{Y}_{\epsilon,\text{cyc}} = H^1_{\mathcal{F}_\epsilon^*}(F, \mathbb{T}_{\text{cyc}}(E)^*)^\vee$.

Remark 6.24. Thanks to Theorem 6.18, the Selmer structure $\mathcal{F}_\epsilon$ agrees with the Kobayashi Selmer structure $\mathcal{F}_{\text{Kob}}$ with the choice $\mathbb{V}_E = \mathbb{V}_E^{\epsilon}$ in Definition 2.30.

Lemma 6.25. $\mathcal{Y}_{\epsilon,\text{cyc}} \cong \mathrm{Sel}^{\epsilon}(E/F^{\text{cyc}})^\vee$.

Proof. The Poitou-Tate global duality sequence

$$\begin{aligned} 0 \longrightarrow H^1_{\mathcal{F}_{\text{str}}}(F, \mathbb{T}(E)) \longrightarrow H^1_{\mathcal{F}_\epsilon}(F, \mathbb{T}(E)) &\xrightarrow{\mathrm{loc}_p} \mathbb{V}_E^{\epsilon} \\ \xrightarrow{\mathfrak{a}} H^1_{\mathcal{F}^*_{\text{str}}}(F, \mathbb{T}(E)^*)^\vee &\longrightarrow \mathcal{Y}_{\epsilon,\infty} \longrightarrow 0 \end{aligned}$$

reduces to the sequence

$$0 \longrightarrow \mathbb{V}_E^{\epsilon} \longrightarrow H^1_{\mathcal{F}^*_{\text{str}}}(F, \mathbb{T}(E)^*)^\vee \longrightarrow \mathcal{Y}_{\epsilon,\infty} \longrightarrow 0$$

thanks to Proposition 2.33 and Theorem 6.22. Applying the functor $- \otimes_\Lambda \Lambda_{\text{cyc}}$ and using the control theorem [MR04, Lemma 3.5.3], we obtain the exact sequence

$$0 \longrightarrow \mathbb{V}_{E,\text{cyc}}^{\epsilon} \xrightarrow{\mathfrak{a}} H^1_{\mathcal{F}^*_{\text{str}}}(F, \mathbb{T}_{\text{cyc}}(E)^*)^\vee \longrightarrow \mathcal{Y}_{\epsilon,\text{cyc}} \longrightarrow 0 \tag{6.12}$$

(where the exactness on the left follows from rank considerations and the fact that $\mathbb{V}_{E,\text{cyc}}^{\epsilon}$ is free of rank g). This shows, using Proposition 6.12(iv), that

$$\mathcal{Y}_{\epsilon,\text{cyc}} \cong H^1_{\mathcal{F}^*_{\text{str}}}(F, \mathbb{T}_{\text{cyc}}(E)^*)^\vee / \mathfrak{a}(\mathbb{V}_{E,\text{cyc}}^{\epsilon}) \cong \mathrm{Sel}^{\pm}(E/F^{\text{cyc}})^\vee.$$

□

Fix a generator $L_p^{\pm,\text{alg}} \in \Lambda_{\text{cyc}}$ of the ideal $\mathrm{char}\big(\mathrm{Sel}^{\pm}(E/F^{\text{cyc}})^\vee\big)$. We have the following result towards Conjecture 6.10.

Theorem 6.26. *We have $L_p^{\pm,\text{alg}} \mid L_p^{\pm}(E/F^+)$ (inside the ring $\Lambda_{\text{cyc}} \otimes \mathbb{Q}_p$). This divisibility is in fact an equality if we assume the Strong Rubin-Stark Conjecture for $\mathfrak{E}$.*

Proof. The proof of Theorem 5.9 applied with the Kolyvagin system

$$\boldsymbol{\kappa}^{\mathrm{cyc}}(\text{R-S}) \in \overline{\mathbf{KS}}(\mathbb{T}_{\mathrm{cyc}}(E), \mathcal{F}_{\mathbb{L}}, \mathcal{P})$$

in place of the Rubin-Stark $\mathcal{L}$-restricted Kolyvagin system for $\mathbb{T}$ and the Selmer structure $\mathcal{F}_\epsilon$ in place of $\mathcal{F}_{\mathfrak{tr}}$ shows that

$$\mathrm{char}\left(H^1_{\mathcal{F}^*_\epsilon}(F, \mathbb{T}(E)^*)^\vee\right) \mid \mathrm{char}\left(\bigwedge^g \mathfrak{O}_{\epsilon,\mathrm{cyc}}/\Lambda_{\mathrm{cyc}} \cdot \bar{\mathfrak{u}}_{\text{R-S}}\right).$$

The first part of the theorem now follows from Theorem 6.21 and Lemma 6.25.

If the Strong Rubin-Stark Conjecture holds true, Theorem 5.9 (after twisting) shows that

$$\mathrm{char}\left(H^1_{\mathcal{F}^*_\epsilon}(F, \mathbb{T}(E)^*)^\vee\right) = \mathrm{char}\left(\bigwedge^g \mathfrak{O}_{\epsilon,\infty}/\Lambda \cdot \mathfrak{u}_{\text{R-S}}\right).$$

This, however, means using Proposition 2.34 and Theorem 6.21 that

$$\mathrm{char}\left(H^1_{\mathcal{F}^*_{\mathbb{L}^*}}(F, \mathbb{T}(E)^*)^\vee\right) = \mathrm{char}\left(H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T}(E))/\Lambda \cdot \kappa_1(\text{R-S})\right)$$

and by Proposition 4.4 that the Kolyvagin system $\boldsymbol{\kappa}(\text{R-S})$ and its image $\boldsymbol{\kappa}^{\mathrm{cyc}}(\text{R-S})$ are both primitive. This shows that

$$\mathrm{char}\left(H^1_{\mathcal{F}^*_{\mathbb{L}^*}}(F, \mathbb{T}_{\mathrm{cyc}}(E)^*)^\vee\right) = \mathrm{char}\left(H^1_{\mathcal{F}_{\mathbb{L}}}(F, \mathbb{T}_{\mathrm{cyc}}(E))/\Lambda_{\mathrm{cyc}} \cdot \kappa_1^{\mathrm{cyc}}(\text{R-S})\right),$$

and once again applying Proposition 2.34, we conclude that

$$\mathrm{char}\left(H^1_{\mathcal{F}^*_\epsilon}(F, \mathbb{T}_{\mathrm{cyc}}(E)^*)^\vee\right) = \mathrm{char}\left(\bigwedge^g \mathfrak{O}_{\epsilon,\mathrm{cyc}}/\Lambda_{\mathrm{cyc}} \cdot \bar{\mathfrak{u}}_{\text{R-S}}\right).$$

The second assertion follows as well. □

Assuming the validity of the Strong Rubin-Stark Conjecture for $\mathfrak{E}$, we may therefore write

$$L_p^{\pm,\mathrm{alg}} = u\,\pi^{\varepsilon} L_p^{\pm}(E/F^+)$$

where $\pi \in \mathfrak{O}$ is a uniformizer, $\varepsilon \in \mathbb{Z}$ and $u \in \Lambda_{\mathrm{cyc}}$ is a unit.

6.5. **Applications of the supersingular main conjecture.**

The assumptions of the previous subsection are in effect until the end. We have the following consequence of Theorem 6.26 to the Birch and Swinnerton-Dyer conjecture for E/F^+, generalizing parts of [Rub91, Theorem 11.4] (which applies in the case $F^+ = \mathbb{Q}$).

Theorem 6.27.

(1) *If $L(E/F^+, 1) \neq 0$, then $E(F^+)$ is finite.*

(2) *Assuming the validity of the Strong Rubin-Stark Conjecture and that $L(E/F^+, 1) = 0$, the classical Selmer group $\mathrm{Sel}_p(E/F^+)$ is infinite.*

Remark 6.28. Assuming the Strong Rubin-Stark Conjecture and in case $L(E/F^+, 1) \neq 0$, one may in fact express the cardinality of $\mathrm{III}(E/F)[p^\infty]$ in terms of ε, u_1 and the L-value. Since this lacks the desired level of precision, we do not include this statement as part of Theorem 6.27.

Proof. The proof of this theorem is essentially identical to the proof of [PR04, Theorem 8.2]. Besides Theorem 6.26, the key points are as follows:

(a) The perfect control theorem for the Selmer group $H^1_{\mathcal{F}^*_{\rm str}}(F, T_p(E) \otimes \Lambda_{\rm cyc})^\vee$, which asserts that

$$H^1_{\mathcal{F}^*_{\rm str}}(F, T_p(E) \otimes \Lambda_{\rm cyc})^\vee \otimes_{\Lambda_{\rm cyc}} \mathfrak{O} \xrightarrow{\sim} H^1_{\mathcal{F}^*_{\rm str}}(F, T_p(E))^\vee$$

holds true thanks to [MR04, Lemma 3.5.3] (or [Nek06, Proposition 8.10.1]).

(b) For every n and $1 \leq i \leq g$, the maps

$$E(F_{\wp_i}) \otimes \Phi/\mathfrak{O} \longrightarrow H^0(\Gamma_{\rm cyc}, E^\pm(F_{n,\mathfrak{p}_i}) \otimes \Phi/\mathfrak{O})$$

are surjective. This assertion is proved as part of [PR04, Lemma 8.3].

(c) Using (a) and (b) above, one may deduce Kobayashi's control theorem:

$$\mathrm{Sel}_p^\pm(E/F^{\rm cyc})^\vee \otimes_{\Lambda_{\rm cyc}} \mathfrak{O} \xrightarrow{\sim} \mathrm{Sel}_p(E/F)^\vee.$$

(d) The exact sequence (6.12), [PR04, Lemma 6.5] and the proof of [Rub91, Theorem 11.16] (applied with [NQĐ84, Theorem 3.1]) show that $\mathrm{Sel}_p^\pm(E/F^{\rm cyc})^\vee$ has no finite-submodules. This together with (c) implies

$$|\left(\mathrm{Sel}_p^\pm(E/F^{\rm cyc})^\vee\right) \otimes_{\Lambda_{\rm cyc}} \mathfrak{O}| = |\mathrm{Sel}_p(E/F)^\vee|\,.$$

The proof now follows from the interpolation property of the signed p-adic L-function $L_p^\pm(E/F^+)$ (considered as the identity character on $\Gamma_{\rm cyc}$) together with the isomorphism $\mathrm{Sel}_p(E/F^+)^\vee \otimes_{\mathbb{Z}_p} \mathfrak{O} \xrightarrow{\sim} \mathrm{Sel}_p(E/F)^\vee$ induced by the theory of complex multiplication. □

Remark 6.29. The analogous statements to Theorem 6.27 may be proved in the ordinary case using the ordinary CM main conjectures; cf. [Hsi12, Büy14].

Acknowledgments

The author would like to thank Ming-Lun Hsieh and Antonio Lei for stimulating conversations and Robert Pollack for his encouragement on this project. He also thanks the referee for constructive suggestions and for proposed corrections to improve the paper. The author is particularly grateful to the referee for pointing out an inaccuracy in Section 6.2, concerning the use of the Park-Shahabi p-adic L-function.

References

[BL15] Kâzım Büyükboduk and Antonio Lei, *Coleman-adapted Rubin-Stark Kolyvagin systems and supersingular Iwasawa theory of CM abelian varieties*, Proc. Lond. Math. Soc. (3) **111** (2015), no. 6, 1338–1378, DOI 10.1112/plms/pdv054. MR3447796

[BL17] Kâzım Büyükboduk and Antonio Lei, *Integral Iwasawa theory of galois representations for non-ordinary primes*, Math. Z. **286** (2017), no. 1-2, 361–398, DOI 10.1007/s00209-016-1765-z. MR3648502

[Büy09a] Kâzim Büyükboduk, *Kolyvagin systems of Stark units*, J. Reine Angew. Math. **631** (2009), 85–107, DOI 10.1515/CRELLE.2009.042. MR2542218

[Büy09b] Kâzım Büyükboduk, *Stark units and the main conjectures for totally real fields*, Compos. Math. **145** (2009), no. 5, 1163–1195, DOI 10.1112/S0010437X09004163. MR2551993

[Büy10] Kâzim Büyükboduk, *On Euler systems of rank r and their Kolyvagin systems*, Indiana Univ. Math. J. **59** (2010), no. 4, 1277–1332, DOI 10.1512/iumj.2010.59.4237. MR2815034

[Büy11] Kâzım Büyükboduk, Λ*-adic Kolyvagin systems*, Int. Math. Res. Not. IMRN **14** (2011), 3141–3206, DOI 10.1093/imrn/rnq186. MR2817676

[Büy14] Kâzım Büyükboduk, *Main conjectures for CM fields and a Yager-type theorem for Rubin-Stark elements*, Int. Math. Res. Not. IMRN **21** (2014), 5832–5873. MR3273065

[Büy16] Barry Mazur, *A celebration of the mathematical work of Glenn Stevens*, Ann. Math. Qué. **40** (2016), no. 1, 1–16, DOI 10.1007/s40316-015-0053-3. MR3512520

[CW77] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), no. 3, 223–251, DOI 10.1007/BF01402975. MR0463176

[Hsi12] Ming-Lun Hsieh, *Iwasawa main conjecture for CM fields*, preprint, 2012.

[HT93] H. Hida and J. Tilouine, *Anti-cyclotomic Katz p-adic L-functions and congruence modules*, Ann. Sci. École Norm. Sup. (4) **26** (1993), no. 2, 189–259. MR1209708

[HT94] H. Hida and J. Tilouine, *On the anticyclotomic main conjecture for CM fields*, Invent. Math. **117** (1994), no. 1, 89–147, DOI 10.1007/BF01232236. MR1269427

[IP06] Adrian Iovita and Robert Pollack, *Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields*, J. Reine Angew. Math. **598** (2006), 71–103, DOI 10.1515/CRELLE.2006.069. MR2270567

[Kat78] Nicholas M. Katz, *p-adic L-functions for CM fields*, Invent. Math. **49** (1978), no. 3, 199–297, DOI 10.1007/BF01390187. MR513095

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et applications arithmétiques. III. Astérisque **295** (2004), ix, 117–290. MR2104361

[Kob03] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36, DOI 10.1007/s00222-002-0265-4. MR1965358

[Mai08] Fabio Mainardi, *On the main conjecture for CM fields*, Amer. J. Math. **130** (2008), no. 2, 499–538, DOI 10.1353/ajm.2008.0019. MR2405166

[MR04] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96, DOI 10.1090/memo/0799. MR2031496

[Nek06] Jan Nekovář, *Selmer complexes*, Astérisque **310** (2006), viii+559. MR2333680

[NQĐ84] Nguyễn-Quang-Đỗ, *Formations de classes et modules d'Iwasawa*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 167–185, DOI 10.1007/BFb0099451. MR756093

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR2392026

[Och05] Tadashi Ochiai, *Euler system for Galois deformations*, Ann. Inst. Fourier (Grenoble) **55** (2005), no. 1, 113–146. MR2141691

[Pol03] Robert Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558, DOI 10.1215/S0012-7094-03-11835-9. MR1983040

[Pop04] Cristian D. Popescu, *Rubin's integral refinement of the abelian Stark conjecture*, Stark's conjectures: recent work and new directions, Contemp. Math., vol. 358, Amer. Math. Soc., Providence, RI, 2004, pp. 1–35, DOI 10.1090/conm/358/06534. MR2088710

[PR84] Bernadette Perrin-Riou, *Arithmétique des courbes elliptiques et théorie d'Iwasawa*, Mém. Soc. Math. France (N.S.) **17** (1984), 130. MR799673

[PR93] Bernadette Perrin-Riou, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 4, 945–995. MR1252935

[PR98] Bernadette Perrin-Riou, *Systèmes d'Euler p-adiques et théorie d'Iwasawa*, Ann. Inst. Fourier (Grenoble) **48** (1998), no. 5, 1231–1307. MR1662231

[PR04] Robert Pollack and Karl Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, Ann. of Math. (2) **159** (2004), no. 1, 447–464, DOI 10.4007/annals.2004.159.447. MR2052361

[PS11] Jeehoon Park and Shahab Shahabi, *Plus/minus p-adic L-functions for Hilbert modular forms*, J. Algebra **342** (2011), 197–211, DOI 10.1016/j.jalgebra.2011.04.033. MR2824537

[Roh84] David E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), no. 3, 409–423, DOI 10.1007/BF01388636. MR735333

[Roh89] David E. Rohrlich, *Nonvanishing of L-functions for* GL(2), Invent. Math. **97** (1989), no. 2, 381–403, DOI 10.1007/BF01389047. MR1001846

[Rub85] Karl Rubin, *Elliptic curves and $\mathbf{Z}_p$-extensions*, Compositio Math. **56** (1985), no. 2, 237–250. MR809869

[Rub87] Karl Rubin, *Local units, elliptic units, Heegner points and elliptic curves*, Invent. Math. **88** (1987), no. 2, 405–422, DOI 10.1007/BF01388915. MR880958

[Rub91] Karl Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68, DOI 10.1007/BF01239508. MR1079839

[Rub92] Karl Rubin, *Stark units and Kolyvagin's "Euler systems"*, J. Reine Angew. Math. **425** (1992), 141–154, DOI 10.1515/crll.1992.425.141. MR1151317

[Rub96] Karl Rubin, *A Stark conjecture "over* **Z**" *for abelian L-functions with multiple zeros*, Ann. Inst. Fourier (Grenoble) **46** (1996), no. 1, 33–62. MR1385509

[Rub00] Karl Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147, Hermann Weyl Lectures, The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000. MR1749177

[Wil78] A. Wiles, *Higher explicit reciprocity laws*, Ann. Math. (2) **107** (1978), no. 2, 235–254. MR0480442

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551, DOI 10.2307/2118559. MR1333035

Department of Mathematics, Koç University, 34450 Sariyer, Istanbul, Turkey
E-mail address: kbuyukboduk@ku.edu.tr
Current address: School of Mathematics and Statistics, University College Dublin, Belfield, Dublin 4, Ireland