A GALOIS COHOMOLOGICAL PROOF OF GROSS'S FACTORIZATION THEOREM

DANIEL KRIZ

Abstract. In this note, we give a new proof for Gross's factorization of the Katz p-adic L-function restricted to the cyclotomic line into two Kubota-Leopoldt p-adic L-functions, formulated via Iwasawa theory as a factorization of characteristic ideals of the Pontryagin duals of relevant Selmer groups. Our argument uses methods of Galois cohomology.

Contents

1. Notation and Conventions

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Throughout, let p denote an odd prime number and fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Fix a prime $\overline{p}$ of $\overline{\mathbb{Q}}$ above p, which is equivalent to fixing an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, and an identification between $G_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and the decomposition group of $\overline{p}$. Fix an identification $\mathbb{C} \cong \overline{\mathbb{Q}}_p$ which is compatible with the embeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Let $K/\mathbb{Q}$ be an imaginary quadratic extension of fundamental discriminant D_K and in which p splits; write $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. Our convention will be that $\mathfrak{p}$ denotes the prime attached to a (henceforth) fixed embedding $K \hookrightarrow \overline{\mathbb{Q}}_p$. Let $G_K := \mathrm{Gal}(\overline{K}/K)$. Given a place v of K, let $I_v \subset G_K$ denote the inertia group of any prime of $\overline{K}$ above v, and let $\mathbb{F}_v$ denote the residue field at v. Let $\varepsilon_K : \mathrm{Gal}(K/\mathbb{Q}) \to \overline{\mathbb{Q}}_p^\times$ be the quadratic character associated with K.

Let K_∞ denote the unique $\mathbb{Z}_p^2$-extension of K. Such an extension has an action of $\mathrm{Gal}(K/\mathbb{Q})$ (given by conjugation), and let K_∞^+ and K_∞^- denote the corresponding $+/-$-isotypic components, respectively; we call these the *cyclotomic* and *anticyclotomic* $\mathbb{Z}_p$-extensions of K, respectively. Let $\Gamma_K = \mathrm{Gal}(K_\infty/K)$, $\Gamma_K^+ = \mathrm{Gal}(K_\infty^+/K)$ and $\Gamma_K^- = \mathrm{Gal}(K_\infty^-/K)$, so that $\Gamma_K^+ \cong \mathbb{Z}_p$ and $\Gamma_K^- \cong \mathbb{Z}_p$. Let $\Lambda_K = \mathbb{Z}_p[\![\Gamma_K]\!]$, $\Lambda_K^+ = \mathbb{Z}_p[\![\Gamma_K^+]\!]$ and $\Lambda_K^- = \mathbb{Z}_p[\![\Gamma_K^-]\!]$. Given the integer ring $\mathcal{O}$ of any finite extension of $\mathbb{Z}_p$, let $\Lambda_{K,\mathcal{O}} = \Lambda_K \otimes \mathcal{O}$ and similarly define $\Lambda_{K,\mathcal{O}}^\pm$.

Given a p-adic Dirichlet character $\chi : \mathbb{A}_K^\times \to \overline{\mathbb{Q}}_p^\times$, let $\mathbb{Z}_p[\chi]$ be the (finite) extension of $\mathbb{Z}_p$ obtained by adjoining the values of χ to $\mathbb{Z}_p$. Henceforth, assume $\mathbb{Z}_p[\chi] \subset \mathcal{O}$; when $\mathcal{O} = \mathbb{Z}_p[\chi]$, then put $\Lambda_{K,\mathcal{O}} = \Lambda_{K,\chi}$. Note that for any χ, $\Lambda_{K,\mathcal{O}}$ has a natural G_K action given by $\Psi_K : G_K \twoheadrightarrow \Gamma_K \hookrightarrow \Lambda_K$, and let $\Lambda_{K,\mathcal{O}}(\chi)$ denote the χ-twist (i.e., the module where the Galois action is given by $\Psi_K \otimes \chi$). Similarly, define $\Lambda^\pm_{K,\mathcal{O}}$, $\Psi^\pm_K : G_K \twoheadrightarrow \Gamma^\pm_K$, and $\Lambda^\pm_{K,\mathcal{O}}(\chi)$, and Λ_χ for any p-adic Hecke character $\chi : \mathbb{A}_\mathbb{Q}^\times \to \overline{\mathbb{Q}}_p^\times$.

Recall that an *algebraic Hecke character over K of infinity type (m,n) over K* is an idèlic character $\Phi : K^\times \backslash \mathbb{A}_K^\times \to \mathbb{C}^\times$ such that the local character at the unique infinite place is given by $\phi_\infty(z) = z^m \overline{z}^n$. Recall the associated *p-adic avatar of Φ* is defined via the (inverse of the) Artin reciprocity map: $\phi : G_K^{ab} \xrightarrow{rec_K^{-1}} K^\times \backslash \mathbb{A}_K^\times / \mathbb{C}^\times \to \overline{\mathbb{Q}}_p^\times$ by $\phi(x) = \Phi(x) x_\infty^{-m} \overline{x}_\infty^{-n} x_\mathfrak{p}^m x_{\overline{\mathfrak{p}}}^n$ for $x \in \mathbb{A}_K^\times$; here we use the above identification $\mathbb{C} \cong \overline{\mathbb{Q}}_p$.

Let $\mathbb{Q}_\infty$ denote the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and let $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$. Then we have a natural isomorphism $\Gamma_K^+ \cong \Gamma$. Let $\chi_{\mathrm{cyc}} : G_\mathbb{Q} \twoheadrightarrow \mathrm{Gal}(K(\mu_{p^\infty})/K) \cong \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_p^\times$ be the *p-adic cyclotomic character*, i.e. the p-adic avatar of the *inverse* of the usual idèlic norm character $\mathbb{N}_\mathbb{Q} : \mathbb{A}_\mathbb{Q}^\times \to \mathbb{C}^\times$ (of infinity type 1). Hence χ_{cyc} is given by $\chi_{\mathrm{cyc}} : \mathrm{Gal}(K(\mu_{p^\infty})/K) \xrightarrow{\sim} \mathbb{Z}_p^\times$ given by $\sigma(\zeta) = \zeta^{\chi_{\mathrm{cyc}}(\sigma)}$. Since $\chi_{\mathrm{cyc}}(x) \in \mathbb{Z}_p^\times = \mu_{2(p-1)} \times (1 + 2p\mathbb{Z}_p)$, we may write it uniquely as $\chi_{\mathrm{cyc}}(x) = \omega(x)\langle x \rangle$ where $\langle x \rangle \equiv 1 \mod 2p$; $\omega : G_\mathbb{Q} \to \mu_{2(p-1)}$ is called the *Teichmüller character*. Let $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$.

Given a topological $\mathbb{Z}_p$-module M, let $M^* = \mathrm{Hom}_{\mathrm{cts}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ denote its Pontryagin dual (henceforth, the subscript "cts" will be suppressed, as all homomorphisms, cocycles and characters under our consideration will be continuous). Recall that given a G-module M, M^* has a natural action given by $(gf)(x) = f(gx)$. For a G-module M, we will let M^G denote the elements of M fixed by the action of G. In the case where $G = G_K$ for some global, local, or finite field K, we write $H^i(K, M) := H^i(G_K, M)$ for the Galois cohomology groups. Henceforth, for a G-module M let $M(n) := M \otimes \chi_{\mathrm{cyc}}^n$ denote the G-module called the *n^{th} Tate twist of M*.

For a general number field L and a finite set of places Σ of L, let L^Σ denote the maximal extension of L (in $\overline{\mathbb{Q}}$) that is unramified outside Σ. Let $G_{L,\Sigma} = \mathrm{Gal}(L^\Sigma/L)$.

2. Preliminaries and Main Theorem

Our main result is to recover a theorem of Gross [5] which factorizes a certain 1-variable p-adic L-function over an imaginary quadratic field K due to Katz into two Kubota-Leopoldt p-adic L-functions over $\mathbb{Q}$. While Gross explicitly compares the measures underlying these two p-adic L-functions in his proof, we use Galois cohomology in order to relate the characteristic ideals of Selmer groups associated with these p-adic L-functions by the Iwasawa main conjectures (now proven) for GL_1 over K and over $\mathbb{Q}$. In order to state our main result, we need to recall some statements from Iwasawa theory.

2.1. The Katz p-adic L-function and some statements from Iwasawa theory.

Recall that the Katz p-adic L-function $\mathcal{L}_p$ interpolates classical L-values of a range of (norm-shifted) anticyclotomic algebraic Hecke characters Φ_v of infinity type $(-(k+d), d)$ where $k \geq 1$ and $d \geq 0$ ([6]). Denote the range of corresponding p-adic avatars by $\mathbb{X}_\mathfrak{p}$. The p-adic avatars of these shifted anticyclotomic Hecke characters are thus given by characters $\phi : \Gamma_K^- \to \overline{\mathbb{Q}}_p^\times$, where $\phi_\mathfrak{p}(x) = \Phi_\mathfrak{p}(x) x^{-(k+d)}$ and $\phi_{\overline{\mathfrak{p}}}(x) = \Phi_{\overline{\mathfrak{p}}}(x) x^d$. Viewing $\Lambda^*_{K,\phi}(\phi)$ as a p-adic Galois

representation of $G_{K_\mathfrak{p}}$ and $G_{K_{\overline{\mathfrak{p}}}}$, these representations are Hodge-Tate with weights $k+d$ and $-d$, respectively (under our conventions; several authors take the negative of this definition for the Hodge-Tate weights). In terms of Hodge filtrations, this implies that

$$\mathrm{Fil}^i \Lambda^*_{K,\phi}(\phi_\mathfrak{p}) = \begin{cases} \Lambda^*_{K,\phi}(\phi_\mathfrak{p}) & i \leq k+d \\ 0 & i > k+d \end{cases} \qquad \mathrm{Fil}^i \Lambda^*_{K,\phi}(\phi_{\overline{\mathfrak{p}}}) = \begin{cases} \Lambda^*_{K,\phi}(\phi_{\overline{\mathfrak{p}}}) & i \leq -d \\ 0 & i > -d \end{cases}.$$

In particular, since $k \geq 1$ and $d \geq 0$, we have $F^+\Lambda^*_{K,\phi}(\phi_\mathfrak{p}) := \mathrm{Fil}^1 \Lambda^*_{K,\phi}(\phi_\mathfrak{p}) = \Lambda^*_{K,\phi}(\phi_\mathfrak{p})$ and $F^+\Lambda^*_{K,\phi}(\phi_{\overline{\mathfrak{p}}}) := \mathrm{Fil}^1 \Lambda^*_{K,\phi}(\phi_{\overline{\mathfrak{p}}}) = 0$. The Bloch-Kato-Greenberg Selmer groups (see [4]) attached to the above Galois representations $\Lambda^*_{K,\phi}(\phi)$ are thus

$$\begin{aligned} &\mathrm{Sel}_p(\phi) \\ &= \ker \left\{ H^1(K, \Lambda^*_{K,\phi}(\phi)) \xrightarrow{\prod_v \mathrm{res}_v} \prod_{v \nmid p} H^1(I_v, \Lambda^*_{K,\phi}(\phi_v)) \times \prod_{v|p} H^1(I_v, \Lambda^*_{K,\phi}(\phi_v)/F^+\Lambda^*_{K,\phi}(\phi_v)) \right\} \\ &= \ker \left\{ H^1(K, \Lambda^*_{K,\phi}(\phi)) \xrightarrow{\prod_{v \neq \mathfrak{p}} \mathrm{res}_v} \prod_{v \neq \mathfrak{p}} H^1(I_v, \Lambda^*_{K,\phi}(\phi_v)) \right\}. \end{aligned}$$

The last line above thus defines the p-adic Selmer group associated to ϕ, i.e., the Selmer group which interpolates the Bloch-Kato-Greenberg Selmer groups for $\phi \in \mathbb{X}_\mathfrak{p}$.

Let $X_p(\phi) = \mathrm{Sel}_p(\phi)^*$. The Main Conjecture (now Theorem) of Iwasawa Theory over K ([8]) states that

$$\mathrm{char}_{\Lambda_{K,\phi}} X_p(\phi) = (\mathcal{L}_p^{\mathrm{Katz}}(\phi^{-1}))$$

where $\mathrm{char}_{\Lambda_{K,\phi}} X_p(\phi)$ denotes the characteristic ideal of $X_p(\phi)$ viewed as a $\Lambda_{K,\phi}$-module, and $\mathcal{L}_p^{\mathrm{Katz}}(\phi^{-1}, 0) \in \Lambda_{K,\phi}$ is the Katz p-adic L-function.

By the Main Theorem of Iwasawa Theory, $\mathrm{Sel}_p(\phi)[\gamma_- - 1]$ corresponds to the restriction of $\mathcal{L}_p(\phi, s)$ to the cyclotomic line. Its Pontryagin dual is $X_p(\phi)/(\gamma_- - 1)X_p(\phi)$. Restricting to characters $\phi : \Gamma_K^+ \to \overline{\mathbb{Q}}_p^\times$, we have the following version of the Main Theorem of Iwasawa Theory "restricted to the cyclotomic line"

$$\mathrm{char}_{\Lambda^+_{K,\phi}}(X_p(\phi)/(\gamma_- - 1)X_p(\phi)) = (\mathcal{L}_p^{\mathrm{Katz},+}(\phi^{-1}))$$

where $\mathrm{char}_{\Lambda^+_{K,\phi}} X_p(\phi)$ denotes the characteristic ideal of $X_p(\phi)$ viewed as a $\Lambda^+_{K,\phi}$-module, and $\mathcal{L}_p^{\mathrm{Katz},+}(\phi^{-1}) \in \Lambda^+_{K,\phi}$ is the Katz p-adic L-function restricted to the cyclotomic line.

We will now briefly recall some Iwasawa theory over $\mathbb{Q}$, with which one associates special values of the Kubota-Leopoldt p-adic L-function (defined, for example, in [10]). For a more comprehensive overview of classical Iwasawa theory, we refer the reader to notes of Skinner, [9]. Suppose we are given two families of p-adic Hecke characters $\phi : \mathbb{A}_\mathbb{Q}^\times \to \overline{\mathbb{Q}}_p^\times$ whose associated p-adic Galois representation $\Lambda^*_\phi(\phi)$ have Hodge-Tate weights $n > 0$ and $n \leq 0$ *odd* at p, respectively. Thus, for each of these families,

$$\mathrm{Fil}^i \Lambda^*_\phi(\phi_p) = \begin{cases} \Lambda^*_\phi(\phi_p) & i \leq n \\ 0 & i > n \end{cases}.$$

For the first family corresponding to the range $n > 0$, we have $F^+\Lambda^*_\phi(\phi_p) := \mathrm{Fil}^1\,\Lambda^*_\phi(\phi_p) = \Lambda^*_\phi(\phi_p)$. For the second family corresponding to the range $n \leq 0$, we have $F^+\Lambda^*_\phi(\phi_p) := \mathrm{Fil}^1\,\Lambda^*_\phi(\phi_p) = 0$. The corresponding Bloch-Kato-Greenberg Selmer groups are thus

$$\begin{aligned}
&H^1_p(\mathbb{Q}, \Lambda^*_\phi(\phi)) \\
&= \ker\left\{ H^1(\mathbb{Q}, \Lambda^*_\phi(\phi)) \xrightarrow{\prod_\ell \mathrm{res}_\ell} \prod_{\ell \neq p} H^1(I_\ell, \Lambda^*_\phi(\phi_\ell)) \times H^1(I_p, \Lambda^*_\phi(\phi_p)/F^+\Lambda^*_\phi(\phi_p)) \right\} \\
&= \ker\left\{ H^1(\mathbb{Q}, \Lambda^*_\phi(\phi)) \xrightarrow{\prod_{\ell \neq p} \mathrm{res}_\ell} \prod_{\ell \neq p} H^1(I_\ell, \Lambda^*_\phi(\phi_\ell)) \right\} \\
&= \ker\left\{ H^1(G_{\mathbb{Q},S}, \Lambda^*_\phi(\phi)) \xrightarrow{\prod_{\ell \in S, \ell \neq p} \mathrm{res}_\ell} \prod_{\ell \in S} H^1(I_\ell, \Lambda^*_\phi(\phi_\ell)) \right\}
\end{aligned}$$

where S is any finite set of places of $\mathbb{Q}$ containing the places at which ϕ is ramified, and

$$\begin{aligned}
&H^1_f(\mathbb{Q}, \Lambda^*_\phi(\phi)) \\
&= \ker\left\{ H^1(\mathbb{Q}, \Lambda^*_\phi(\phi)) \xrightarrow{\prod_\ell \mathrm{res}_\ell} \prod_{\ell \neq p} H^1(I_\ell, \Lambda^*_\phi(\phi_\ell)) \times H^1(I_p, \Lambda^*_\phi(\phi_p)/F^+\Lambda^*_\phi(\phi_p)) \right\} \\
&= \ker\left\{ H^1(\mathbb{Q}, \Lambda^*_\phi(\phi)) \xrightarrow{\prod_\ell \mathrm{res}_\ell} \prod_{\ell} H^1(I_\ell, \Lambda^*_\phi(\phi_\ell)) \right\} \\
&= \ker\left\{ H^1(G_{\mathbb{Q},S}, \Lambda^*_\phi(\phi)) \xrightarrow{\prod_{\ell \in S} \mathrm{res}_\ell} \prod_{\ell \in S} H^1(I_\ell, \Lambda^*_\phi(\phi_\ell)) \right\}
\end{aligned}$$

where S is any finite set of places of $\mathbb{Q}$ containing the places where ϕ is ramified and p.

Let $X_p(\phi) = H^1_p(\mathbb{Q}, \Lambda^*_\phi(\phi))^*$ and $X_f(\phi) = H^1_f(\mathbb{Q}, \Lambda^*_\phi(\phi))^*$. The Main Conjecture (now Theorem) of Iwasawa Theory over $\mathbb{Q}$ ([7], [9, Section 4.5]) says that that when ϕ is *odd*,

$$\mathrm{char}_{\Lambda_\phi} X_f(\phi) = (\mathcal{L}_p(\phi^{-1}))$$

where $\mathrm{char}_{\Lambda_\phi} X_f(\phi)$ denotes the characteristic ideal of $X_f(\phi)$ viewed as a Λ_ϕ-module and $\mathcal{L}_p(\phi^{-1}) \in \Lambda_\phi$ is the Kubota-Leopoldt p-adic L-function. (Here we are taking the normalization of $\mathcal{L}_p$ as in [9, Section 4.2].) Fix a topological generator γ of Γ. Given an $s \in \mathbb{Z}_p$, denote the specialization at of $\mathcal{L}_p(\phi^{-1})$ at $\gamma \mapsto \langle\gamma\rangle^{-s}$ by $L_p(\phi^{-1}\omega, s)$.

When ϕ is even, we first invoke Greenberg's "functional equation for characteristic ideals", [3, Theorem 2] to relate the characteristic ideal of its Selmer group to that of its dual character:

$$\mathrm{char}_{\Lambda_\phi} X_p(\phi) = \mathrm{char}_{\Lambda_\phi} X_f(\phi^{-1}\chi_{\mathrm{cyc}})^\iota = (\mathcal{L}_p(\phi\chi_{\mathrm{cyc}}^{-1})^\iota).$$

where $\mathrm{char}_{\Lambda_\phi} X_p(\phi)$ denotes the characteristic ideal of $X_p(\phi)$ viewed as a Λ_ϕ-module, and $\mathcal{L}_p(\phi\chi_{\mathrm{cyc}}^{-1})^\iota \in \Lambda_\phi^\iota$ is the "involuted" Kubota-Leopoldt p-adic L-function, i.e. an element whose specialization at $\langle\cdot\rangle^{-s}$ for $s \in \mathbb{Z}_p$ is $L_p(\phi\chi_{\mathrm{cyc}}^{-1}\omega(\langle\cdot\rangle^{-s} \circ \Psi^\iota), 0) = L_p(\phi\langle\cdot\rangle^{s-1}, 0) = L_p(\phi, 1-s)$. Here Λ_ϕ^ι is the Λ_ϕ-module whose underlying $\mathbb{Z}_p$-module is Λ_ϕ but on which Γ acts through the involution $\iota(\gamma) = \gamma^{-1}$ (so that the Galois action $\Psi^\iota : G_\mathbb{Q} \twoheadrightarrow \Gamma \xrightarrow{\iota} \Gamma \hookrightarrow \Lambda_\phi$ is also involuted).

Our Main Theorem is a version of Gross's factorization of the Katz p-adic L-function restricted to the cyclotomic line ([5]), stated in terms of characteristic ideals.

Theorem 1 (Main Theorem)**.** *Let $\phi_K : G_K \twoheadrightarrow \Gamma_K \to \overline{\mathbb{Q}}_p^\times$ be such that $\phi_K = \phi_{|_{G_K}}$ where $\phi : G_{\mathbb{Q}} \twoheadrightarrow \Gamma \to \overline{\mathbb{Q}}_p^\times$ is an even Dirichlet character. Then under the canonical identifications $\Gamma_K^+ \cong \Gamma$ and $\Lambda_{K,\phi_K}^+ \cong \Lambda_\phi$, we have the following factorization of ideals of Λ_ϕ:*

$$(\mathcal{L}_p^{\mathrm{Katz},+}(\phi_K^{-1})) = (\mathcal{L}_p(\phi^{-1}\varepsilon_K))(\mathcal{L}_p(\phi\chi_{\mathrm{cyc}}^{-1})^\iota).$$

Remark 2. Theorem 1 thus implies

$$\mathcal{L}_p^{\mathrm{Katz},+}(\phi_K^{-1}) = \mathcal{L}_p(\phi^{-1}\varepsilon_K)\mathcal{L}_p(\phi\chi_{\mathrm{cyc}}^{-1})^\iota \mod \Lambda_\phi^\times. \tag{1}$$

Taking the specialization at $\langle\cdot\rangle^{-s}$ for $s \in \mathbb{Z}_p$, we have

$$L_p^{\mathrm{Katz},+}(\phi_K, s) = L_p(\phi\varepsilon_K\omega, s)L_p(\phi^{-1}, 1-s) \mod \mathbb{Z}_p[\phi]^\times$$

which is Gross's original factorization theorem on the cyclotomic line, modulo a p-adic unit. In fact, we can recover Gross's original theorem (i.e., show that the "equality up to unit" in (1) is an actual equality) using some specific special value formulas.

Corollary 3. *Let ϕ, ϕ_K be as in the notation of Theorem 1. Then for any $s \in \mathbb{Z}_p$, we have*

$$L_p^{\mathrm{Katz},+}(\phi_K, s) = L_p(\phi\varepsilon_K\omega, s)L_p(\phi^{-1}, 1-s). \tag{2}$$

Proof. First, note that it suffices to establish this equality at $s = 0$ for all non-trivial finite-order characters. This follows because $\langle\cdot\rangle^{-s}$, for any $s \in \mathbb{Z}_p$, can be approximated by a sequence of finite-order characters, so that if (1) is established at all such specializations, then we have shown (1) holds on a dense subset of the weight space, and so by Theorem 1 we know that we have shown an equality of continuous measures on a dense subset and thus we have equality everywhere. For any finite-order character ϕ, (2) follows from the special value formulas in [5, Sections 3 and 5, eq. (3.5)]. □

The proof of the Theorem 1 will be given in Section 3.

2.2. **Acknowledgements.** The author would like to thank Chris Skinner for helpful discussions during the preparation of this note.

2.3. **A few control theorems.** Henceforth, fix topological generators $\gamma_\pm$ of $\Gamma_K^\pm$ respectively, and let γ be the topological generator of Γ which is the image of γ_+ under the isomorphism $\Gamma_K^+ \cong \Gamma$. (Note that we can write $\Lambda_K = \mathbb{Z}_p[\![T, S]\!]$ where $T = \gamma_+ - 1$ and $S = \gamma_- - 1$.)

Suppose now that $\phi_K : \Gamma_K^+ \to \overline{\mathbb{Q}}_p^\times$ is a *cyclotomic* p-adic Galois character. Using the canonical isomorphism $\Gamma_K^+ \cong \Gamma$, we can view ϕ_K as a character $\phi : \Gamma \to \overline{\mathbb{Q}}_p^\times$, where ϕ is related to ϕ_K by $\phi_{|_{G_K}} = \phi_K$ (here we precompose with the projection $G_K \twoheadrightarrow \Gamma_K^+$). Assume henceforth that ϕ is *even*.

Remark 4. For the rest of the paper, we will let $M_K = \Lambda_{K,\phi_K}^*(\phi_K)$ and for any place v of K, $M_{K_v} = \Lambda_{K,\phi_K}^*(\phi_{K,v})$ (as G_{K_v}=modules). Similarly, let $M_K^\pm = \Lambda_{K,\phi_K}^{\pm,*}(\phi_K)$, $M_{K_v}^\pm = \Lambda_{K,\phi_K}^{\pm,*}(\phi_{K_v})$, $M = \Lambda_\phi^*(\phi)$ and for any place ℓ of $\mathbb{Q}$, $M_\ell = \Lambda_\phi^*(\phi_\ell)$ (as a $G_{\mathbb{Q}_\ell}$-module).

Lemma 5. *We have* $M_K^{G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}}} = 0$, $M_{K_{\overline{\mathfrak{p}}}}^{+,I_{\overline{\mathfrak{p}}}} = 0$ *and* $M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}}/(\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}} = 0$. *Furthermore,* $M_p^{I_p} = M_p(\varepsilon_{K,p})^{I_p} = 0$.

Proof. First recall the projection $G_K \twoheadrightarrow \Gamma_K = \Gamma_K^+ \oplus \Gamma_K^-$. Since the cyclotomic $\mathbb{Z}_p$-extension K_∞^+/K is *totally ramified* at $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ (and totally unramified everywhere else), then in fact the restriction $\Psi_{K|I_{\mathfrak{p}}} : I_{\mathfrak{p}} = I_{\overline{\mathfrak{p}}} \hookrightarrow G_K \twoheadrightarrow \Gamma_K^+$ is a surjection. Recalling that $M_K = \mathrm{Hom}(\Lambda_{K,\phi_K}, \mathbb{Q}_p/\mathbb{Z}_p(\phi_K))$ and $M_{K_{\overline{\mathfrak{p}}}} = \mathrm{Hom}(\Lambda_{K,\phi_K}^+, \mathbb{Q}_p/\mathbb{Z}_p(\phi_{K,\overline{\mathfrak{p}}}))$ where the original (untwisted) Galois action is given by $\Psi_K : G_K \twoheadrightarrow \Gamma_K$, the surjections $G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}} \twoheadrightarrow \Gamma_K$ and $I_{\overline{\mathfrak{p}}} \twoheadrightarrow \Gamma_K^+$ imply that

$$M_K^{G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}}} = \{f \in \mathrm{Hom}(\Lambda_{K,\phi_K}, \mathbb{Q}_p/\mathbb{Z}_p) : f(g) = \phi_K^{-1}(g)f(1_{\Gamma_K}) = 0, \forall g \in \Gamma_K\} = 0$$

$$M_{K_{\overline{\mathfrak{p}}}}^{+,I_{\overline{\mathfrak{p}}}} = \{f \in \mathrm{Hom}(\Lambda_{K,\phi_K}^+, \mathbb{Q}_p/\mathbb{Z}_p) : f(g) = \phi_{K,\overline{\mathfrak{p}}}^{-1}(g)f(1_{\Gamma_K^+}) = 0, \forall g \in \Gamma_K^+\} = 0$$

(since $f(1_{\Gamma_K}) = f(1_{\Gamma_K^+}) = 0$). The fact that $M_p^{I_p} = 0$ now follows from the canonical isomorphism $M_K^+ \cong M$ and $I_{\overline{\mathfrak{p}}} = I_p$. Since p is split in K, ε_K is unramified at p, i.e. $\varepsilon_{K,p}(I_p) = 1$, so $M_p(\varepsilon_{K,p})^{I_p} = 0$ also follows.

We will now show that $M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}}/(\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}} = 0$. Note that

$$M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}} = \{f \in \mathrm{Hom}(\Lambda_{K,\phi_K}, \mathbb{Q}_p/\mathbb{Z}_p) : f(\Psi_K(g)x) = \phi_{K,\overline{\mathfrak{p}}}^{-1}(g)f(x), \forall g \in I_{\overline{\mathfrak{p}}}, \forall x \in \Gamma_K\}.$$

We claim that $M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}} \cap (\gamma_- - 1)M_{K_{\overline{p}}} = (\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}}$. First, note that $\Gamma_K \cong \mathbb{Z}_p^2$ is in particular *abelian*, and so for any $\alpha \in I_{\overline{\mathfrak{p}}}$ and any $(\gamma_- - 1)f \in (\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}}$ where $f \in M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}}$ and so $\Psi_K(\alpha)f = f$, we have

$$\Psi_K(\alpha)(\gamma_- - 1)f = (\gamma_- - 1)\Psi_K(\alpha)f = (\gamma_- - 1)f$$

and so since $(\gamma_- - 1)f \in (\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}}$ was arbitary, we have $(\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}} \subset M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}} \cap (\gamma_- - 1)M_{K_{\overline{p}}}$. Now take any $(\gamma_- - 1)f \in M_{K_{\overline{p}}}^{I_{\overline{\mathfrak{p}}}} \cap (\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}$ where $f \in M_{K_{\overline{\mathfrak{p}}}}$, meaning

$$(\gamma_- - 1)f = \Psi_K(\alpha)(\gamma_- - 1)f = (\gamma_- - 1)\Psi_K(\alpha)f$$

and so

$$(\gamma_- - 1)(\Psi_K(\alpha) - 1)f = 0$$

which implies that $(\Psi_K(\alpha) - 1)f$ factors through the quotient $\Lambda_K \twoheadrightarrow \Lambda_K^+$, and that the induced map $(\Psi_K(\alpha) - 1)f : \Lambda_K \twoheadrightarrow \Lambda_K^+$ is in $M_{K_{\overline{\mathfrak{p}}}}^{+,I_{\overline{\mathfrak{p}}}} = 0$. Hence $(\Psi_K(\alpha) - 1)f = 0$, and so since $\alpha \in I_{\overline{\mathfrak{p}}}$ was arbitrary, we have $f \in M_{K_{\overline{\mathfrak{p}}}}$, and so $(\gamma_- - 1)f \in (\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}}$. Since $(\gamma_- - 1)f \in M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}} \cap (\gamma_- - 1)M_{K_{\overline{p}}}$ was arbitrary, we thus have $M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}} \cap (\gamma_- - 1)M_{K_{\overline{p}}} \subset (\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}}$. Hence, the claim is established.

In particular we have $M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}}/(\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}} \hookrightarrow M_{K_{\overline{\mathfrak{p}}}}/(\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}$, so we are done if we can show that $M_{K_{\overline{\mathfrak{p}}}}/(\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}} = 0$. For this, note that since Pontryagin duality interchanges quotients and torsion, we have

$$M_{K_{\overline{\mathfrak{p}}}}/(\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}} = (\Lambda_{K,\phi_K}(\phi_{K,\overline{\mathfrak{p}}})[\gamma_- - 1])^*.$$

As a Λ_K-module, we have $\Lambda_{K,\phi_K}(\phi_{K,\overline{\mathfrak{p}}})[\gamma_- - 1] = \mathbb{Z}_p[\![\gamma_+ - 1, \gamma_- - 1]\!][\gamma_- - 1] = 0$ since $\gamma_- - 1$ is a free variable. Now dualizing, we are done. □

Now let

$$\begin{aligned}\mathrm{Sel}_p^+(\phi_K) :&= \ker\left\{H^1(K,M_K^+)\xrightarrow{\prod_v \mathrm{res}_v}\prod_{v\nmid p}H^1(I_v,M_{K_v}^+)\times\prod_{v|p}H^1(I_v,M_{K_v}^+/F^+M_{K_v}^+)\right\}\\ &= \ker\left\{H^1(K,M_K^+)\xrightarrow{\prod_{v\in S_K,v\neq\mathfrak{p}}\mathrm{res}_v}\prod_{v\neq\mathfrak{p}}H^1(I_v,M_{K_v}^+)\right\}\\ &= \ker\left\{H^1(G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}},M_K^+)\xrightarrow{\mathrm{res}_{\overline{\mathfrak{p}}}}H^1(I_{\overline{\mathfrak{p}}},M_{K_{\overline{\mathfrak{p}}}}^+)\right\}.\end{aligned}$$

Corollary 6. *We have*

$$\begin{aligned}\mathrm{Sel}_p^+(\phi_K) &= \ker\left\{H^1(G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}},M_K^+)\xrightarrow{\mathrm{res}_{\overline{\mathfrak{p}}}}H^1(K_{\overline{\mathfrak{p}}},M_{K_{\overline{\mathfrak{p}}}}^+)\right\},\\ &= \ker\left\{H^1(G_{K,S_K},M_K^+)\xrightarrow{\prod_{v\neq\mathfrak{p}}\mathrm{res}_v}H^1(K_v,M_{K_v}^+)\right\},\\ H_f^1(\mathbb{Q},M(\varepsilon_K)) &= \ker\left\{H^1(G_{\mathbb{Q},S},M(\varepsilon_K))\xrightarrow{\prod_{\ell\in S}\mathrm{res}_\ell}\prod_{\ell\in S}H^1(\mathbb{Q}_\ell,M_\ell(\varepsilon_{K,\ell}))\right\}\end{aligned}$$

where S_K is any finite set of places of K containing $\{\mathfrak{p},\overline{\mathfrak{p}}\}$ and S is any finite set of places of $\mathbb{Q}$ containing the places where $\phi\varepsilon_K$ is ramified and p.

Proof. First note that the restriction $H^1(G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}},M_K^+)\to H^1(I_{\overline{\mathfrak{p}}},M_{K_{\overline{\mathfrak{p}}}}^+)$ factors through $H^1(G_{K,\{\mathfrak{p}\}},M_K^+)$. By Lemma 5, we have $H^1(K_{\overline{\mathfrak{p}}},M_{K_{\overline{\mathfrak{p}}}}^+)\hookrightarrow H^1(I_{\overline{\mathfrak{p}}},M_{K_{\overline{\mathfrak{p}}}}^+)$, so the restriction of $x\in H^1(G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}},M_K^+)$ to $H^1(I_{\overline{\mathfrak{p}}},M_{K,\overline{\mathfrak{p}}}^+)$ is 0 if and only if its restriction to $H^1(K_{\overline{\mathfrak{p}}},M_{K,\overline{\mathfrak{p}}}^+)$ is 0. For $v\nmid p$, the assertion follows because $G_{\mathbb{F}_v}$ has profinite order prime to p, so $\ker(H^1(K_v,M_{K_v}^+)\xrightarrow{\mathrm{res}_v}H^1(I_v,M_{K_v}^+))=H^1(\mathbb{F}_v,M_{K_v}^+)=0$. The assertion for $H_f^1(\mathbb{Q},M)$ follows completely analogously. □

Now we show that

Proposition 7.

$$\mathrm{Sel}_p(\phi_K)[\gamma_- - 1]\cong\mathrm{Sel}_p^+(\phi_K).$$

Proof. We have the short exact sequences of $G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}}$-modules

$$0\to M_K^+=M_K[\gamma_- - 1]\to M_K\xrightarrow{\gamma_- -1}M_K\to 0$$

and the short exact sequence of $I_{\overline{\mathfrak{p}}}$-modules

$$0\to M_{K_{\overline{\mathfrak{p}}}}^+=M_{K_{\overline{\mathfrak{p}}}}[\gamma_- - 1]\to M_{K_{\overline{\mathfrak{p}}}}\xrightarrow{\gamma_- -1}M_{K_{\overline{\mathfrak{p}}}}\to 0.$$

From the corresponding long exact sequences of group cohomology, we obtain the following commutative diagram

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & \mathrm{Sel}_p^+(\phi_K) & \longrightarrow & \mathrm{Sel}_p(\phi_K)[\gamma_- - 1] & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_K^{G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}}}/(\gamma_- - 1)M_K^{G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}}} & \longrightarrow & H^1(G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}}, M_K^+) & \longrightarrow & H^1(G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}}, M_K)[\gamma_- - 1] & \longrightarrow & 0 \\
 & & \downarrow \mathrm{res}_{\overline{\mathfrak{p}}} & & \downarrow \mathrm{res}_{\overline{\mathfrak{p}}} & & \downarrow \mathrm{res}_{\overline{\mathfrak{p}}} & & \\
0 & \longrightarrow & M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}}/(\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}} & \longrightarrow & H^1(I_{\overline{\mathfrak{p}}}, M_{K_{\overline{\mathfrak{p}}}}^+) & \longrightarrow & H^1(I_{\overline{\mathfrak{p}}}, M_{K_{\overline{\mathfrak{p}}}})[\gamma_- - 1] & \longrightarrow & 0
\end{array}$$

where the horizontal and vertical arrows are exact. By Lemma 5, we have $M_K^{G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}}} = 0$ and $M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}}/(\gamma_- - 1)M_{K_{\overline{\mathfrak{p}}}}^{I_{\overline{\mathfrak{p}}}} = 0$. Thus we have $H^1(K, M_K^+) \xrightarrow{\sim} H^1(K, M_K)[\gamma_- - 1]$ and $H^1(I_{\overline{\mathfrak{p}}}, M_{K_{\overline{\mathfrak{p}}}}^+) \xrightarrow{\sim} H^1(I_{\overline{\mathfrak{p}}}, M_{K_{\overline{\mathfrak{p}}}})[\gamma_- - 1]$, and hence $\mathrm{Sel}_p^+(\phi_K) \xrightarrow{\sim} \mathrm{Sel}_p(\phi_K)[\gamma_- - 1]$, as claimed. □

2.4. **An exact sequence of Selmer groups.** Recall from the discussion in Section 2.1 that $\mathrm{Sel}_p(\phi_K)$ corresponds to the restriction of the Katz p-adic L-function to the cyclotomic line evaluated at ϕ_K. By Proposition 7, $\mathrm{Sel}_p(\phi_K)[\gamma_- - 1] = \mathrm{Sel}_p^+(\phi_K)$ is thus the pertinent Selmer group.

By Shapiro's lemma, we have an isotypic decomposition

$$H^1(K, M_K^+) = H^1(\mathbb{Q}, \mathrm{Ind}_K^{\mathbb{Q}} M_K^+) = H^1(\mathbb{Q}, M) \oplus H^1(\mathbb{Q}, M(\varepsilon_K)).$$

Recall that since p is split in K, we have $\varepsilon_{K,p} = 1$. For $v|\ell$ where ℓ splits in K, we have the usual restriction map

$$\mathrm{res}_v : H^1(K, M_K^+) = H^1(\mathbb{Q}, M) \oplus H^1(\mathbb{Q}, M(\varepsilon_K)) \to H^1(K_v, M_{K_v}^+) = H^1(I_\ell, M_\ell) = H^1(I_\ell, M_\ell(\varepsilon_{K,\ell}))$$

which is the sum of the restriction maps $H^1(\mathbb{Q}, M_\ell) \to H^1(I_\ell, M_\ell)$ and $H^1(\mathbb{Q}, M(\varepsilon_K)) \to H^1(\mathbb{Q}, M_\ell(\varepsilon_{K,\ell})) = H^1(\mathbb{Q}, M_\ell)$. In particular for $\ell = p$, we have $\mathrm{res}_{\mathfrak{p}}(x, y) = \mathrm{res}_p x + \mathrm{res}_p y$ and $\mathrm{res}_{\overline{\mathfrak{p}}}(x, y) = \mathrm{res}_p x + \mathrm{res}_p y$. If $v|\ell$ where ℓ is ramified or inert in K, we have

$$\mathrm{res}_v : H^1(K, M_K^+) \to H^1(K_v, M_{K_v}^+) = H^1(I_\ell, M_\ell) \oplus H^1(I_\ell, M_\ell(\varepsilon_{K,\ell})).$$

Let $S_K = \{v \text{ place of } K : v|pD_K\infty\}$ and $S = \{\ell \text{ place of } \mathbb{Q} : \ell|pD_K\infty\}$. Recall that by the discussion in Section 2.1 and Corollary 6, we have

$$\begin{aligned}
&\mathrm{Sel}_p^+(\phi_K) = \ker\left\{H^1(G_{K,\{\mathfrak{p},\overline{\mathfrak{p}}\}}, M_K^+) \xrightarrow{\mathrm{res}_{\overline{\mathfrak{p}}}} H^1(K_{\overline{\mathfrak{p}}}, M_{K_{\overline{\mathfrak{p}}}}^+)\right\} \\
&= \ker\left\{H^1(G_{K,S_K}, M_K^+) \xrightarrow{\prod_{v\in S_K, v\neq\mathfrak{p}} \mathrm{res}_{\overline{\mathfrak{p}}}} H^1(K_v, M_{K_v}^+)\right\} \\
&= \left\{(x, y) \in H^1(G_{\mathbb{Q},S}, M) \oplus H^1(G_{\mathbb{Q},S}, M(\varepsilon_K)) : \prod_{v\in S_K, v\neq\mathfrak{p}} \mathrm{res}_v(x, y) = 0\right\} \\
&= \left\{(x, y) \in H^1(G_{\mathbb{Q},S}, M) \oplus H^1(G_{\mathbb{Q},S}, M(\varepsilon_K)) : \mathrm{res}_\ell x = \mathrm{res}_\ell y = 0\ \forall p \neq \ell \in S, \mathrm{res}_p x = -\mathrm{res}_p y\right\}.
\end{aligned}$$

The last equality follows since the condition that $\mathrm{res}_{\overline{\mathfrak{p}}}(x,y)=0$ is equivalent to $\mathrm{res}_p x = -\mathrm{res}_p y$ by the isotypic decomposition mentioned above.

Looking at local conditions, we thus have the following exact sequence:

$$0 \to H^1_f(\mathbb{Q}, M(\varepsilon_K)) \to \mathrm{Sel}_p^+(\phi_K) \to H^1_p(\mathbb{Q}, M) \tag{3}$$

where the second and third maps are given by $y \mapsto (x,y)$ and $(x,y)\mapsto x$ under the coordinates given by $\mathrm{Sel}_p^+(\phi_K) \subset H^1(G_{\mathbb{Q},S}, M)\oplus H^1(G_{\mathbb{Q},S}, M(\varepsilon_K))$, respectively, and $H^1_f(\mathbb{Q}, M(\varepsilon_K))$ and $H^1_p(\mathbb{Q}, M)$ are described in Section 2.1:

$$H^1_f(\mathbb{Q}, M(\varepsilon_K)) = \ker\left\{ H^1(G_{\mathbb{Q},S}, M(\varepsilon_K)) \xrightarrow{\prod_{\ell\in S}\mathrm{res}_\ell} \prod_{\ell\in S} H^1(I_\ell, M_\ell(\varepsilon_{K,\ell}))\right\}$$

and

$$H^1_p(\mathbb{Q}, M) = \ker\left\{ H^1(G_{\mathbb{Q},S}, M) \xrightarrow{\prod_{\ell\in S,\ell\neq p}\mathrm{res}_\ell} \prod_{\ell\in S,\ell\neq p} H^1(I_\ell, M_\ell)\right\}.$$

The brunt of the proof of the Main Theorem will be showing one can add a "$\to 0$" to the right side of the above exact sequence. To this end, we show this assertion can be reduced to the "Key Lemma" proven in Section 3. Let

$$H^1_p(G_{\mathbb{Q},S}, M(\varepsilon_K)) = \ker\left\{ H^1(G_{\mathbb{Q},S}, M(\varepsilon_K)) \xrightarrow{\prod_{\ell\in S,\ell\neq p}\mathrm{res}_\ell} \prod_{\ell\in S,\ell\neq p} H^1(I_\ell, M_\ell(\varepsilon_{K,\ell}))\right\}.$$

Proposition 8. *Let $S = \{\ell \text{ place of } \mathbb{Q} : \ell | pD_K\infty\}$. Suppose the map*

$$\mathrm{res}_p : H^1_p(G_{\mathbb{Q},S}, M(\varepsilon_K)) \to H^1(\mathbb{Q}_p, M_p(\varepsilon_{K,p}))$$

were surjective. Then $\mathrm{Sel}_p^+(\phi_K) \twoheadrightarrow H^1_p(\mathbb{Q}, M)$.

Proof. The map $\mathrm{Sel}_p^+(\phi_K) \to H^1_p(\mathbb{Q}, M)$ is given by $(x,y)\mapsto x$ (under the coordinates given by $\mathrm{Sel}_p^+(\phi_K) \subset H^1(G_{\mathbb{Q},S}, M)\oplus H^1(G_{\mathbb{Q},S}, M(\varepsilon_K))$). Thus, if $\mathrm{res}_p : H^1_p(G_{\mathbb{Q},S}, M(\varepsilon_K)) \to H^1(\mathbb{Q}_p, M_p(\varepsilon_{K,p})) = H^1(\mathbb{Q}_p, M_p)$ were surjective, then for any $x \in H^1_p(\mathbb{Q}, M)$, there would exist $y \in H^1_p(G_{\mathbb{Q},S}, M(\varepsilon_K))$ such that $\mathrm{res}_p x = -\mathrm{res}_p y$. Thus we have found an element $(x,y)\in \mathrm{Sel}_p^+(\phi_K)$ which maps to x under $\mathrm{Sel}_p^+(\phi_K) \to H^1_p(\mathbb{Q}, M)$, and we are done. □

3. Proof of the Main Theorem

Lemma 9 (Key Lemma)**.** *Let $S = \{\ell \text{ place of } \mathbb{Q} : \ell | pD_K\infty\}$. The map*

$$\prod_{\ell\in S}\mathrm{res}_\ell : H^1(G_{\mathbb{Q},S}, M(\varepsilon_K)) \to \prod_{\ell\in S} H^1(\mathbb{Q}_\ell, M_\ell(\varepsilon_{K,\ell}))$$

is surjective. In particular, the map

$$\mathrm{res}_p : H^1_p(G_{\mathbb{Q},S}, M(\varepsilon_K)) = \ker\left(\prod_{\ell\in S,\ell\neq p}\mathrm{res}_\ell\right) \to H^1(\mathbb{Q}_p, M_p(\varepsilon_{K,p}))$$

is surjective.

Proof. By Tate global and local duality, we have an exact sequence

$$H^1(G_{\mathbb{Q},S}, M(\varepsilon_K)) \xrightarrow{\mathrm{res}_S := \prod_{\ell\in S}\mathrm{res}_\ell} \prod_{\ell\in S} H^1(\mathbb{Q}_\ell, M_\ell(\varepsilon_{K,\ell}))$$
$$\cong \prod_{\ell\in S} H^1(\mathbb{Q}_\ell, M_\ell(\varepsilon_{K,\ell})^*(1))^* \xrightarrow{\lambda_S^* := \prod_{\ell\in S}\lambda_\ell^*} H^1(G_{\mathbb{Q},S}, M(\varepsilon_K)^*(1))^*$$

where (1) denotes the Tate twist by $\chi_{\mathrm{cyc},p}$ and for $\ell \in S$, λ_ℓ^* is the dual of the natural restriction map

$$\lambda_\ell : H^1(G_{\mathbb{Q},S}, M(\varepsilon_K)^*(1)) \to H^1(\mathbb{Q}_\ell, M_\ell(\varepsilon_{K,\ell})^*(1)).$$

Our assertion that res_S is surjective is equivalent to the assertion $(\ker\lambda_S)^* = \mathrm{im}\,\lambda_S^* = \mathrm{coker}\,\mathrm{res}_S = 0$, which is equivalent to $\ker\lambda_S = 0$. (Note that $\ker\lambda_S$ itself defines a Selmer group attached to $M(\varepsilon_K)^*(1)$.) Observe that $M(\varepsilon_K)^*(1) = \mathbb{Z}_p[\phi][\![\Gamma]\!](\phi\varepsilon_K\chi_{\mathrm{cyc}})$, and so $M(\varepsilon_K)^*(1)/(\gamma-1)M(\varepsilon_K)^*(1) \cong \mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}})$ as $G_{\mathbb{Q},S}$-modules. Hence, from the associated long exact sequence of cohomology, we get an injection

$$H^1(G_{\mathbb{Q},S}, M(\varepsilon_K)^*(1))/(\gamma-1)H^1(G_{\mathbb{Q},S}, M(\varepsilon_K)^*(1)) \hookrightarrow H^1(G_{\mathbb{Q},S}, \mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}})).$$

From this, we get an injection

$$\ker\lambda_S/(\gamma-1)\ker\lambda_S \hookrightarrow \ker\{H^1(G_{\mathbb{Q},S}, \mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}})) \xrightarrow{\mathrm{res}_S} \prod_{\ell\in S} H^1(\mathbb{Q}_\ell, \mathbb{Z}_p[\phi](\phi_\ell\varepsilon_{K,\ell}\chi_{\mathrm{cyc},\ell}))\}$$
$$= \ker\{H^1(G_{\mathbb{Q},S}, \mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}})) \xrightarrow{\mathrm{res}_S} \prod_{\ell\in S} H^1(I_\ell, \mathbb{Z}_p[\phi](\phi_\ell\varepsilon_{K,\ell}\chi_{\mathrm{cyc},\ell}))\}$$

where the last equality follows because for $\ell \in S$,

$$H^1(\mathbb{Q}_\ell, \mathbb{Z}_p[\phi](\phi_\ell\varepsilon_{K,\ell}\chi_{\mathrm{cyc},\ell})) \hookrightarrow H^1(I_\ell, \mathbb{Z}_p[\phi](\phi_\ell\varepsilon_{K,\ell}\chi_{\mathrm{cyc},\ell}))$$

by the inflation-restriction exact sequence: for $\ell = p$, the kernel of inflation is zero since $\mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}})^{I_p} = 0$ since $\phi\varepsilon_K\chi_{\mathrm{cyc}}$ is ramified at p (which one sees because ϵ_K is unramiifed at p since p is split in K, and ϕ_p is of finite order and $\chi_{\mathrm{cyc},p}$ is of infinite order), and for $\ell \neq p$, this follows because $G_{\mathbb{F}_\ell}$ has profinite order prime to p so that $H^1(\mathbb{F}_\ell, \mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}})^{I_\ell}) = 0$.

We claim that

$$\mathrm{Sel}_S^+(\phi\varepsilon_K\chi_{\mathrm{cyc}}) := \ker\{H^1(G_{\mathbb{Q},S}, \mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}})) \xrightarrow{\mathrm{res}_S} \prod_{\ell\in S} H^1(I_\ell, \mathbb{Z}_p[\phi](\phi_\ell\varepsilon_{K,\ell}\chi_{\mathrm{cyc},\ell}))\}$$

is both torsion and torsion-free, and hence trivial. To show torsion-freeness, we show $H^1(G_{\mathbb{Q},S}, \mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}}))$ is torsion-free. Recall the short exact sequence of $G_{\mathbb{Q},S}$-modules

$$0 \to p\mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}}) \to \mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}}) \to \mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}})/p\mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}}) \to 0.$$

Taking the long exact sequence in group cohomology, we get a natural surjection

$$\mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}})^{G_{\mathbb{Q},S}}/p\mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}})^{G_{\mathbb{Q},S}} \twoheadrightarrow H^1(G_{\mathbb{Q},S}, \mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}}))[p].$$

Again using the fact that $G_{\mathbb{Q},S} \twoheadrightarrow \Gamma$ (as p is the only prime ramified in $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$), one can check that $\mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}})^{G_{\mathbb{Q},S}} = 0$. Thus $H^1(G_{\mathbb{Q},S}, \mathbb{Z}_p[\phi](\phi\varepsilon_K))[p] = 0$, and so the action by $\mathbb{Z}_p$ is torsion-free ($\mathbb{Z}_p^\times = \mathbb{Z}_p - p\mathbb{Z}_p$, so multiplication by anything not divisible by p is invertible, and hence has trivial kernel).

To show that $\mathrm{Sel}_S^+(\phi\varepsilon_K\chi_{\mathrm{cyc}})$ is torsion, note that since it is torsion-free, then

$$\begin{aligned}&\mathrm{Sel}_S^+(\phi\varepsilon_K\chi_{\mathrm{cyc}})\otimes_{\mathbb{Z}_p[\phi]}\mathbb{Q}_p[\phi]/\mathbb{Z}_p[\phi]\hookrightarrow\mathrm{Sel}_S(\phi\varepsilon_K\chi_{\mathrm{cyc}})\\&:=\ker\{H^1(G_{\mathbb{Q},S},\mathbb{Q}_p[\phi]/\mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}}))\xrightarrow{\mathrm{res}_S}\prod_{\ell\in S}H^1(I_\ell,\mathbb{Q}_p[\phi]/\mathbb{Z}_p[\phi](\phi_\ell\varepsilon_{K,\ell}\chi_{\mathrm{cyc},\ell}))\}.\end{aligned}$$

This latter group is in fact finite, which we see as follows. By Greenberg's functional equation of Selmer groups ([3, Theorem 2]), we have a pseudo-isomorphism $\sim$ (i.e. a Λ_ϕ-homomorphism with finite kernel and cokernel) of Λ_ϕ-modules $\mathrm{Sel}_S(\phi\varepsilon_K\chi_{\mathrm{cyc}})\sim\mathrm{Sel}_S(\phi^{-1}\varepsilon_K)^\iota$ where $\mathrm{Sel}_S(\phi^{-1}\varepsilon_K)$ is defined analogously to $\mathrm{Sel}_S(\phi\varepsilon_K\chi_{\mathrm{cyc}})$ above and the superscript ι denotes that Λ_ϕ acts through the involution $\iota:\Gamma\to\Gamma$, $\iota(\gamma)=\gamma^{-1}$. (In loc. cit., this is formulated by saying both Selmer groups have the same characteristic ideal.)

We will now show that $\mathrm{Sel}_S(\phi^{-1}\varepsilon_K)$ is finite. Let $\gamma\in\Gamma$ be a topological generator, so that we can write $\Lambda_\phi=\mathbb{Z}_p[\phi][\![\Gamma]\!]=\mathbb{Z}_p[\phi][\![\gamma-1]\!]$. Assume first that $\phi\neq1$, which is equivalent to ϕ being ramified at p since ϕ is only possibly ramified at p by assumption. By a standard Selmer group control theorem (see [9, Proposition 4.4], for example), we have, since $\phi_p^{-1}\varepsilon_{K,p}\neq1$ (ϕ is ramified and ε_K unramified at p),

$$\mathrm{Sel}_S(\phi^{-1}\varepsilon_K)\cong H^1_f(\mathbb{Q},\Lambda_\phi^*(\phi^{-1}\varepsilon_K))[\gamma-1].$$

By Iwasawa's theorem ([9, Proposition 4.8]), since $\phi^{-1}\varepsilon_K$ is odd, we have that the Pontryagin dual $X_f(\phi^{-1}\varepsilon_K)$ is a torsion Λ_ϕ-module. In particular,

$$(H^1_f(\mathbb{Q},\Lambda_\phi^*(\phi^{-1}\varepsilon_K))[\gamma-1])^*=X_f(\phi^{-1}\varepsilon_K)/(\gamma-1)X_f(\phi^{-1}\varepsilon_K)$$

which we will now show is finite. By the structure theorem of finitely-generated Λ_ϕ-modules,

$$X_f(\phi^{-1}\varepsilon_K)\sim\prod_{i=1}^r\Lambda_\phi/(f_i)$$

where $f_i\in\Lambda_\phi$, and in fact $f_i\neq0$ for all i since $X_f(\phi^{-1}\varepsilon_K)$ is a torsion Λ_ϕ-module. Now by the Weierstrass preparation theorem, we have that $f_i=\varpi^{r_i}f_{i,0}f_{i,1}$ where ϖ is a uniformizer of $\mathbb{Z}_p[\phi]$, $r_i\in\mathbb{Z}_{\geq0}$, $f_{i,0}\in\mathbb{Z}_p[\phi][\gamma-1]$ is "distinguished", i.e. a monic polynomial in the variable $\gamma-1$ such that each non-leading coefficient is a non-unit (i.e. divisible by ϖ), and $f_{i,1}\in\mathbb{Z}_p[\phi][\![\gamma-1]\!]^\times$. Thus, we see that each f_i is congruent to a *positive* power of ϖ modulo $(\gamma-1)$, and hence $X_f(\phi^{-1}\varepsilon_K)/(\gamma-1)X_f(\phi^{-1}\varepsilon_K)$ is finite. Hence, dualizing, we see that $H^1_f(\mathbb{Q},\Lambda_\phi^*(\phi^{-1}\varepsilon_K))[\gamma-1]$ is finite, as claimed.

Now assume that $\phi=1$. Since ε_K is odd and $p^2\nmid D_K$ (indeed $p\nmid D_K$), it is a consequence of the Main Theorem of Iwasawa Theory (see Corollary 10 of loc. cit.) that

$$\#\mathrm{Sel}_S(\varepsilon_K)=\#(\mathcal{C}\ell(\mathbb{Q}(\mu_{D_K})/\mathbb{Q})\otimes_{\mathbb{Z}}\mathbb{Z}_p)^{\varepsilon_K}$$

and so, in particular, is finite.

Thus we have shown that $\mathrm{Sel}_S^+(\phi\varepsilon_K\chi_{\mathrm{cyc}})=0$, and so $\ker\lambda_S=0$. By our initial discussion, we are done. □

Remark 10. To show that $\mathrm{Sel}_S(\phi^{-1}\varepsilon_K)$ is finite in the proof of Lemma 9, we could have used the following formula, which is an application of a more general result originally due to Wiles and Darmon-Diamond-Taylor (see [11], [2] or [1, Chapter IV, Theorem 2]) to show that $\mathrm{Sel}_S(\phi^{-1}\varepsilon_K)$ is finite. The proof again uses local and global duality, and was inspired

by the work of Greenberg. First, we recall the Selmer group defined by dual local conditions to those of $\mathrm{Sel}_S(\phi^{-1}\varepsilon_K)$:

$$T_S(\phi\varepsilon_K\chi_{\mathrm{cyc}}) := \ker\{H^1(G_{\mathbb{Q},S}, \mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}})) \xrightarrow{\prod_{\ell\in S}\mathrm{res}_\ell} H^1(I_\ell, \mathbb{Z}_p[\phi](\phi_\ell\varepsilon_{K,\ell}\chi_{\mathrm{cyc},\ell}))\}.$$

Proposition 11. *We have that* $\mathrm{Sel}_S(\phi^{-1}\varepsilon_K)$ *and* $T_S(\phi\varepsilon_K\chi_{\mathrm{cyc}})$ *are finite, and in fact*

$$\frac{\#\mathrm{Sel}_S(\phi^{-1}\varepsilon_K)}{\#T_S(\phi\varepsilon_K\chi_{\mathrm{cyc}})} = \frac{\#H^0(\mathbb{Q}, (\mathbb{Q}_p[\phi]/\mathbb{Z}_p[\phi])(\phi^{-1}\varepsilon_K))}{\#H^0(\mathbb{Q}, \mathbb{Z}_p[\phi](\phi\varepsilon_K\chi_{\mathrm{cyc}}))} \prod_{\ell\leq\infty} \frac{\#H^1(\mathbb{F}_\ell, (\mathbb{Q}_p[\phi]/\mathbb{Z}_p[\phi])(\phi^{-1}\varepsilon_K))}{\#H^0(\mathbb{Q}_\ell, (\mathbb{Q}_p[\phi]/\mathbb{Z}_p[\phi])(\phi^{-1}\varepsilon_K))}.$$

Finally, we have the following corollary of Proposition 8 and Lemma 9.

Corollary 12. *We have an exact sequence*

$$0 \to H^1_f(\mathbb{Q}, M(\varepsilon_K)) \to \mathrm{Sel}_p^+(\phi_K) \to H^1_p(\mathbb{Q}, M) \to 0.$$

Proof. This follows immediately from Lemma 9, (3) and Proposition 8. □

Proof of Theorem 1. By Corollary 12 and the discussion in Section 2.1, we get the factorization of ideals of $\Lambda^+_{K,\phi_K} = \Lambda_\phi$

$$\mathrm{char}_{\Lambda^+_{K,\phi_K}} X_p(\phi_K) = \mathrm{char}_{\Lambda_\phi} X_f(\phi\varepsilon_K)\mathrm{char}_{\Lambda_\phi} X_p(\phi)$$

which, by the Main Theorems of Iwasawa Theory over K and $\mathbb{Q}$, implies that

$$(\mathcal{L}_p^{\mathrm{Katz},+}(\phi_K^{-1})) = (\mathcal{L}_p(\phi^{-1}))(\mathcal{L}_p(\phi\chi_{\mathrm{cyc}}^{-1})^\iota)$$

and we are done. □

References

[1] G. Cornell, J. H. Silverman, G. Stevens, *Modular Forms and Fermat's Last Theorem*: Chapter IV Galois Cohomology by L. Washington, Springer-Verlag 1997, New York, pp. 101-120.

[2] H. Darmon, F. Diamond, R. Taylor, *Fermat's Last Theorem*, Duke Math. Journal 102 (2000), 413-499.

[3] R. Greenberg, *Iwasawa Theory for p-adic Representations*, Advanced Studies in Pure Mathematics, 17 (1989), p. 97-137.

[4] R. Greenber, *Iwasawa Theory and p-adic deformations of motives*, Motives (Seattle, WA, 1991), 193-223, Proc. Sympos. Pure Math., 55, Part 2, Amer. Math. Soc., Providence, RI, 1994.

[5] B. H. Gross, *On the factorization of p-adic L-series*, Invent. Math. 57 (1980), 83-95.

[6] N. Katz, *p-adic l-functions for CM fields*, Invent. Math. 49 (1978), no. 3, 199-297.

[7] B. Mazur, A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. 76 (2): 179-330, 1984.

[8] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1): 25-68, 1991.

[9] C. Skinner, *Galois Representations and Iwasawa Theory*, Clay Mathematics Proceedings, Volume 15, 2011.

[10] L. C. Washington, *Introduction to Cyclotomic fields*, Second Edition, Graduate texts in Mathematics, Springer-Verlag Inc., New York, 1997.

[11] A. Wiles, *Modular Forms and Fermat's Last Theorem*, Ann. of Math. 142 (1995), 443-551.

Department of Mathematics, Princeton University, Fine Hall, Washington Rd, Princeton, NJ 08544

E-mail address: dkriz@princeton.edu