On Free Resolutions of Iwasawa Modules

Alexandra Nichifor and Bharathwaj Palvannan

Received: November 13, 2018
Revised: December 8, 2018

Communicated by Otmar Venjakob

Abstract. Let Λ (isomorphic to $\mathbb{Z}_p[[T]]$) denote the usual Iwasawa algebra and G denote the Galois group of a finite Galois extension L/K of totally real fields. When the non-primitive Iwasawa module over the cyclotomic $\mathbb{Z}_p$-extension has a free resolution of length one over the group ring $\Lambda[G]$, we prove that the validity of the non-commutative Iwasawa main conjecture allows us to find a representative for the non-primitive p-adic L-function (which is an element of a K_1-group) in a maximal Λ-order. This integrality result involves a study of the Dieudonné determinant. Using a cohomolgoical criterion of Greenberg, we also deduce the precise conditions under which the non-primitive Iwasawa module has a free resolution of length one. As one application of the last result, we consider an elliptic curve over $\mathbb{Q}$ with a cyclic isogeny of degree p^2. We relate the characteristic ideal in the ring Λ of the Pontryagin dual of its non-primitive Selmer group to two characteristic ideals, viewed as elements of group rings over Λ, associated to two non-primitive classical Iwasawa modules.

2010 Mathematics Subject Classification: Primary 11R23; Secondary 11R34, 11S25
Keywords and Phrases: (Non-commutative) Iwasawa theory, Selmer groups, Galois cohomology

1 Introduction

Over the years, the Iwasawa main conjecture has been formulated in various setups and various guises. The underlying principle in each formulation has been to relate objects on the algebraic side to the objects on the analytic side. On the algebraic side of Iwasawa theory, one studies modules over Iwasawa

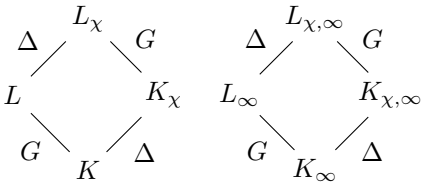
algebras. An Iwasawa algebra is a completed group ring $\mathbb{Z}_p[[\mathcal{G}]]$, for some p-adic Lie group $\mathcal{G}$. On the analytic side, one studies p-adic L-functions. The p-adic L-functions are believed to satisfy certain integrality properties. For example, consider the case when the group $\mathcal{G}$ is isomorphic to $\mathbb{Z}_p \times \Delta$, for some finite abelian group Δ. Under suitable conditions, the p-adic L-function is known to be a measure (not just a pseudo-measure). Our results in this paper are motivated by similar integrality properties of p-adic L-functions, in the non-commutative setting, as predicted by the non-commutative Iwasawa main conjectures.

Throughout this paper, fix p to be an odd prime. Let us first introduce all the notations that will be required to describe our results precisely. Let L/K be a finite Galois extension of totally real fields. Let $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathbb{F}_p^\times \hookrightarrow \mathbb{Z}_p^\times$ be a finite character that is either totally even or totally odd. For the sake of simplicity, we have chosen to work with a finite character χ taking values in $\mathbb{Z}_p^\times$. One could also consider a finite character taking values in an unramified extension of $\mathbb{Q}_p$. Our results would hold analogously.

We let K_χ denote the number field $\overline{\mathbb{Q}}^{\ker(\chi)}$. We let L_χ denote the compositum of L and K_χ. We let the fields K_∞, $K_{\chi,\infty}$, L_∞ and $L_{\chi,\infty}$ denote the cyclotomic $\mathbb{Z}_p$-extensions of K, K_χ, L and L_χ respectievly. Let $G := \mathrm{Gal}(L/K)$, $\Delta := \mathrm{Gal}(K_\chi/K)$ and $\Gamma := \mathrm{Gal}(K_\infty/K)$. Throughout this paper, we will impose the following condition:

$$K_\infty \cap L_\chi = K. \tag{1}$$

Condition (1) imposed above allows us to view χ naturally as a character of the groups $\mathrm{Gal}(K_\chi/K)$, $\mathrm{Gal}(L_\chi/L)$, $\mathrm{Gal}(K_{\chi,\infty}/K_\infty)$ and $\mathrm{Gal}(L_{\chi,\infty}/L_\infty)$ (and throughout this paper, we shall take this point of view). We have the following field diagrams and natural isomorphisms in mind:



We will consider the non-primitive classical Iwasawa module $\mathfrak{X}$ (defined in the next paragraph). Let Λ denote the completed group ring $\mathbb{Z}_p[[\Gamma]]$. Let $\Lambda[G]$ denote the group ring over Λ. In what follows, we will assume that all the $\Lambda[G]$-modules are left $\Lambda[G]$-modules with a left G-action. It turns out that $\mathfrak{X}$ is a finitely generated torsion module over $\Lambda[G]$. See [22, Proposition 1]. We refer the reader to this work of Greenberg to see how the Iwasawa module $\mathfrak{X}$ relates to Galois groups appearing in classical Iwasawa theory.

Let $\mathfrak{D}(\chi)$ equal $\frac{\mathbb{Q}_p(\chi)}{\mathbb{Z}_p(\chi)}$, that is, $\frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ with an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ via the character χ. Let us define the (non-primitive) Selmer group $\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}(L_\infty)$. The definition

of the Selmer group depends on the parity of χ. Let Σ denote a finite set of primes in K containing the primes above p, ∞, a finite prime number ν_0 not lying above p, and all the primes ramified in the extensions L/K and K_χ/K. For any algebraic extension F of K, we let $\Sigma_p(F)$ denote the set of all primes above p in F. We let Σ_0 equal the set $\Sigma \setminus \Sigma_p(K)$. We let K_Σ denote the maximal extension of K that is unramified outside Σ.

If the character χ is totally even, the Selmer group is defined as follows:

$$\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}(L_\infty) = H^1\left(\mathrm{Gal}(K_\Sigma/L_\infty), \mathfrak{D}(\chi)\right).$$

If the character χ is totally odd, the Selmer group is defined as follows:

$$\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}(L_\infty) = \ker\left(H^1\left(\mathrm{Gal}(K_\Sigma/L_\infty), \mathfrak{D}(\chi)\right) \xrightarrow{\phi^{\Sigma_0}_{\mathfrak{D}(\chi),\mathrm{odd}}} \prod_{\omega \in \Sigma_p(L_\infty),} H^1\left(I_\omega, \mathfrak{D}(\chi)\right)^{\Gamma_\omega} \right).$$

Here, I_ω denotes the inertia subgroup inside the decomposition group G_ω corresponding to the prime ω. We let Γ_ω denote the quotient group $\frac{G_\omega}{I_\omega}$. The map $\phi^{\Sigma_0}_{\mathfrak{D}(\chi),\mathrm{odd}}$ denotes the (natural) restriction map. Let $\mathfrak{X}$ denote the Pontryagin dual of $\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}(L_\infty)$. We will sometimes write $\mathfrak{X}_{\mathfrak{D}(\chi)}(L_\infty)$ when we want to emphasize the field L and the character χ.

Remark 1.1. We work with non-primitive Selmer groups since one can use Greenberg's results to show that the global-to-local map $\phi^{\Sigma_0}_{\mathfrak{D}(\chi),\mathrm{odd}}$ is surjective. We include the auxillary prime ν_0 not lying above p to ensure that we are working with Selmer groups that are genuinely non-primitive. When χ equals the Teichmüller character ω, the global-to-local map defining the primitive Selmer group is not surjective. See [20, Proposition 5.3.3] and the illustration that follows.

1.1 Integrality property for the non-primitive p-adic L-function

The main conjecture (Conjecture 3.2) allows us to deduce certain integrality properties for the non-primitive p-adic L-function ξ from the non-primitive Iwasawa module $\mathfrak{X}$. Let Q_Λ denote the fraction field of Λ. On the algebraic side, one considers an element in the relative K_0-group $K_0\left(\Lambda[G], Q_\Lambda[G]\right)$. On the analytic side, we have a non-primitive p-adic L-function ξ in $K_1\left(Q_\Lambda[G]\right)$. The interpolation properties of the p-adic L-function ξ are recalled in Section 3.1. Under the connecting homomorphism $\partial : K_1\left(Q_\Lambda[G]\right) \to K_0\left(\Lambda[G], Q_\Lambda[G]\right)$ in K-theory, the non-commutative Iwasawa main conjecture relates the non-primitive p-adic L-function ξ to the element on the algebraic side in the relative K_0-group. Works of Ritter-Weiss ([48]) and Kakde ([30]) independently

show that the non-commutative Iwasawa main conjecture holds when χ is totally even, assuming Iwasawa's $\mu = 0$ conjecture holds. Progress towards the Iwasawa main conjecture, without assuming the validity of Iwasawa's $\mu = 0$ conjecture, has been made in recent work of Johnston-Nickel [29].
The Artin-Wedderburn theorem gives us the following isomorphism:

$$Q_\Lambda[G] \cong \prod_i M_{m_i}(D_{\Lambda,i}), \tag{2}$$

where the $D_{\Lambda,i}$'s are division algebras, finite-dimensional over Q_Λ. One obtains the following sequence of isomorphisms:

$$K_1\left(Q_\Lambda[G]\right) \cong \prod_i K_1\left(M_{m_i}(D_{\Lambda,i})\right) \overset{\det}{\cong} \prod_i \left(M_{m_i}\left(D_{\Lambda,i}\right)^*\right)^{ab} \cong \left(Q_\Lambda[G]^*\right)^{\mathrm{ab}}. \tag{3}$$

Here, $\left(Q_\Lambda[G]^*\right)^{\mathrm{ab}}$ denotes the maximal abelian quotient of the multiplicative group of units in the ring $Q_\Lambda[G]$. The det in equation (3) refers to the Dieudonné determinant. Its definition is recalled in Section 2. One has a natural surjection $Q_\Lambda[G]^* \twoheadrightarrow K_1\left(Q_\Lambda[G]^*\right)$ of groups. One can ask the following question:

Question 1.2. *When χ is non-trivial, does ξ belong to the image of the following natural map of multiplicative monoids?*

$$\Lambda[G] \cap Q_\Lambda[G]^* \to K_1\left(Q_\Lambda[G]\right).$$

A similar question, pertaining to the integrality properties of p-adic L-functions, was raised in the five author paper [5]. See Conjecture 4.8 in [5]. In that paper, the authors considered p-adic L-functions associated to ordinary elliptic curves. Note that the formulation of Question 1.2 is stronger than Conjecture 4.8 in [5] as the authors of [5] state their conjecture assuming that the group G has no element of order p. One can also consider this question as a (non-commutative, non-primitive) refinement of the p-adic Artin conjecture of Greenberg [15].

Remark 1.3. In the setup of our theorems, the p-adic L-function (if it exists, as is conjectured) turns out to be unique. To see this, it suffices to show that the reduced Whitehead group $\mathrm{SK}_1\left(Q_\Lambda[G]\right)$ equals zero. This, in turn, reduces to showing that $\mathrm{SK}_1\left(D_{\Lambda,i}\right)$ equals zero for each of the division algebras $D_{\Lambda,i}$ appearing in equation (2). In Section 2.1, we show that each of these division algebras $D_{\Lambda,i}$ are of the form $D \otimes_{\mathbb{Q}_p} Q_\Lambda$, where D is a finite dimensional division algebra over $\mathbb{Q}_p$. A result of Nakayama-Matsushima [35] shows that for finite dimensional division algebras D over $\mathbb{Q}_p$, we have $\mathrm{SK}_1(D) = 0$. This result of Nakayama-Matsushima combined with the fact that Q_Λ is a purely transcendental extension of $\mathbb{Q}_p$ along with Platanov's Stability Theorem ([41, Page 315]) is then sufficient to show that $\mathrm{SK}_1\left(D_{\Lambda,i}\right)$ equals zero for each the division algebras $D_{\Lambda,i}$ appearing in equation (2).

Let $M_{\Lambda[G]}$ denote the maximal Λ-order inside $Q_\Lambda[G]$ containing $\Lambda[G]$ as defined in equation (27). Inside $Q_\Lambda[G]$, we have the inclusions

$$\Lambda[G] \subset M_{\Lambda[G]} \subset \frac{1}{|G|}\Lambda[G].$$

We prove the following partial result towards Question 1.2.

Theorem 1. *Suppose χ is non-trivial and Conjecture 3.2 holds. Suppose also that the $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one. Then, the non-primitive p-adic L-function ξ belongs to the image of the following natural map of multiplicative monoids:*

$$M_{\Lambda[G]} \cap Q_\Lambda[G]^* \to K_1\left(Q_\Lambda[G]\right).$$

Suppose χ is non-trivial and Conjecture 3.2 holds. When p does not divide the order of G, the $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one (see Remark 4.3) and the maximal Λ-order $M_{\Lambda[G]}$ coincides with $\Lambda[G]$. One has an affirmative answer to Question 1.2. When p divides the order of G, the maximal Λ-order $M_{\Lambda[G]}$ containing $\Lambda[G]$ does not coincide with $\Lambda[G]$. When G is abelian, Question 1.2 has an affirmative answer. In the commutative case, the question amounts to asking whether the non-primitive p-adic L-function is a measure (and not just a pseudo-measure). It is already known that the non-primitive (abelian) p-adic L-function is a measure, due to works of Barsky [2], Cassou-Noguès [4] and Deligne-Ribet [8]. These results in the commutative case served as an additional source of motivation for us to pursue this question in the non-commutative setting.

Remark 1.4. A variant of Conjecture 3.2 involving the maximal order $M_{Z(Q_\Lambda[G])}$ of the center $Z(Q_\Lambda[G])$ of $Q_{\Lambda[G]}$ is known. See work of Johnston-Nickel [29, Theorem 4.9] or Ritter-Weiss [47, Theorem 16 and Remark (H)] for the exact statement. In light of those results, it may be helpful to remark that the conclusion of Theorem 1 would follow without requiring the validity of Conjecture 3.2 if the reduced norm $\mathrm{Nrd} : M^\times_{\Lambda[G]} \to M^\times_{Z(Q_\Lambda[G])}$ is surjective. Since p is odd, the extension $Q_\Lambda[G] \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(\mu_p)$ is a product of matrix rings over commutative fields. See [40, Theorem 1.10(ii)]. One way to bypass requiring the validity of Conjecture 3.2 in Theorem 1 then is to simply work with the pair $\left(\Lambda[G] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mu_p],\ Q_\Lambda[G] \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(\mu_p)\right)$ instead of the pair $(\Lambda[G], Q_\Lambda[G])$.

1.2 Free resolutions of length one over $\Lambda[G]$

One can ask when the $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one. Over the integral group ring $\Lambda[G]$, the situation is much easier to handle when the order of G is co-prime to p. See Remark 4.3. When p does not divide $|G|$, the global dimension of the ring $\Lambda[G]$ equals two; in this case the $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one. The situation is more complicated when

there exists an element of order p in G since the ring $\Lambda[G]$ would then have infinite global dimension; in this case it is possible for $\Lambda[G]$-modules to have no non-trivial pseudo-null submodules and yet have infinite projective dimension over $\Lambda[G]$. The purpose of Theorems 2 and 3 is to precisely circumvent these difficulties.

Theorem 2. *Suppose χ is totally even. Suppose p divides $|G|$. The $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one if and only if χ is non-trivial.*

Theorem 3. *Suppose χ is totally odd. Suppose p divides $|G|$. The $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one if and only if one of the two following conditions holds for every prime $\omega \in \Sigma_p(L_\infty)$:*

(I) $H^0\left(G_\omega, \mathfrak{D}(\chi)\right) = 0$

(II) ω is tamely ramified in the extension L_∞/K_∞.

In the first author's thesis [37] in 2004, Theorems 2 and 3 were proved in the case when G is a cyclic p-group using a formula of Kida ([31]) and assuming the validity of Iwasawa's $\mu = 0$ conjecture. The results in this paper are a natural generalization of the results of [37], though the methods in this paper are significantly different. We use a cohomological criterion developed by Greenberg in [21]. This allows us to prove our results, without having to assume the validity of Iwasawa's $\mu = 0$ conjecture. See Proposition 3.1.1 in [21] for similar results concerning the Pontryagin duals of Selmer groups associated to elliptic curves. Much of our motivation towards this paper stems from this work of Greenberg. Nickel has shown that when the character χ is odd and when all the primes ω in $\Sigma_p(L_\infty)$ are *almost tame*, then the $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one. The condition that a prime ω in $\Sigma_p(L_\infty)$ is *almost tame* is related to Condition II in Theorem 3 and the image of complex conjugation in the decomposition group corresponding to ω. See Proposition 4.1 in [39] and Proposition 7 in [38]. Theorem 2 can also be deduced from the machinery of Selmer complexes appearing in the work of Fukaya and Kato [12], as we indicate in Section 3. For Theorem 2, one can also use results from the work of Ritter and Weiss [46, 47]. See also Chapter 5 of Witte's habilitation thesis [53].

Remark 1.5. In light of results of Nickel [38, 39] and Ritter-Weiss [46, 47], Theorems 2 and 3 are not essentially new. However, one of our main objectives in this paper is to initiate an approach towards studying integrality properties of p-adic L-functions (as in Question 1.2) in general situations using Greenberg's cohomological criterion ([21, Proposition 2.4.1]) and the Dieudonné determinant. Greenberg's cohomological criterion is valid over general 1-dimensional p-adic Lie groups. Our approach via the theory of Dieudonné determinant may be of independent interest from the perspective of non-commutative algebra. In the non-commutative setting, the study of the Dieudonné determinant seems a rather subtle question to us. See Examples 2.1, 2.3, 2.6 and 2.7 in Section 2.

These examples suggest establishing, that the non-primitive Iwasawa module has a free resolution of length 1, alone may not be sufficient to provide an affirmative answer towards Question 1.2 (whenever it does have an affirmative answer).

1.3 Elliptic curves with a cyclic p^2 isogeny

We will now consider applications of Theorems 2 and 3 to a setting involving an elliptic curve defined over $\mathbb{Q}$ with a cyclic p^2 isogeny. Our main theorem (Theorem 4) in this setting is a generalization of a result that appears implicitly in the work of Greenberg and Vatsal [24]. For a generalization of this work of Greenberg and Vatsal in another direction, see work of Hirano [26].

Let E be an elliptic curve defined over $\mathbb{Q}$ with good ordinary or split multiplicative reduction at p. Let $\Phi : E \to E'$ be a cyclic isogeny over $\mathbb{Q}$ of degree p^2. Let $\tilde{\Phi} : E' \to E$ be the dual isogeny. We shall suppose that the Galois action on the kernel of the isogeny Φ is even. We will first state the theorem in this setting before explaining the notations.

Theorem 4. *Suppose the even character χ_ϕ is ramified at p. Suppose the condition (Non-DG) holds. We have the following equality of ideals in $\frac{\Lambda}{(p^2)}$:*

$$\sigma_{p^2}\left(\mathrm{Char}_\Lambda\left(\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee\right)\right) = \sigma_\phi\left(\left(\det\left(A_\phi\right)\right)\right)\sigma_{\tilde{\phi}}\left(\left(\det\left(A_{\tilde{\phi}}\right)\right)\right). \quad (4)$$

The non-primitive Selmer group $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)$ associated to E is defined in the work of Greenberg and Vatsal [24]. The characteristic ideal of the Λ-module $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee$ is denoted by $\mathrm{Char}_\Lambda\left(\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee\right)$. We will need to consider the natural map $\sigma_{p^2} : \Lambda \to \frac{\Lambda}{(p^2)}$. Here, G_ϕ and $G_{\tilde{\phi}}$ are abelian Galois groups, of order dividing p, of Galois extensions $L_\phi/\mathbb{Q}$ and $L_{\tilde{\phi}}/\mathbb{Q}$ respectively. These fields are "cut out", in a certain sense, by the cyclic isogenies Φ and $\tilde{\Phi}$. We will need to impose the condition that $L_\phi \cap \mathbb{Q}_\infty = \mathbb{Q}$, similar to the condition given in (1). This condition is labeled (Non-DG). See Section 5 for the precise definitions of the various objects along with the description of the ring homomorphisms $\sigma_\phi : \Lambda[G_\phi] \to \frac{\Lambda}{(p^2)}$ and $\sigma_{\tilde{\phi}} : \Lambda[G_{\tilde{\phi}}] \to \frac{\Lambda}{(p^2)}$ given in (54). The Galois action on $\ker(\Phi)[p]$ is given the character χ_ϕ. In this setup, as we shall see in Section 5, Theorems 2 and 3 will allow us to consider two non-primitive Iwasawa modules that have free resolutions of length one over $\Lambda[G_\phi]$ and $\Lambda[G_{\tilde{\phi}}]$ respectively. These free resolutions of length one will naturally lead us to consider two square matrices A_ϕ and $A_{\tilde{\phi}}$ in group rings $\Lambda[G_\phi]$ and $\Lambda[G_{\tilde{\phi}}]$ respectively. See equation (55).

Remark 1.6. For the purposes of indentation in this manuscript, a short exact sequence $0 \to A \to B \to C \to 0$ is also denoted by $A \hookrightarrow B \twoheadrightarrow C$.

2 Dieudonné determinant

To answer Question 1.2, that deals with the integrality properties of non-primitive p-adic L-functions, we will need to develop some preliminaries on the Dieudonné determinant. We shall follow some of the terminology introduced in Lam's book on non-commutative rings [32]. In our discussions, the rings will always be associative rings with a unity. The units of a ring T, denoted by T^*, will consist of elements that have both a left and a right inverse. We will say that a ring T is Noetherian if it is both left and right Noetherian. We will say that a Noetherian ring T is a local ring if it has a unique maximal left ideal $\mathfrak{m}_T$ (this ideal $\mathfrak{m}_T$ turns out to be the unique maximal right ideal).

We will say that a Noetherian ring T is a semi-local ring if the quotient ring $\frac{T}{\mathrm{Jac}(T)}$ is semisimple. Here, $\mathrm{Jac}(T)$ is the Jacobson radical of T (which is a two-sided ideal in T). Let T be a semi-local ring. We recall three properties associated to it:

1. The matrix ring $M_n(T)$ is a semi-local ring with Jacobson radical equal to $M_n\left(\mathrm{Jac}(T)\right)$. See 20.4 in Lam's book [32].

2. A semi-local ring is Dedekind-finite. That is, whenever an element u is right-invertible, then u is left-invertible (or equivalently, whenever an element u is left-invertible, then u is right-invertible). See Proposition 20.8 in Lams' book [32].

3. A matrix A in $M_n(T)$ is invertible if and only if it becomes invertible in $M_n\left(\frac{T}{\mathrm{Jac}(T)}\right)$. See Theorem 1.11 in Oliver's book [40]. In particular, an element u in T is invertible if and only if its image in the quotient ring $\frac{T}{\mathrm{Jac}(T)}$ is invertible.

For each integer $n \geq 1$, one can consider the inclusions $\mathrm{GL}_n(T) \hookrightarrow \mathrm{GL}_{n+1}(T)$ via the map $g \to \begin{pmatrix} g & 0 \\ 0 & 1 \end{pmatrix}$. Let $\mathrm{GL}_\infty\left(T\right)$ equal $\bigcup_{n \geq 0} \mathrm{GL}_n\left(T\right)$. The group $K_1(T)$ is defined below:

$$K_1\left(T\right) := \frac{\mathrm{GL}_\infty(T)}{[\mathrm{GL}_\infty(T), \mathrm{GL}_\infty(T)]}.$$

Here, $[\mathrm{GL}_\infty(T), \mathrm{GL}_\infty(T)]$ is the commutator subgroup of $\mathrm{GL}_\infty(T)$. We will need to consider a subgroup $W(T)$, of the multiplicative group T^*, generated by elements of the form $(1+rs)(1+sr)^{-1}$, whenever $1+rs$ is a unit in the ring T. Here, r, s are elements of the ring T. The group $W(T)$ contains the commutator subgroup $[T^*, T^*]$. One has a natural "determinant" map, often called the Dieudonné or Whitehead determinant. See Example 1.3.7 and

Exercise 1.2, both in Chapter III of Weibel's K-book [52] for more details. The Dieudonné determinant is the unique group homomorphism:

$$\det : K_1(T) \to \frac{T^*}{W(T)},$$

characterized by the following properties:

1. If A is an elementary $n \times n$ matrix, then $\det(A) = 1$. We say that an $n \times n$ matrix $A = (a_{ij})$ is elementary if there exists distinct indices r, s $(r \neq s)$ and an element λ in T such that $a_{ij} = \begin{cases} 1, & \text{if } i = j, \\ \lambda, & \text{if } i = r,\ j = s, \\ 0 & \text{otherwise.} \end{cases}$
2. If $\operatorname{diag}(t) = \begin{pmatrix} t & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ and g belong to $\mathrm{GL}_n(T)$, then $\det\big(\operatorname{diag}(t)g\big) = t \det(g)$.

In fact, Vaserstein [49] has shown that the Dieudonné determinant is an isomorphism. One can use these properties of the Dieudonné determinant to deduce the following additional properties:

3. If A is a permutation matrix, then $\det(A)$ is a unit in T (since $\det(A)^2 = 1$). We say that the matrix $A = (a_{ij})$ is a permutation matrix if there exists distinct indices r, s $(r \neq s)$ such that $a_{ij} = \begin{cases} 1, & \text{if } i = j \neq r,\ i = j \neq s \\ 1 & \text{if } i = r,\ j = s, \\ 1 & \text{if } i = s,\ j = r, \\ 0 & \text{otherwise.} \end{cases}$
4. If A is a triangular matrix in $\mathrm{GL}_n(T)$, then $\det(A) = \prod_i a_{ii}$ in $K_1(T)$, where a_{ii}'s are the entries on the main diagonal of A.

We will consider the following property for the semi-local ring T:

(**WP**) $\frac{T}{\mathrm{Jac}(T)}$ is a product of matrix rings, none of which is $M_2(\mathbb{F}_2)$ and at most one of these factors is $\mathbb{F}_2$.

Note that if 2 is invertible in T, then the property (**WP**) holds. Vaserstein [49] has shown that for a semi-local ring, if property (**WP**) holds, then we have the following natural isomorphism of abelian groups

$$\frac{T^*}{W(T)} \cong (T^*)^{ab}.$$

Here, $(T^*)^{ab}$ denotes the abelianization of the unit group T^*. To provide an illustration, consider a 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in $\mathrm{GL}_2(T)$. Also, assume that the element a is invertible in T. Then, using properties of determinants described above, one can show that

$$\begin{aligned} \det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) &= \det\left(\begin{bmatrix} 1 & 0 \\ ca^{-1} & 1 \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & d-ca^{-1}b \end{bmatrix}\begin{bmatrix} 1 & a^{-1}b \\ 0 & 1 \end{bmatrix}\right) \\ &= [ad - aca^{-1}b] \in (T^*)^{\mathrm{ab}}\,. \end{aligned} \tag{5}$$

EXAMPLE 2.1. Let $\mathbb{H}$ be the quaternion division algebra over the real numbers $\mathbb{R}$. Note that $\mathbb{H}$ is a 4-dimensional vector space over $\mathbb{R}$ generated by 1, i, j and k satisfying the usual properties:

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k, \qquad jk = -kj = i, \qquad ki = -ik = j.$$

Consider the following example of an invertible 2×2 matrix in $\mathrm{GL}_2(\mathbb{H})$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} i & j \\ j & i \end{bmatrix}, \qquad \begin{bmatrix} i & j \\ j & i \end{bmatrix}\begin{bmatrix} i & j \\ j & i \end{bmatrix} = \begin{bmatrix} -2 & 0 \\ 0 & -2 \end{bmatrix},$$
$$ad - aca^{-1}b = -2, \qquad ad - bc = da - bc = ad - cb = da - cb = 0.$$

The example above shows that $\det(A)$, in general, is not uniformly represented by $ad - bc$ or $da - bc$ or $ad - cb$ or $da - cb$. Nevertheless, one may still ask the following question:

QUESTION 2.2. *Let T be a semi-local ring satisfying* (**WP**). *Let $R \hookrightarrow T$ be a subring. Suppose the $n \times n$ matrix A belongs to $M_n(R) \cap \mathrm{GL}_n(T)$. Does* $\det(A)$ *lie in the image of the natural map*

$$i : R \cap T^* \to (T^*)^{ab},$$

of multiplicative monoids?

When T is commutative, Question 2.2 has an affirmative answer. However, considering the level of generality at which it is phrased, Question 2.2 has a negative answer. Consider the following example described in Problem 3 in Section 7.10 of Cohn's book [6].

EXAMPLE 2.3. Let k be a field such that $\mathrm{Char}(k) \neq 2$. Let $R = k < x, y, z, t >$ be the free (non-commutative) algebra in 4 indeterminates. Let U_R denote its universal skewfield of fractions. See Section 7.2 in [6] for the definition of universal skewfield of fractions and the properties that this skewfield U_R satisfies. See Corollary 2.5.5 and Corollary 7.5.14 in [6], as to why this ring R has a universal skewfield of fractions. For our purposes, we will simply keep in mind that U_R is not obtained via the Ore localization of R at the multiplicatively closed set $R \setminus \{0\}$. Let A be the 2×2 matrix $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$

in $M_2(R) \cap \mathrm{GL}_2(U_R)$. In this case, $\det(A) = \left[x\left(t - zx^{-1}y\right)\right]$ inside $(U_R^*)^{\mathrm{ab}}$. However, this element of $(U_R^*)^{\mathrm{ab}}$ has no representative in R. □

For our purposes, we would like to refine Question 2.2 so that the refined question may have an affirmative answer. We will follow some of the terminology given in the book of Goodearl and Warfield [13]. Let S be a multiplicatively closed set in a ring R. The set S is called a left-reversible left-Ore set if it satisfies the following two conditions:

1. (left cancellation) If $ns = ms$, for some n, m in R and some s in S, then there exists s' in S such that $s'n = s'm$.

2. (left Ore condition) For every $r \in R$ and $s \in S$, there exists $r' \in R$, $s' \in S$ so that $s'r = r's$.

One can similarly define a right-reversible right-Ore set. A multiplicatively closed set S will be called an Ore set if it is both a left-reversible left-Ore set and a right-reversible right-Ore set. If S is an Ore set in a ring R, it will be possible to consider the localization R_S. The set S is also often called a denominator set and the ring R_S is often called the Ore localization of R at S. See Chapter 9 in the book of Goodearl and Warfield [13], especially Theorem 9.7 and Proposition 9.8 there. We ask the following variant of Question 2.2.

Question 2.4. *Let S be an Ore set in a semi-local ring R, so that the localization R_S is also a semi-local ring. Suppose R_S satisfies* **(WP)**. *Let A be a matrix that belongs to $M_n(R) \cap \mathrm{GL}_n(R_S)$. When does* $\det(A)$ *lie in the image of the natural map*

$$i : R \cap R_S^* \to (R_S^*)^{ab}.$$

of multiplicative monoids?

To introduce one piece of terminology, we will follow the notations of Question 2.4. We will say that Question 2.4 has a positive answer for the pair (R, R_S) if the following statement is true:

$$\forall n \geq 0, \forall A \in M_n(R) \cap \mathrm{GL}_n(R_S) \implies \det(A) \in i\left(R \cap R_S^*\right) \subset (R_S^*)^{ab}.$$

Otherwise, we will say that Question 2.4 has a negative answer for (R, R_S).

To introduce another piece of terminology, we will say that a matrix A in $M_n(T)$ admits a *diagonal reduction via elementary operations*, if there exists matrices U and V in $\mathrm{GL}_n(T)$, and a diagonal matrix B in $M_n(T)$, so that

1. $A = UBV$,

2. The matrices U and V are obtained as products of matrices of the following kinds:

- elementary matrices,
- permutation matrices,
- scalar matrices in $\mathrm{GL}_n(T)$.

We recall the definition of a principal ideal domain in the non-commutative setting given in Jacobson's book [28]. A (not necessarily commutative) domain is said to be a principal left ideal domain if every left ideal is principal. A domain is said to be a principal right ideal domain if every right ideal is principal. A domain is said to be a principal ideal domain if it is both a principal left ideal domain and a principal right ideal domain.

PROPOSITION 2.5 (Theorem 16, Chapter 3 in [28]). *Let T be a principal ideal domain. Every matrix A in $M_n(T)$ admits a diagonal reduction via elementary operations.*

Let O be a complete discrete valuation ring, whose fraction field is denoted by K. Let D be a division algebra whose center contains K and such that the index $[D : K]$ is finite. Let O_D be the maximal O-order inside D. In this case, O_D is a (non-commutative) principal ideal domain. See Theorem 13.2 in Reiner's book on Maximal orders [43] where it is established that O_D is a principal ideal domain. Every $n \times n$ matrix with entries in O_D admits a diagonal reduction via elementary operations. See also Theorem 17.7 in [43] for this fact. In this case, Question 2.4 has a positive answer for the pair (O_D, D).

Unfortunately, we will not be able to classify the tuples (R, R_S) for which Question 2.4 has a positive answer. Nevertheless, we will provide one example (Example 2.6) when Question 2.4 has a positive answer and one example (Example 2.7) when Question 2.4 has a negative answer.

EXAMPLE 2.6. Let p be an odd prime. In this example, we shall show that Question 2.4 has a positive answer for the pair $(\mathbb{Z}_p[D_{2p}], \mathbb{Q}_p[D_{2p}])$. Let D_{2p} be the dihedral group of order $2p$ which has the following presentation

$$D_{2p} = \{x, y | x^2 = y^p = 1,\ xyx^{-1} = y^{-1}\}.$$

Note that since p is odd, the ring $\mathbb{Z}_p[D_{2p}]$ satisfies **(WP)**.
Let $L = \mathbb{Q}_p(\zeta_p)$. Let $F = \mathbb{Q}_p(\zeta_p + \zeta_p^{-1})$. Here, we let ζ_p denote a primitive p-th root of unity. The Galois group $\mathrm{Gal}(L/F)$ is of order two. Let α denote the non-trivial element in $\mathrm{Gal}(L/F)$. Let O_L and O_F denote the ring of integers in L and F respectively. Let $\mathfrak{p}_L$ and $\mathfrak{p}_F$ denote the unique prime lying above p in O_L and O_F respectively. We have the following equality:

$$\mathfrak{p}_L = (1 - \zeta_p) \text{ as ideals in } O_L, \qquad \mathfrak{p}_F = (2 - \zeta_p - \zeta_p^{-1}) \text{ as ideals in } O_F.$$

Since the field extensions $L/\mathbb{Q}_p$ and $F/\mathbb{Q}_p$ are totally ramified, we have the following natural isomorphisms of residue fields:

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \xhookrightarrow{\cong} \frac{O_F}{\mathfrak{p}_F} \xhookrightarrow{\cong} \frac{O_L}{\mathfrak{p}_L}. \tag{6}$$

Note that the Artin-Wedderburn theorem gives us an isomorphism of $\mathbb{Q}_p$-algebras:

$$\mathbb{Q}_p[D_{2p}] \cong \mathbb{Q}_p[C_2] \times L < \tau > . \tag{7}$$

Here, C_2 is a cyclic group of order 2 with generator e. The central simple F-algebra $L < \tau >$ is given by $L \oplus L \cdot \tau$, where we have $\tau^2 = 1$ and $\tau a = \alpha(a)\tau$, for all $a \in L$. The center of $L < \tau >$ equals F. Note that since $(\tau - 1)(\tau + 1) = 0$, the simple algebra $L < \tau >$ cannot be a division algebra. Also, $\dim_F L < \tau >= 4$. By a simple dimension counting argument and the Artin-Wedderburn theorem, one can see that we have the isomorphism $L < \tau > \cong M_2(F)$ of F-algebras. However, it will be convenient to view $L < \tau >$ naturally inside $L < \tau > \otimes_F L$ since this allows us to consider the isomorphism $L < \tau > \otimes_F L \cong M_2(L)$. One can obtain such an isomorphism by considering the following assignments:

$$\zeta_p \to \begin{bmatrix} \zeta_p & 0 \\ 0 & \zeta_p^{-1} \end{bmatrix}, \quad \tau \to \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{8}$$

The isomorphism in (7) is chosen to agree with the following two projection maps:

$$\begin{aligned} &\sigma_1 : \mathbb{Q}_p[D_{2p}] \to \mathbb{Q}_p[C_2], && \sigma_2 : \mathbb{Q}_p[D_{2p}] \to L < \tau > . \\ &\sigma_1(x) = e,\ \sigma_1(y) = 1 && \sigma_2(x) = \tau,\ \sigma_2(y) = \zeta_p. \end{aligned}$$

Let n denote a positive integer. Let us label det, $\det_1$ and $\det_2$ for the Dieudonné determinants involving the invertible matrices in $\mathrm{GL}_n(\mathbb{Q}_p[D_{2p}])$, $\mathrm{GL}_n(\mathbb{Q}_p[C_2])$ and $\mathrm{GL}_n(L < \tau >)$ respectively. Note that the reduced norm $\mathrm{Nrd} : L < \tau >^* \to F^*$ is given by the formula $\mathrm{Nrd}(c + d\tau) = c\alpha(c) - d\alpha(d)$. The reduced norm gives us an isomorphism $\mathrm{Nrd} : (L < \tau >^*)^{ab} \xrightarrow{\cong} F^*$. See Theorem 2.3 in Oliver's book [40]. We have the following diagram relating these Dieudonné determinants:

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{Q}_p[D_{2p}]) & \xrightarrow{\cong} & \mathrm{GL}_n(\mathbb{Q}_p[C_2]) \times \mathrm{GL}_n(L < \tau >) \\ & \searrow^{\det} & \downarrow{\scriptstyle (\det_1, \det_2)} \\ & & \mathbb{Q}_p[C_2]^* \times (L < \tau >^*)^{ab} \xrightarrow[\cong]{\mathrm{Nrd}} \mathbb{Q}_p[C_2]^* \times F^* \end{array}$$

We will follow the description of the integral group ring $\mathbb{Z}_p[D_{2p}]$, i.e. its image under the isomorphism (7), given in Section 8 of the work of Reiner and Ullom [44]. Let $O_{L<\tau>}$ denote the subring $O_L \oplus O_L \cdot \tau$ of the central simple F-algebra $L < \tau >$. This is a maximal $\mathbb{Z}_p$-order inside $L < \tau >$. Under the isomorphism (7), we have

$$\begin{aligned} \mathbb{Z}_p[D_{2p}] \cong \big\{ (a + be, c + d\tau) \in \mathbb{Z}_p[C_2] \times O_{L<\tau>} \text{ such that} \\ a \equiv c \pmod{\mathfrak{p}_L}, \quad b \equiv d \pmod{\mathfrak{p}_L} \big\}. \end{aligned}$$

The ring $\mathbb{Z}_p[D_{2p}]$ is a semi-local ring whose Jacobson radical is given below:

$$\mathrm{Jac}(\mathbb{Z}_p[D_{2p}]) = \ker\left(\mathbb{Z}_p[D_{2p}] \to \mathbb{F}_p[C_2]\right).$$

Let $\mathfrak{m}$ denote the ideal $(p, y-1, x-1)$ and let $\mathfrak{m}'$ denote the ideal $(p, y-1, x+1)$ in $\mathbb{Z}_p[D_{2p}]$. The ideals $\mathfrak{m}$ and $\mathfrak{m}'$ are both left-maximal and right-maximal ideals. An element u in $\mathbb{Z}_p[D_{2p}]$, that does not belong to both $\mathfrak{m}$ and $\mathfrak{m}'$, must be a unit in the ring $\mathbb{Z}_p[D_{2p}]$. See Theorem 1.11 in Oliver's book [40].
The description of the Jacboson radical of $\mathbb{Z}_p[C_2]$ is given below:

$$\mathrm{Jac}(\mathbb{Z}_p[C_2]) = \{a + be \in \mathbb{Z}_p[C_2], \text{ such that } a \in p\mathbb{Z}_p,\ b \in p\mathbb{Z}_p\}.$$

We would like to record three observations.

1. Suppose we are given an element $a + be \in \mathrm{Jac}(\mathbb{Z}_p[C_2])$, where $a, b \in p\mathbb{Z}_p$. Suppose also that we are given an element ϖ in the maximal ideal $\mathfrak{p}_F$ of the ring O_F. It will be possible to write ϖ as $(2 - \zeta_p - \zeta_p^{-1})^n v$ for some positive integer n and some unit v of the ring O_F. It is easy to see that $\mathrm{Nrd}(1 - \zeta_p) = 2 - \zeta_p - \zeta_p^{-1}$. Also, the restriction of the reduced norm $\mathrm{Nrd} : O^\times_{L<\tau>} \twoheadrightarrow O_F^\times$ is surjective on the units. See Theorem 2.3 in Oliver's book [40]. This lets us find a unit u in the ring $O_{L<\tau>}$ such that $\mathrm{Nrd}(u) = v$. Our observations allow us to make the following deduction:

$$\epsilon = \Big(a + be,\ (1 - \zeta_p)^n u\Big) \in \mathbb{Z}_p[D_{2p}], \qquad \mathrm{Nrd}\big((1 - \zeta_p)^n u\big) = \varpi. \tag{9}$$

2. Suppose now we are given an element $a + be \in \mathbb{Z}_p[C_2]$ such that (i) both a and b belong to $\mathbb{Z}_p^\times$ and such that (ii) $a - b \equiv 0 \pmod p$ or $a + b \equiv 0 \pmod p$. Suppose also that we are given an element ϖ in the maximal ideal $\mathfrak{p}_F$ of the ring O_F. The restriction of the reduced norm map $\mathrm{Nrd} : 1 + \mathfrak{p}_L \twoheadrightarrow 1 + \mathfrak{p}_F$ is surjective. See Chapter 1, Section 8, Proposition 2 of Fröhlich's article on local fields [11] as to why the reduced norm map is surjective on the group of principal units for tamely ramified extensions. So, it will be possible to find an element $u_1 \in 1 + \mathfrak{p}_L$ such that $\mathrm{Nrd}(u_1) = 1 + \frac{\varpi}{a^2}$. Set

$$z = \begin{cases} au_1 + a\tau, & \text{if } a - b \equiv 0 \pmod p \\ au_1 - a\tau, & \text{if } a + b \equiv 0 \pmod p \end{cases}$$

   It is then straightforward to check that

$$\epsilon = \Big(a + be,\ z\Big) \in \mathbb{Z}_p[D_{2p}], \qquad \mathrm{Nrd}\,(z) = \varpi. \tag{10}$$

3. Suppose we have two elements a and a' in the ring $\mathbb{Z}_p[D_{2p}]$ such that

$$a \notin \mathfrak{m}, \qquad a \in \mathfrak{m}',$$
$$a' \in \mathfrak{m}, \qquad a' \notin \mathfrak{m}'.$$

Then, $a + a' \notin \mathfrak{m}$ and $a + a' \notin \mathfrak{m}'$. In particular, $a + a'$ is a unit in the ring $\mathbb{Z}_p[D_{2p}]$.

Let $A \in M_n(\mathbb{Z}_p[D_{2p}]) \cap \mathrm{GL}_n(\mathbb{Z}_p[D_{2p}])$. We shall show that we can find a representative for $\det(A)$ in $M_n(\mathbb{Z}_p[D_{2p}])$.

First, we will consider the case when A belongs to $M_n(\mathfrak{m}\mathbb{Z}_p[D_{2p}])$ or $M_n(\mathfrak{m}'\mathbb{Z}_p[D_{2p}])$. Without loss of generality, we shall assume that A belongs to $M_n(\mathfrak{m}'\mathbb{Z}_p[D_{2p}])$. The argument proceeds similarly when A belongs to $M_n(\mathfrak{m}\mathbb{Z}_p[D_{2p}])$. Note that the ring $\mathbb{Q}_p[C_2]$ is commutative. The matrix $\sigma_1(A)$ is an $n \times n$ matrix with entries in $\mathbb{Z}_p[C_2]$. Let us write $\det_1(\sigma_1(A))$ as $a + be$. Since we have assumed that A belongs to $M_n(\mathfrak{m}'\mathbb{Z}_p[D_{2p}])$, every entry in the matrix $\sigma_1(A)$ must belong to ideal $(p, e + 1)$. So, p must divide $a - b$. As a result, one sees that in this first case, we have

$$(1)\ a + be \in \mathrm{Jac}(\mathbb{Z}_p[C_2]),\ \text{or} \qquad (2)\ a, b \in \mathbb{Z}_p^{\times} \text{ such that } a - b \equiv 0 \bmod p.$$

The matrix $\sigma_2(A)$ is an $n \times n$ matrix with entries in $O_{L<\tau>}$. One can check that the (i, j)-th entry of $\sigma_2(A)$ can be written as $a_{ij}(\tau+1)+b_{ij}p+c_{ij}(\zeta_p-1)$, for some elements a_{ij}, b_{ij} and c_{ij} in $O_{L<\tau>}$. We will use the assignments given in (8) to fix an embedding $\mathfrak{i} : L < \tau > \hookrightarrow M_2(L)$. It will be possible to view the matrix $\mathfrak{i}(\sigma_2(A))$ as a matrix in $M_{2n}(O_L)$. Note that $\zeta_p - 1$ and p belong to the ideal $\mathfrak{p}_L O_L$. The assignment given in (8) sends $\tau + 1$ to the 2×2 matrix $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$. We have the following equality of $2n \times 2n$ matrices modulo $\mathfrak{p}_L O_L$:

$$\mathfrak{i}(\sigma_2(A)) \equiv \begin{bmatrix} \mathfrak{i}(a_{11}(\tau+1)) & \cdots & \mathfrak{i}(a_{1n}(\tau+1)) \\ \vdots & \ddots & \vdots \\ \mathfrak{i}(a_{n1}(\tau+1)) & \cdots & \mathfrak{i}(a_{nn}(\tau+1)) \end{bmatrix}$$

$$\equiv \begin{bmatrix} \mathfrak{i}(a_{11}) & \cdots & \mathfrak{i}(a_{1n}) \\ \vdots & \ddots & \vdots \\ \mathfrak{i}(a_{n1}) & \cdots & \mathfrak{i}(a_{nn}) \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ & & & & \ddots & & \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \end{bmatrix}.$$

It is then easy to see that

$$\det(\mathfrak{i}(\sigma_2(A))) \equiv 0 \pmod{\mathfrak{p}_L}. \tag{11}$$

The det in (11) involves the determinant, over the commutative field L, of the $2n \times 2n$ matrix $\mathfrak{i}(\sigma_2(A))$. This lets us conclude that $\mathrm{Nrd}(\sigma_2(A))$ belongs to $\mathfrak{p}_F O_F$ (since $O_F \cap \mathfrak{p}_L = \mathfrak{p}_F$). If we let ϖ denote $\mathrm{Nrd}(\sigma_2(A))$, we have

$$\mathrm{Nrd}(\sigma_2(A)) = \varpi \in \mathfrak{p}_F O_F.$$

In this first case, our earlier observations in equation (9) and equation (10) allow us to find an element ϵ in $\mathbb{Z}_p[D_{2p}]$ such that $\det([\epsilon]) = \det(A)$.

In the second case, we shall suppose that there exists entries $a_{i,j}$ and $a_{i',j'}$ of the matrix A such that $a_{i,j} \notin \mathfrak{m}$ and $a_{i',j'} \notin \mathfrak{m}'$. It is then straightforward (but slightly tedious) to see that one can perform a sequence of elementary row and column operations on the matrix A to find a new matrix, one of whose entries lies in neither $\mathfrak{m}$ nor $\mathfrak{m}'$. Such an entry must be a unit in the ring $\mathbb{Z}_p[D_{2p}]$. Since the elementary row and column operations do not change the Dieudonné determinant, this new matrix would have the same Dieudonné determinant as the matrix A. So without loss of generality, in this second case, we can suppose that there exists an entry u, in the $n \times n$ matrix A, which is a unit in the ring $\mathbb{Z}_p[D_{2p}]$. One can perform elementary row and column operations (similar to the ones used to obtain the formula in (5)) and use permutation matrices to obtain an $n \times n$ matrix B_n so that

$$B_n := \begin{bmatrix} u & 0 \\ 0 & B_{n-1} \end{bmatrix}, \text{ such that } B_{n-1} \in M_{n-1}\left(\mathbb{Z}_p[D_{2p}]\right) \cap \mathrm{GL}_{n-1}(\mathbb{Z}_p[D_{2p}]),$$
$$\det(A) = \det(B_n).$$

We have $\det(A)$ equals $u \det(B_{n-1})$ as elements of $(\mathbb{Q}_p[D_{2p}]^*)^{ab}$. One can now use mathematical induction to conclude that Question 2.4 has a positive answer for the pair $(\mathbb{Z}_p[D_{2p}], \mathbb{Q}_p[D_{2p}])$. □

EXAMPLE 2.7. Let H_8 denote the group of quaternions. This group has 8 elements given by the following presentation:

$$H_8 = \{x, y | x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1}\}$$

Note that $\mathbb{Z}_2[H_8]$ is a (non-commutative) local ring and that the quotient $\frac{\mathbb{Z}_2[H_8]}{\mathrm{Jac}(\mathbb{Z}_2[H_8])}$ is isomorphic to $\mathbb{F}_2$. The ring $\mathbb{Z}_2[H_8]$ satisfies **(WP)**. Question 2.4 has a negative answer for the pair $(\mathbb{Z}_2[H_8], \mathbb{Q}_2[H_8])$. In fact, we will give an example of a matrix A in $M_2(\mathbb{Z}_2[H_8]) \cap \mathrm{GL}_2(\mathbb{Q}_2[H_8])$, such that under the Dieudonné determinant $\det : \mathrm{GL}_2(\mathbb{Q}_2[H_8]) \to (\mathbb{Q}_2[H_8]^*)^{ab}$, the determinant $\det(A)$ does not lie in the image of the map $\mathbb{Z}_2[H_8] \cap \mathbb{Q}_2[H_8]^* \to (\mathbb{Q}_2[H_8]^*)^{ab}$.

Note that the Artin-Wedderburn theorem gives us an isomorphism of $\mathbb{Q}_2$-algebras:

$$\mathbb{Q}_2[H_8] \cong \mathbb{Q}_2[C_2 \oplus C_2] \times D. \tag{12}$$

Here, D is the division algebra of rational quaternions given by

$$D = \mathbb{Q}_2 \oplus \mathbb{Q}_2 i \oplus \mathbb{Q}_2 j \oplus \mathbb{Q}_2 ij.$$

We will write the Klein-four group $C_2 \oplus C_2$ as $\{e, f | e^2 = f^2 = 1, ef = fe\}$, so that

$$\mathbb{Q}_2[C_2 \oplus C_2] = \mathbb{Q}_2 \oplus \mathbb{Q}_2 e \oplus \mathbb{Q}_2 f \oplus \mathbb{Q}_2 ef.$$

The isomorphism in (12) is chosen to agree with the following two projection maps:

$$\sigma_1 : \mathbb{Q}_2[H_8] \to \mathbb{Q}_2[C_2 \oplus C_2], \qquad \sigma_2 : \mathbb{Q}_2[H_8] \to D.$$
$$\sigma_1(x) = e, \sigma_1(y) = f \qquad \sigma_2(x) = i, \sigma_2(y) = j.$$

Let us label det, $\det_1$ and $\det_2$ for the Dieudonné determinants involving the invertible matrices in $\mathrm{GL}_2(\mathbb{Q}_2[H_8])$, $\mathrm{GL}_2(\mathbb{Q}_2[C_2 \oplus C_2])$ and $\mathrm{GL}_2(D)$ respectively. Note that the reduced norm $\mathrm{Nrd} : D^* \to \mathbb{Q}_2^*$ is given by the formula $\mathrm{Nrd}(b_1 + b_2 i + b_3 j + b_4 ij) = b_1^2 + b_2^2 + b_3^2 + b_4^2$. The reduced norm gives us an isomorphism $\mathrm{Nrd} : (D^*)^{ab} \to \mathbb{Q}_2^*$. See Theorem 2.3 in Oliver's book [40]. We have the following diagram relating these Dieudonné determinants:

$$\begin{array}{ccc} \mathrm{GL}_2(\mathbb{Q}_2[H_8]) & \xrightarrow{\cong} & \mathrm{GL}_2(\mathbb{Q}_2[C_2 \oplus C_2]) \times \mathrm{GL}_2(D) \\ & \searrow^{\det} & \downarrow{\scriptstyle (\det_1, \det_2)} \\ & & \mathbb{Q}_2[C_2 \oplus C_2]^* \times (D^*)^{ab} \xrightarrow[\cong]{\mathrm{Nrd}} \mathbb{Q}_2[C_2 \oplus C_2]^* \times \mathbb{Q}_2^* \end{array}$$

We will follow the description of the integral group ring given in Section 7b of the work of Reiner and Ullom [45]. Let $Z_D := \mathbb{Z}_2 \oplus \mathbb{Z}_2 i \oplus \mathbb{Z}_2 j \oplus \mathbb{Z}_2 ij$. Reiner and Ullom identify $\mathbb{Z}_2[H_8]$ with the following subring of $\mathbb{Q}_2[C_2 \oplus C_2] \times D$ under the isomorphism given in (12) :

$$\mathbb{Z}_2[H_8] \cong \left\{ \left(a_1 + a_2 e + a_3 f + a_4 ef, b_1 + b_2 i + b_3 j + b_4 ij \right) \in \mathbb{Z}_2[C_2 \oplus C_2] \times Z_D, \right.$$
$$\left. \text{such that } (a_1, a_2, a_3, a_4) \equiv (b_1, b_2, b_3, b_4) \in \mathbb{F}_2[C_2 \oplus C_2] \right\}. \tag{13}$$

Note that $\mathbb{Z}_2[H_8]$ is a local ring, with a unique maximal left ideal given below:

$$\mathrm{Jac}(\mathbb{Z}_2[H_8]) = \left\{ a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 y + a_5 xy + a_6 x^2 y + a_7 x^3 y \in \mathbb{Z}_2[H_8] \right.$$
$$\left. \text{such that } a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 \in 2\mathbb{Z}_2 \right\}.$$

Suppose we have a matrix in $M_2(\mathbb{Z}_2[H_8] \cap \mathrm{GL}_2(\mathbb{Q}_2[H_8]))$. If one of the non-zero elements in this matrix belongs to the center of $\mathbb{Q}_2[H_8]$ or is a unit in $\mathbb{Z}_2[H_8]$, one can use a formula analogous to the one in (5), to show that the Dieudonné determinant of this matrix does have a representative in $\mathbb{Z}_2[H_8]$.

Let A denote the 2×2 matrix $\begin{bmatrix} 9+x+2y & 1+y \\ 1+xy & 9+x \end{bmatrix}$. Note that every element of this matrix belongs to the maximal ideal of $\mathbb{Z}_2[H_8]$. Note also that both $1+y$ and $1+xy$ do not belong to the centralizer of $9+x+2y$ or to the centralizer of $9+x$. The field $\mathbb{Q}_2(\sqrt{-1})$ is a splitting field for D. That is, we have an isomorphism $D \otimes_{\mathbb{Q}_2} \mathbb{Q}_2(\sqrt{-1}) \cong M_2(\mathbb{Q}_2(\sqrt{-1}))$ obtained by the following assignments:

$$x \to \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{bmatrix}, \quad y \to \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad xy \to \begin{bmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix}.$$

A direct computation then gives us the following equalities:

$$\begin{aligned} \det{}_1(\sigma_1(A)) &= 81+17e+17f+ef \in \mathbb{Q}_2[C_2 \ \oplus C_2]^*, \\ \mathrm{Nrd}\left(\det{}_2(\sigma_2(A))\right) &= \det \begin{bmatrix} 9+\sqrt{-1} & 2 & 1 & 1 \\ -2 & 9-\sqrt{-1} & -1 & 1 \\ 1 & \sqrt{-1} & 9+\sqrt{-1} & 0 \\ \sqrt{-1} & 1 & 0 & 9-\sqrt{-1} \end{bmatrix} \\ &= 8\times 857 \in \mathbb{Q}_2^*. \end{aligned}$$

Recall that if

$$a \equiv 1 \mod 2\mathbb{Z}_2 \implies a^2 \equiv 1 \mod 8\mathbb{Z}_2.$$

Let us use this observation along with the isomorphism in (13). Suppose that the element

$$(81+17e+17f+ef, b_1+b_2i+b_3j+b_4ij) \in \mathbb{Z}_2[C_2 \oplus C_2] \times Z_D$$

belongs to the subring $\mathbb{Z}_2[H_8]$. Then, $\mathrm{Nrd}(b_1+b_2i+b_3j+b_4ij) \equiv 4 \mod 8\mathbb{Z}_2$ (in particular, the reduced norm is not divisible by 8). This shows us the Dieudonné determinant $\det(A)$, for the 2×2 matrix A given in this example does not have any representative in the integral group $\mathbb{Z}_2[H_8]$. □

2.1 A maximal Λ-order

The Artin-Wedderburn theorem gives us the following isomorphism of $\mathbb{Q}_p$-algebras:

$$\mathbb{Q}_p[G] \cong \prod_i M_{m_i}(D_i). \tag{14}$$

Here, D_i is a finite-dimensional division algebra over $\mathbb{Q}_p$. Let O_{D_i} denote the unique maximal $\mathbb{Z}_p$-order inside D_i. Note that any $\mathbb{Z}_p$-order in $\mathbb{Q}_p[G]$ can be embedded in a maximal order and any two maximal orders in $M_n(D_i)$ are

isomorphic via an inner automorphism of $M_n(D_i)$. This allows us to choose the isomorphism in (14) so that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{Z}_p[G] & \longrightarrow & \mathbb{Q}_p[G] \\ \downarrow & & \downarrow \cong \\ \prod_i M_{m_i}(O_{D_i}) & \longrightarrow & \prod_i M_{m_i}(D_i). \end{array} \tag{15}$$

The horizontal maps are the natural injections. The vertical map on the left is also injective. This induces the commutative diagram given below:

$$\begin{array}{ccc} \Lambda[G] & \longrightarrow & Q_\Lambda[G] \\ \downarrow & & \downarrow \cong \\ \prod_i M_{m_i}\left(O_{D_i} \otimes_{\mathbb{Z}_p} \Lambda\right) & \longrightarrow & \prod_i M_{m_i}(D_i \otimes_{Q_p} Q_\Lambda). \end{array} \tag{16}$$

Here, Q_Λ denotes the fraction field of Λ. Once again, the horizontal maps are injective. The vertical map on the left is also injective.

For the rest of Section 3, we let D denote a divison ring containing $\mathbb{Q}_p$ inside its center and such that $[D : \mathbb{Q}_p]$ is finite. We let F denote the center of D, whose ring of integers is denoted by O_F. Let L denote (unfortunately, in other sections, the letter L has been used in another context. In this section, and only in this section, we use the letter L to denote the maximal subfield of the division algebra D) a maximal subfield of D containing F. Let O_L denote the ring of integers in L. The fields F and L are finite extensions of $\mathbb{Q}_p$. We let O_D denote the unique maximal $\mathbb{Z}_p$-order inside D. We recall some of the properties of O_D from Reiner's book on maximal orders [43]:

1. O_D is the integral closure of $\mathbb{Z}_p$ in D. See Theorem 12.8 in Reiner's book [43].
2. There exists a discrete valuation w on D, extending the p-adic valuation on $\mathbb{Z}_p$. The ring O_D is the valuation ring, with respect to w, inside D. See Chapter 12 in Reiner's book [43]. We let π_D denote a uniformizer in O_D, for this valuation.

We will also use the following notations:

$$F_\Lambda := F \otimes_{\mathbb{Q}_p} Q_\Lambda, \quad O_{F_\Lambda} := O_F \otimes_{\mathbb{Z}_p} \Lambda, \quad L_\Lambda := L \otimes_{\mathbb{Q}_p} Q_\Lambda, \quad O_{L_\Lambda} := O_L \otimes_{\mathbb{Z}_p} \Lambda$$
$$D_\Lambda := \underbrace{D \otimes_F F_\Lambda}_{\cong D \otimes_{\mathbb{Q}_p} Q_\Lambda}, \quad O_{D_\Lambda} := O_D \otimes_{\mathbb{Z}_p} \Lambda$$

We have the following equalities of vector space dimensions (see Theorem 7.15 in Reiner's book [43]):

$$\sqrt{\dim_{F_\Lambda} D_\Lambda} = \sqrt{\dim_F D} = \dim_F L = \dim_{F_\Lambda} L_\Lambda = \dim_L D = \dim_{L_\Lambda} D_\Lambda. \tag{17}$$

The number, that is equal to all the quantities appearing in (17), is called the index of the division algebra D in the Brauer group $\mathrm{Br}(F)$. As we will shall show in Lemma 2.10, D_Λ is a division algebra with center F_Λ. The number appearing in (17), is also the index of the division algebra D_Λ in the Brauer group $\mathrm{Br}(F_\Lambda)$.
One can obtain a non-canonical isomorphism $\Lambda \cong \mathbb{Z}_p[[x]]$ of topological rings, by sending a topological generator γ_0 of the topological group Γ to the element $x+1$ in $\mathbb{Z}_p[[x]]$. Since O_D has finite rank as a $\mathbb{Z}_p$-module, we have the following lemma:

Lemma 2.8. *The isomorphism $\Lambda \cong \mathbb{Z}_p[[x]]$ of topological rings, obtained by sending a topological generator γ_0 of Γ to $x+1$ $\Lambda \cong \mathbb{Z}_p[[x]]$, lets us obtain the following isomorphisms:*

$$\Lambda \cong \mathbb{Z}_p[[x]], \quad O_{F_\Lambda} \cong O_F[[x]], \quad O_{L_\Lambda} \cong O_L[[x]], \quad O_{D_\Lambda} \cong O_D[[x]].$$

Lemma 2.9. *O_{D_Λ} is a local ring with global dimension equal to two.*

Proof. Let gldim denote global dimension. The power series ring $O_D[[x]]$ in one variable x over the valuation ring O_D is local. By Theorem 2.3 and Proposition 2.7 in [1], the global dimension $\mathrm{gldim}\,(O_D)$ equals one. Note that by Theorem 7.5.3 in [34], we have

$$\mathrm{gldim}\,(O_D[[x]]) = \mathrm{gldim}\,(O_D) + 1 = 2.$$

□

Lemma 2.10. *D_Λ is a divison ring with center F_Λ, satisfying property (**WP**). L_Λ is a maximal commutative subfield, inside D_Λ, containing F_Λ.*

Proof. Note that Q_Λ is a purely transcendental extension of $\mathbb{Q}_p$, while F is a finite (algebraic) extension of $\mathbb{Q}_p$. As a result, F_Λ is a field. Since D is a finite-dimensional central simple F-algebra, D_Λ is a finite-dimensional central simple F_Λ-algebra (Corollary 7.8 in Reiner's book [43]). A finite-dimensional central simple algebra over the field F_Λ is isomorphic to a matrix ring over a division algebra. To prove the lemma, it suffices to show that D_Λ is a (not necessarily commutative) domain.
For this, observe that D_Λ is the localization of $O_D \otimes_{O_F} O_F[[x]]$ at the multiplicatively closed set $O_F[[x]] \setminus \{0\}$. The set $O_F[[x]] \setminus \{0\}$ is central in D_Λ and has no zero-divisors. Now, to prove the lemma, we are reduced to showing that $O_D \otimes_{O_F} O_F[[x]]$ is a (not necessarily commutative) domain. This follows simply because $O_D \otimes_{O_F} O_F[[x]]$, as observed in Lemma 2.8, is isomorphic to the power series ring $O_D[[x]]$ in one variable x over the domain O_D, and is hence a (not necessarily commutative) domain.
2 is invertible in the division algebra D_Λ. As a result, property (**WP**) holds.

An argument, similar to the one above, shows that L_Λ is a field. Note that L_Λ splits D_Λ since

$$D_\Lambda \otimes_{F_\Lambda} L_\Lambda \cong (D \otimes_F F_\Lambda) \otimes_{F_\Lambda} (F_\Lambda \otimes_F L) \cong (D \otimes_F L) \otimes_F F_\Lambda \\ \cong M_d(L) \otimes_F F_\Lambda \cong M_d(L_\Lambda).$$

Here, we let d equal $\dim_{F_\Lambda} L_\Lambda$. The relationship between various vector space dimensions given in (17), along with Corollary 28.10 in Reiner's book [43], lets us conclude that L_Λ is a maximal commutative subfield, inside D_Λ, containing F_Λ. □

Proposition 2.11. *For every integer m, the matrix ring $M_m(O_{D_\Lambda})$ is a maximal Λ-order inside $M_m(D_\Lambda)$. Furthermore, every maximal Λ-order inside $M_m(D_\Lambda)$ is isomorphic to $M_m(O_{D_\Lambda})$ by an inner automorphism via a unit in $M_m(D_\Lambda)$.*

Proof. The proposition follows from Ramras's work on maximal orders over regular local rings of dimension two. See Theorem 5.4 in [42]. To verify the hypotheses of Ramras's theorem, we need to show that for each integer m, the matrix ring $M_m(O_{D_\Lambda})$ is a semi-local ring with global dimension equal to two. Note that since O_{D_Λ} is a local ring, the matrix ring $M_m(O_{D_\Lambda})$ is semi-local (see 20.4 in Lam's book [32]). Furthermore, the global dimension is a Morita invariant (see the Proposition in 3.5.10 in [34]). Note that by Theorem 1.12 in Ramras's work [42], for a semi-local ring that is finitely generated over a commutative Noetherian ring, the left and right global dimensions coincide. By Lemma 2.9, the global dimension of the matrix ring $M_m(O_{D_\Lambda})$ is equal to two, for each integer n. The proposition follows. □

Remark 2.12. In our situation, we are considering maximal orders over the ring Λ, which is a complete regular local ring of dimension two. One can manufacture (non-commutative) examples when O_{D_Λ} is not the unique maximal Λ-order inside the division algebra D_Λ. Contrast this with the fact that O_D is the unique maximal $\mathbb{Z}_p$-order inside the division algebra D.

2.2 Reduced Norms

Let us first recall the definition of reduced norms in a general setting. Let $\mathcal{D}$ be a division algebra, finite dimensional over its center $\mathcal{F}$. Let $\mathcal{L}$ denote a maximal subfield of $\mathcal{D}$ containing $\mathcal{F}$. Let d equal the vector space dimension $\dim_{\mathcal{F}} \mathcal{L}$. The field $\mathcal{L}$ is a splitting field for $\mathcal{D}$. That is, we have $\mathcal{D} \otimes_{\mathcal{F}} \mathcal{L} \cong M_d(\mathcal{L})$. Consider the inclusion induced by the above isomorphism:

$$\mathfrak{i} : \mathcal{D} \hookrightarrow \mathcal{D} \otimes_{\mathcal{F}} \mathcal{L} \cong M_d(\mathcal{L}) \tag{18}$$

We have a group homomorphism $\mathrm{Nrd} : K_1(\mathcal{D}) \to \mathcal{F}^\times$ called the reduced norm map. To recall the definition of the reduced norm, let $\mathcal{A}$ denote a matrix in

$\mathrm{GL}_n(\mathcal{D})$. One can view the matrix $\mathfrak{i}(\mathcal{A})$ as an element of $M_{dn}(\mathcal{L})$. The reduced norm $\mathrm{Nrd}(\mathcal{A})$ is defined as the determinant, over the commutative field $\mathcal{L}$, of the $dn \times dn$ matrix $\mathfrak{i}(\mathcal{A})$. One can show that this is an element of $\mathcal{F}^\times$. One can also show that the definition of the reduced norm is independent of the choice of the splitting field and the choice of the isomorphism $\mathcal{D} \otimes_{\mathcal{F}} \mathcal{L} \cong M_d(\mathcal{L})$. See the description in Section 1.2.4 in Chapter III of Weibel's K-book [52] for more details. If we let $f(t)$ denote the characteristic polynomial of the endomorphism $\mathcal{L}^{dn} \xrightarrow{\mathcal{A}} \mathcal{L}^{dn}$, of $\mathcal{L}$ vector-spaces, induced by the matrix $\mathfrak{i}(\mathcal{A})$, then one sees that $\mathrm{Nrd}(\mathcal{A})$ is also equal to the constant term of the polynomial $f(t)$. By abuse of notation, we will let Nrd also denote the following composition of maps $\mathcal{D}^\times \to K_1(\mathcal{D}) \xrightarrow{\mathrm{Nrd}} \mathcal{F}^\times$.

Concerning the properties of the restriction of the reduced norm of the division algebra to the subring O_D, see Chapter 14 in Reiner's book [43]. What we will need is the fact that $\mathrm{Nrd}(\pi_D)$ is a uniformizer in O_F. Let us denote $\mathrm{Nrd}(\pi_D)$ by π_F.

Now, we return to our setting. We have a natural inclusion of rings $R \hookrightarrow T$, where $R = M_m(O_{D_\Lambda})$ and $T = M_m(D_\Lambda)$. The set $\mathrm{GL}_m(D_\Lambda) \cap M_m(O_{D_\Lambda})$, denoted by S (say) is an Ore set inside R. We have a natural isomorphism $R_S \cong T$. Morita equivalence lets us obtain the natural isomorphism

$$(R_S^*)^{ab} \overset{\det^{-1}}{\cong} K_1\left(M_m(D_\Lambda)\right) \underset{\text{Morita}}{\cong} K_1(D_\Lambda) \overset{\det}{\cong} (D_\Lambda^*)^{ab}.$$

Proposition 2.13. $\det(A)$ *belongs to the image of the natural map*

$$R \cap R_S^* \to (R_S^*)^{ab}.$$

of multiplicative monoids, where

$$R = M_m(O_{D_\Lambda}),\ R_S = M_m(D_\Lambda),\ A \in M_n(R) \cap \mathrm{GL}_n(R_S),\ (R_S^*)^{ab} \cong (D_\Lambda^*)^{ab}.$$

Proof. We proceed in several steps.

Step 1: The reduced norm of A is integral

We will show that $\mathrm{Nrd}(A)$ belongs to O_{F_Λ}. Let d denote $\dim_{F_\Lambda} L_\Lambda$. We will fix an inclusion $\mathfrak{i} : D_\Lambda \hookrightarrow M_d(L_\Lambda)$ as in (18). Let $f(t)$ denote the characteristic polynomial (this is the reduced characteristic polynomial associated to the central simple algebra $M_{mn}(D_\Lambda)$ over F_Λ) of the endomorphism $L_\Lambda^{dmn} \xrightarrow{\mathfrak{i}(A)} L_\Lambda^{dmn}$, induced by the matrix $\mathfrak{i}(A)$. Note that $f(t)$ is an element of the polynomial ring $F_\Lambda[t]$. See Theorem 9.3 in Reiner's book [43]. Note that D_Λ is a vector space of dimension d^2 over F_Λ. Let $g(t)$ denote the characteristic polynomial of the endomorphism $F_\Lambda^{d^2mn} \xrightarrow{\alpha_A} F_\Lambda^{d^2mn}$, induced by the matrix A. Since the entries of the matrix A lie in O_{D_Λ}, we have the following commutative diagram

of O_{F_Λ}-modules:

$$\begin{array}{ccc} (O_{D_\Lambda})^{mn} & \xrightarrow{\alpha_A} & (O_{D_\Lambda})^{mn} \\ \downarrow \cong & & \downarrow \cong \\ O_{F_\Lambda}^{d^2mn} & \xrightarrow{\alpha_A} & O_{F_\Lambda}^{d^2mn} \end{array} \tag{19}$$

The endomorphism $F_\Lambda^{d^2mn} \xrightarrow{A} F_\Lambda^{d^2mn}$ is induced by the O_{F_Λ}-module endomorphism given in (either row of) the commutative diagram in (19). Thus, the polynomial $g(t)$ must belong to $O_{F_\Lambda}[t]$. By Theorem 9.5 in Reiner's book [43], $f(t)$ divides $g(t)$, in $F_\Lambda[t]$. Note that the domain $O_{F_\Lambda}[t]$ is integrally closed. Note also that both $f(t)$ and $g(t)$ are monic polynomials. Since the coefficients of $g(t)$ are in O_{F_Λ}, so must the coefficients of $f(t)$. See Proposition 4.11 in Eisenbud's book [9]. Hence, $\mathrm{Nrd}(A)$ must lie in O_{F_Λ}.

Step 2: A non-commutative Weierstrass preparation theorem over $O_D[x]]$

For the rest of the proof, we shall fix an isomorphism

$$O_{D_\Lambda} \cong O_D[[x]]. \tag{20}$$

To each element $f = \sum_{n=0}^{\infty} a_n(f)x^n$ in $O_D[[x]]$, we can define a quantity called the reduced order of f, denoted $\mathrm{ord}(f)$, as follows:

$$\mathrm{ord}(f) = \min\left\{n \mid a_n \in O_D^\times\right\}.$$

We set $\mathrm{ord}(f)$ to be ∞, if the set $\left\{n \mid a_n \in O_D^\times\right\}$ is empty. Every non-zero element f in $O_D[[x]]$ can be written as $\pi_D^\mu f_0$, where f_0 is some power series in $O_D[[x]]$ such that $\mathrm{ord}(f_0) < \infty$.

Just as in the commutative case, we have a Weierstrass preparation theorem over $O_D[[x]]$ too. Firstly, let f_1 and f_2 be two elements in $O_D[[x]]$ such that $\mathrm{ord}(f_2) < \infty$. Then, there exists elements a, b, r, s in $O_D[[x]]$ such that

$$f_1 = af_2 + r, \qquad f_1 = f_2 b + s,$$

and such that both r and s are polynomials whose degrees are less than $\mathrm{ord}(f_2)$. Secondly, every element f in $O_D[[x]]$ can be written as

$$f = \pi_D^{\mu_f} U_f J_f, \text{ where } U_f \in O_D[[x]]^\times, \quad J_f \text{ is a monic polynomial under the isomorphism in (20)},$$

and

$$f = H_f V_f \pi_D^{\mu_f}, \text{ where } V_f \in O_D[[x]]^\times, \quad H_f \text{ is a monic polynomial under the isomorphism in (20)}.$$

These facts follow from the work of Venjakob [51]. See Theorem 3.1 and Corollary 3.2 in [51].

Step 3: $O_{D_\Lambda}\left[\frac{1}{p}\right]$ is a non-commutative PID

Theorem 14.3 in Reiner's book [43] tells us that $u_0\pi_D^d = \pi_F$, for some $u_0 \in O_D^\times$. As a result, there exists a positive integer d' so that

$$u_1\pi_D^{d'} = p, \text{ where } u_1 \in O_D^\times. \tag{21}$$

Since p is invertible in $O_{D_\Lambda}\left[\frac{1}{p}\right]$, so is π_D. This observation along with the Weierstrass preparation theorem allows us to conclude that $O_{D_\Lambda}\left[\frac{1}{p}\right]$ is a non-commutative PID. To see this: for each non-zero left (right) ideal I in $O_{D_\Lambda}\left[\frac{1}{p}\right]$, choose a monic polynomial f in I with least reduced order. A standard application of the Weierstrass preparation theorem, just as in the commutative case, will show us that this element f is a generator for the left (right) ideal I. We would like to make two further useful observations:

1. If J is a monic polynomial of degree r, then $\mathrm{Nrd}(J)$ is a monic polynomial of degree rd.
2. Every unit in the ring $O_{D_\Lambda}\left[\frac{1}{p}\right]$ is of the form $\pi_D^r\beta$, for some integer r and some β in $O_{D_\Lambda}^\times$.

Step 4: Diagonal reduction over $O_{D_\Lambda}\left[\frac{1}{p}\right]$:

Proposition 2.5 tells us that the matrix A admits a diagonal reduction via elementary operations in $M_{mn}\left(O_{D_\Lambda}\left[\frac{1}{p}\right]\right)$. So, there exists a diagonal matrix B in $M_{mn}\left(O_{D_\Lambda}\left[\frac{1}{p}\right]\right)$ and invertible matrices U and V (obtained as products of elementary matrices, permutation matrices and scalar matrices in $\mathrm{GL}_{mn}\left(O_{D_\Lambda}\left[\frac{1}{p}\right]\right)$) so that $A = UBV$. This allows us to obtain following equality in $K_1(D_\Lambda)$:

$$\det(U) = \pi_D^{r_U}\beta_U, \qquad \det(V) = \pi_D^{r_V}\beta_V,$$

where r_U and r_V are integers while β_U and β_V are elements of $O_{D_\Lambda}^\times$. Since B is a diagonal matrix, by multiplying all the elements in the main diagonal of B, we obtain the following equality in $K_1(D_\Lambda)$:

$$\det(B) = \pi_D^{r_B}\beta_B J_B,$$

where r_B is an integer, β_B is an element of $O_{D_\Lambda}^\times$ and J_B is a monic polynomial in O_{D_Λ} (under the isomorphism $O_{D_\Lambda} \cong O_D[[x]]$ given in (20)). Set

$$J_A := J_B \in O_D[x], \qquad r_A := r_U + r_B + r_V \in \mathbb{Z}, \qquad \beta_A := \beta_U\beta_B\beta_V \in O_{D_\Lambda}^\times.$$

Step 5: Completing the proof:
Set

$$C := \begin{bmatrix} \beta_A J_A \pi_D^{r_A} & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & 1 \end{bmatrix} \in M_m\left(O_{D_\Lambda}\left[\frac{1}{p}\right]\right).$$

Since $K_1(D_\Lambda)$ is an abelian group, we have the following equality in $K_1(D_\Lambda)$:

$$\begin{aligned} \det(A) &= \det(U)\det(B)\det(V) \\ &= \pi_D^{r_U}\beta_U \cdot \pi_D^{r_B}\beta_B J_B \cdot \pi_D^{r_V}\beta_V \\ &= \beta_U\beta_B\beta_V \cdot J_B \cdot \pi_D^{r_U+r_B+r_V} \\ &= \beta_A J_A \pi_D^{r_A} = \det(C). \end{aligned}$$

Now, to complete the proof of the proposition, we will show that r_A is non-negative. This would tell us that C is a matrix in $M_m(O_{D_\Lambda})$ and that C is a representative for $\det(A)$ in $M_m(O_{D_\Lambda})$.
Computing reduced norms, we obtain the following equality in F_Λ:

$$\begin{aligned} & \mathrm{Nrd}(A) = \mathrm{Nrd}(\det(A)) = \mathrm{Nrd}(\beta_A J_A \pi_D^{r_A}) \\ \Longrightarrow\ & \mathrm{Nrd}(A) = \mathrm{Nrd}(\beta_A)\cdot\mathrm{Nrd}(J_A)\cdot\pi_F^{dr_A}. \end{aligned}$$

We have shown that $\mathrm{Nrd}(A)$ is an element of O_{F_Λ}. So, $\mathrm{Nrd}\beta_A \cdot \mathrm{Nrd}(J_A)\cdot\pi_F^{dr_A}$ must belong to the unique factorization domain O_{F_Λ} as well. Since β_A is a unit in the ring O_{D_Λ}, the element $\mathrm{Nrd}(\beta_A)$ is a unit in O_{F_Λ}. This follows from Theorem 10.1 in Reiner's book [43] and the fact the reduced norm is a group homomorphism. The irreducible π_F cannot divide the monic polynomial $\mathrm{Nrd}(J_A)$. As a result, dr_A must be non-negative and hence, so must the integer r_A. This completes the proof of the proposition. □

3 The non-commutative Iwasawa main conjecture and Proof of Theorem 1

We will readily borrow the terminologies used in Weibel's K-book [52], the work of Fukaya-Kato [12] and Section 2 of Kakde's work [30] to describe various objects appearing in the non-commutative Iwasawa main conjecture. The "canonical" Ore sets $\mathfrak{S}$ and $\mathfrak{S}^*$, that come into play, are given below:

$$\mathfrak{S} = \left\{ s \in \Lambda[G],\ \text{such that } \frac{\Lambda[G]}{\Lambda[G]s} \text{ is a finitely generated } \mathbb{Z}_p\text{-module} \right\},$$
$$\mathfrak{S}^* = \bigcup_{n\geq 0} p^n\mathfrak{S}, \quad S^* = \Lambda \setminus \{0\}.$$

In this article, we will only consider the localization $\Lambda[G]_{\mathfrak{S}^*}$. The set $\mathfrak{S}^*$ is a multiplicatively closed set, consisting of non-zero divisors in $\Lambda[G]$. Since the group G is finite, we have the isomorphisms

$$\Lambda[G]_{\mathfrak{S}^*} \cong \Lambda[G]_{S^*} \cong Q_\Lambda[G].$$

It will be advantageous to work with S^* since all the elements of S^* are central. To formulate the main conjecture, we will have to consider the connecting homomorphism (obtained from the localization sequence in K-theory):

$$\partial : K_1\left(Q_\Lambda[G]\right) \to K_0\left(\Lambda[G], Q_\Lambda[G]\right).$$

3.1 Interpolation properties of the p-adic L-functions

To describe the interpolation properties of p-adic L-functions, we will follow the illustrations provided in the works of Johnston-Nickel [29, Section 4.3] and Ritter-Weiss [47, Section 4].
Let $Z(Q_\Lambda[G])$ denote the center of $Q_\Lambda[G]$. Corresponding to each Weddernburn component $M_{m_i}(D_i)$ of $\mathbb{Q}_p[G]$ appearing in equation (14), we let F_i denote the center $Z(D_i)$ and n_i denote $\dim_{F_i}(D_i)$. Note that F_i is a finite extension of $\mathbb{Q}_p$. Let O_{F_i} denote the ring of integers of F_i. Note also that every simple (left) module of $M_{m_i}(D_i)$ is isomorphic to the simple module $D_i^{m_i}$ with the natural (left) action of the matrix ring $M_{m_i}(D_i)$. As a result, each Weddernburn component $M_{m_i}(D_i)$ corresponds uniquely to an irreducible (totally even) Artin representation $\rho_i : \mathrm{Gal}(L/K) \to \mathrm{GL}_{n_i m_i}(F_i)$, given as follows:

$$\rho_i : \underbrace{\mathrm{Gal}(L/K)}_{G} \hookrightarrow \mathbb{Q}_p[G]^\times \twoheadrightarrow \mathrm{GL}_{m_i}(D_i) \cong \mathrm{Aut}\left(D_i^{m_i}\right) \cong \mathrm{GL}_{m_i n_i}(F_i).$$

To describe the local Euler factors at primes $\nu \in \Sigma_0$, we will follow the illustration provided in work of Greenberg-Vatsal [24, Proposition 2.4]. Suppose F denotes a finite extension of $\mathbb{Q}_p$. Suppose $\rho : G \to \mathrm{GL}_n(F)$ denotes an Artin representation. Let V and $V^* := \mathrm{Hom}_F\left(V, F(1)\right)$ denote the $F[G]$-modules corresponding to ρ and its Tate dual ρ^* respectively. For each ν in Σ_0, we consider $P_{\nu,\rho}(x) := \det\left(1 - x\rho^* \mid_{V_{I_\nu}^*} (\mathrm{Frob}_\nu^{-1})\right)$ in $F[x]$. Here, $V_{I_\nu}^*$ denotes the maximal quotient of V^* on which the inertia group I_ν acts trivially. Here, I_ν denotes the inertia subgroup inside $\mathrm{Gal}(\overline{K}_\nu/K_\nu)$ and Frob_ν is the Frobenius element in $\frac{\mathrm{Gal}(\overline{K}_\nu/K_\nu)}{I_\nu}$. Let Γ_ν denote a decomposition group corresponding to ν inside Γ. We can naturally view γ_ν, the Frobenius automorphism at ν of Γ_ν, as an element of Γ via the inclusion $\Gamma_\nu \subset \Gamma$. We will let $f_{\nu,\rho}$ denote $P_{\nu,\rho}(\gamma_\nu)$, viewed as an element of $\mathrm{Frac}(O_F[[\Gamma]])$.
Suppose first that the character χ is totally even. For each i, note that $\chi\rho_i$ then is a totally even Artin representation of K of "type S". Greenberg [15, Section 2] has constructed a primitive p-adic L-function $L_{p,\chi\rho_i}$ as an element

of Frac $(O_{F_i}[[\Gamma]])$. In this case, we let

$$\Phi_{\chi}^{\Sigma_0} := \left(L_{p,\chi\rho_i} \prod_{\nu \in \Sigma_0} f_{\nu,\chi\rho_i} \right)_i \qquad \text{in } Z(Q_\Lambda[G]).$$

Suppose now that the character χ is totally odd. For each i, note that $\chi^{-1}\omega\rho_i^{-1}$ then is a totally even Artin representation of K of "type S". Let $\iota : \mathbb{Z}_p[[\Gamma]] \to \mathbb{Z}_p[[\Gamma]]$ denote the $\mathbb{Z}_p$-linear ring homomorphism induced by sending $\gamma \to \gamma^{-1} < \gamma >$, for each γ in Γ. Here, we obtain the element $< \gamma >$ via the canonical injection $<>: \Gamma \hookrightarrow \mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}) \xrightarrow{\cong} 1 + p\mathbb{Z}_p$. In this case, we let

$$\Phi_{\chi}^{\Sigma_0} := \left(\iota\left(L_{p,\chi^{-1}\omega\rho_i^{-1}} \right) \prod_{\nu \in \Sigma_0} f_{\nu,\chi\rho_i} \right)_i \qquad \text{in } Z(Q_\Lambda[G]).$$

Conjecture 3.1 (Interpolation property for the p-adic L-function).
There exists a unique element ξ in $K_1(Q_\Lambda[G])$ such that $\mathrm{Nrd}(\xi) = \Phi_{\chi}^{\Sigma_0}$ *in* $Z(Q_\Lambda[G])$.

Remark 3.1. The fact that the primitive p-adic L-function for a totally odd Artin representation ρ is related to the primitive p-adic L-function for the corresponding totally even Artin representation $\rho^{-1}\omega$ is also mirrored on the algebraic side. In the commutative setting, this is the "reflection principle". See works of Greenberg [14, Section 2] and [16, Theorem 2]. The analog of the reflection principle in the non-commutative setting is discussed, from both the algebraic and analytic perspective, in the work of Fukaya-Kato [12, Section 4.4].

3.2 The non commutative Iwasawa main conjecture

On the algebraic side of Iwasawa theory, one works with the relative K_0-group $K_0(\Lambda[G], Q_\Lambda[G])$. One can give two different descriptions of this relative K_0-group. The first description involves the exact category $\mathbf{H}_{1,S^*}$. The category $\mathbf{H}_{1,S^*}$ is a subcategory of the category of finitely generated left $\Lambda[G]$-modules. The objects of $\mathbf{H}_{1,S^*}$ are $\Lambda[G]$-modules that are S^*-torsion and that have projective dimension less than or equal to one. To define the relative K_0-group $K_0(\Lambda[G], Q_\Lambda[G])$, we refer the reader to Definition 2.10 and Exercise 7.11 in Chapter II of Weibel's K-book [52]. We will need to consider tuples (P_1, α, P_2), where

- P_1 and P_2 are projective $\Lambda[G]$-modules, and
- the map $\alpha : Q_\Lambda[G] \otimes_{\Lambda[G]} P_1 \to Q_\Lambda[G] \otimes_{\Lambda[G]} P_2$ is an isomorphism of $Q_\Lambda[G]$-modules.

The relative K_0-group $K_0(\Lambda[G], Q_\Lambda[G])$ is defined to be the quotient of the free abelian group generated by such tuples (P_1, α, P_2) subject to the following two relations:

(i) $[(P_1, \alpha_1, Q_1)] + [(P_3, \alpha_2, Q_3)] = [(P_2, \alpha_2 \circ \alpha_1, Q_2)]$, whenever we have two exact sequences of projective $\Lambda[G]$-modules

$$0 \to P_1 \to P_2 \to P_3 \to 0, \qquad 0 \to Q_1 \to Q_2 \to Q_3 \to 0,$$

along with an induced commutative diagram of $Q_\Lambda[G]$-modules with exact rows:

$$\begin{array}{ccccc} Q_\Lambda[G] \otimes_{\Lambda[G]} P_1 & \hookrightarrow & Q_\Lambda[G] \otimes_{\Lambda[G]} P_2 & \twoheadrightarrow & Q_\Lambda[G] \otimes_{\Lambda[G]} P_3 \\ \cong \downarrow \alpha_1 & & \cong \downarrow \alpha_2 & & \cong \downarrow \alpha_3 \\ Q_\Lambda[G] \otimes_{\Lambda[G]} Q_1 & \hookrightarrow & Q_\Lambda[G] \otimes_{\Lambda[G]} Q_2 & \twoheadrightarrow & Q_\Lambda[G] \otimes_{\Lambda[G]} Q_3 \end{array}$$

(ii) $[(P_1, \alpha_{21}, P_2)] + [(P_2, \alpha_{32}, P_3)] = [(P_1, \alpha_{32} \circ \alpha_{21}, P_3)]$.

One can give a second description of this relative K_0-group involving the Waldhausen category $\mathbf{Ch}^\flat_{S^*}\big(\mathbf{P}(\Lambda[G])\big)$. This is the category of bounded chain complexes of finitely generated projective $\Lambda[G]$-modules whose cohomologies are S^*-torsion. In [12], Fukaya and Kato use the second description of this relative K_0-group to formulate the non-commutative Iwasawa main conjecture. Fukaya and Kato construct an element of this category $\mathbf{Ch}^\flat_{S^*}\big(\mathbf{P}(\Lambda[G])\big)$, whose cohomology is closely related to $\mathfrak{X}$. Fukaya and Kato label this chain complex $\mathrm{SC}\left(U, T, T^0\right)$. We will follow their notations to describe this chain complex.
If χ is totally even, we have

$$U = \Sigma_0, \quad T = \mathbb{Z}_p(\chi^{-1}\chi_p), \qquad T^0 = 0,$$

and the cohomology of the chain complex $\mathrm{SC}\left(U, T, T^0\right)$ is given below:

$$H^i\Big(\mathrm{SC}\left(U, T, T^0\right)\Big) = \begin{cases} \mathbb{Z}_p, & \text{if } i = 3 \text{ and } \chi \text{ is trivial,} \\ \mathfrak{X}, & \text{if } i = 2, \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

Here, $\chi_p : G_\Sigma \to \mathbb{Z}_p^\times$ denotes the p-adic cyclotomic character given by the action of G_Σ on the p-power roots of unity μ_{p^∞}.
If χ is totally odd, we have

$$U = \Sigma_0, \quad T = \mathbb{Z}_p(\chi^{-1}\chi_p), \qquad T^0 = \mathbb{Z}_p(\chi^{-1}\chi_p).$$

As for the cohomology of the chain complex when χ is totally odd, we have $H^i\Big(\mathrm{SC}\left(U, T, T^0\right)\Big) = 0$, if $i \neq 2$. We also have the following exact sequence:

$$0 \to \bigoplus_{\omega \in \Sigma_p(L_\infty)} H^1\left(\Gamma_\omega, H^0\left(I_\omega, \frac{\mathbb{Q}_p(\chi)}{\mathbb{Z}_p(\chi)}\right)\right)^\vee \to \mathfrak{X} \to H^2\Big(\mathrm{SC}\left(U, T, T^0\right)\Big) \to$$
$$\to \bigoplus_{\omega \in \Sigma_p(L_\infty)} H^0\left(G_\omega, \frac{\mathbb{Q}_p(\chi)}{\mathbb{Z}_p(\chi)}\right)^\vee \to 0. \tag{23}$$

Remark 3.2. A word of caution about the terminology in [12]: the module labeled $\mathcal{X}(T, T^0)$ in Fukaya and Kato's work [12] is the Pontryagin dual of the "strict" Selmer group.

Remark 3.3. There is a nice illustration on how to compute the cohomology of the chain complex $\mathrm{SC}\left(U, T, T^0\right)$ in Examples 4.5.1 and 4.5.2 of Fukaya and Kato's work [12]. We have mainly followed those illustrations. See Section 2.3 in Kakde's work for the description of the cohomology of the chain complex $\mathrm{SC}(U, T, T^0)$ when the character χ is totally even.
When χ is totally odd, we will need to use the description of $\mathrm{SC}(U, T, T^0)$ given in equation (4.1) in Section 4.1.2 of Fukaya and Kato's work [12]. The illustration given in the proof of Proposition 4.2.35 in [12] is helpful for this computation. The fact that $H^1\left(\mathrm{SC}\left(U, T, T^0\right)\right) = 0$ crucially relies on the observation that the global-local map defining the non-primitive "strict" Selmer group is surjective.

For the definition of $K_0\left(\mathbf{Ch}^{\flat}_{S^*}\left(\mathbf{P}(\Lambda[G])\right)\right)$, we refer the reader to Definition 9.1.2 in Chapter II of Weibel's K-book [52]. For our purposes, we will simply keep in mind that $K_0\left(\mathbf{Ch}^{\flat}_{S^*}\left(\mathbf{P}(\Lambda[G])\right)\right)$ is a certain quotient of the free abelian group generated by the objects of $\mathbf{Ch}^{\flat}_{S^*}\left(\mathbf{P}(\Lambda[G])\right)$. Using the second description of the relative K_0-group involving $\mathbf{Ch}^{\flat}_{S^*}\left(\mathbf{P}(\Lambda[G])\right)$ allows us to consider the element $\left[\mathrm{SC}\left(U, T, T^0\right)\right]$.
We will follow the formulation of the non-commutative Iwasawa main conjecture given in work of Johnston-Nickel [29, Conjecture 4.4]. See also work of Fukaya-Kato [12] and Ritter-Weiss [47].

Conjecture 3.2. *Conjecture 3.1 holds. Furthermore, we have the following equality in* $K_0\left(\Lambda[G], Q_\Lambda[G]\right)$*:*

$$\partial(\xi) \stackrel{?}{=} \left[\mathrm{SC}\left(U, T, T^0\right)\right]. \tag{24}$$

Let $\mathbf{H}_{S^*}$ denote the exact subcategory of the category of $\Lambda[G]$-modules, whose objects are finitely generated $\Lambda[G]$-modules that are S^*-torsion and that have finite projective dimension. It turns out that we have the following natural isomorphisms:

$$\begin{aligned} K_0(\Lambda[G], Q_\Lambda[G]) &\cong K_0\left(\mathbf{H}_{1,S^*}\right) \\ &\cong K_0\left(\mathbf{H}_{S^*}\right), \\ &\cong K_0\left(\mathbf{Ch}^{\flat}_{S^*}\left(\mathbf{P}(\Lambda[G])\right)\right). \end{aligned}$$

The second isomorphism follows from [52, Corollary 7.7.3 to the Resolution Theorem 7.6 in Chapter II]. The third isomorphism follows [52, Exercise 9.13 in Chapter II].

From the perspective of homological algebra, one difficulty with using the first description of the relative K_0-group is that the Iwasawa algbera $\Lambda[G]$ may have infinite global dimension. As a result, one really does need to use this workaround to work with an element in the relative K_0-group. Suppose, as when Theorems 2 and 3 indicate, for the rest of this section that the $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one. That is, we have the following short exact sequence of $\Lambda[G]$-modules:

$$0 \to \Lambda[G]^n \xrightarrow{A_{\mathfrak{X}}} \Lambda[G]^n \to \mathfrak{X} \to 0. \tag{25}$$

We have the following equality in the $K_0(\Lambda[G], Q_\Lambda[G])$:

$$\left[\mathrm{SC}\left(U, T, T^0\right)\right] = \left[\left(\Lambda[G], A_{\mathfrak{X}}, \Lambda[G]\right)\right]. \tag{26}$$

When χ is totally even and non-trivial, this equality follows from equation (22). Let us now see why equality holds in equation (26) when the character χ is totally odd. Note that $\mathbf{H}_{S^*}$ is closed under kernels of surjections inside the abelian category of finitely generated (left) $\Lambda[G]$-modules. By Theorem 9.2.2 in Chapter II of Weibel's K-book [52], we have the natural isomorphism $K_0\left(\mathbf{H}_{S^*}\right) \cong K_0\left(\mathbf{Ch}^\flat\left(\mathbf{H}_{S^*}\right)\right)$. Here, $\mathbf{Ch}^\flat\left(\mathbf{H}_{S^*}\right)$ is the category of bounded chain complexes in $\mathbf{H}_{S^*}$. By the same theorem, the equality in equation (26) would follow if one can show that the Euler characteristic of the chain complex $\mathfrak{X} \to H^2\left(\mathrm{SC}\left(U, T, T^0\right)\right)$, obtained from equation (23), equals zero in $K_0\left(\mathbf{Ch}^\flat\left(\mathbf{H}_{S^*}\right)\right)$.

Theorem 3 tells us that $\mathfrak{X}$ has a free resolution of length one under one of the following conditions:

(I) $H^0\left(G_\omega, \mathfrak{D}(\chi)\right) = 0$.

(II) ω is tamely ramified in the extension L_∞/K_∞.

One can compare the modules on either side of the exact sequence (23) using the observations in Section 4.2.1. If condition I holds for the prime ω in $\Sigma_p(L_\infty)$, then

$$H^1\left(\Gamma_\omega, H^0\left(I_\omega, \frac{\mathbb{Q}_p(\chi)}{\mathbb{Z}_p(\chi)}\right)\right)^\vee \cong H^0\left(G_\omega, \frac{\mathbb{Q}_p(\chi)}{\mathbb{Z}_p(\chi)}\right)^\vee = 0.$$

If condition I does not hold and condition II holds for the prime ω in $\Sigma_p(L_\infty)$, then

$$H^1\left(\Gamma_\omega, H^0\left(I_\omega, \frac{\mathbb{Q}_p(\chi)}{\mathbb{Z}_p(\chi)}\right)\right)^\vee \cong H^0\left(G_\omega, \frac{\mathbb{Q}_p(\chi)}{\mathbb{Z}_p(\chi)}\right)^\vee \cong \mathbb{Z}_p.$$

The equality in equation (26) follows from these observations and equation (23).

3.3 Proof of Theorem 1

We let

$$M_{\Lambda[G]} := \prod M_{m_i}\left(O_{D_i} \otimes_{\mathbb{Z}_p} \Lambda\right). \tag{27}$$

Proposition 10.5 in Reiner's book [43] and Proposition 2.11 tell us that $M_{\Lambda[G]}$ is a maximal Λ-order containing $\Lambda[G]$ inside $Q_\Lambda[G]$.

Theorem 1. *Suppose χ is non-trivial and Conjecture 3.2 holds. Suppose also that the $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one. Then, the non-primitive p-adic L-function ξ belongs to the image of the following natural map of multiplicative monoids:*

$$M_{\Lambda[G]} \cap Q_\Lambda[G]^* \to K_1\left(Q_\Lambda[G]\right).$$

Proof. Consider the following resolution of the $\Lambda[G]$-module $\mathfrak{X}$:

$$0 \to \Lambda[G]^n \xrightarrow{A_{\mathfrak{X}}} \Lambda[G]^n \to \mathfrak{X} \to 0. \tag{28}$$

Here, $A_{\mathfrak{X}}$ is a matrix in $M_n(\Lambda[G]) \cap \mathrm{GL}_n(Q_\Lambda[G])$. Note that, since Conjecture 3.2 is assumed to hold, we have the following equality in $K_0\left(\Lambda[G], Q_\Lambda[G]\right)$:

$$\partial(\xi) = \partial\left(A_{\mathfrak{X}}\right) = \left(\Lambda[G]^n, A_{\mathfrak{X}}, \Lambda[G]^n\right). \tag{29}$$

The localization exact sequence in K-theory gives us the following exact sequence

$$K_1(\Lambda[G]) \to K_1(Q_\Lambda[G]) \xrightarrow{\partial} K_0\left(\Lambda[G], Q_\Lambda[G]\right).$$

Since the ring $\Lambda[G]$ is also a semi-local ring, the Dieudonné determinant also provides us an isomorphism $K_1(\Lambda[G]) \cong (\Lambda[G]^*)^{ab}$. We have

$$\det(\xi) = \det\left(A_{\mathfrak{X}}\right)\det(B) \in (Q_\Lambda[G]^*)^{ab},$$

where B in a matrix in $\mathrm{GL}_\infty(\Lambda[G])$. The isomorphism $K_1(\Lambda[G]) \cong (\Lambda[G]^*)^{ab}$ allows us to find a representative for $\det(B)$ in $\Lambda[G]$. To prove the theorem, it now suffices to show that $\det\left(A_{\mathfrak{X}}\right)$ belongs to the image of the natural map of multiplicative monoids:

$$M_{\Lambda[G]} \cap Q_\Lambda[G]^* \to K_1\left(Q_\Lambda[G]\right)$$

The Artin-Weddernburn theorem and equation (16) gives us the following isomorphism:

$$Q_\Lambda[G] \cong \prod_i M_{m_i}(D_i \otimes_\Lambda Q_\Lambda) \tag{30}$$

Let σ_i denote the projection onto the i-th factor. The description of the maximal order, given in (27), now allows us to work with each factor in the product decomposition of (30). It now suffices to show that $\det(\sigma_i(A_{\mathfrak{X}}))$ belongs to the image of the natural map of multiplicative monoids:

$$M_{m_i}\left(O_{D_i}\otimes_{\mathbb{Z}_p}\Lambda\right)\bigcap \mathrm{GL}_{m_i}(D_i\otimes_\Lambda Q_\Lambda)\to \underbrace{K_1\left(M_{m_i}(D_i\otimes_\Lambda Q_\Lambda)\right)}_{\cong (D_i\otimes_\Lambda Q_\Lambda)^{ab}}.$$

This last statement, and hence the theorem, follows from Proposition 2.13. □

4 Cohomological criterion

In this section, we recall the cohomological criterion developed by Ralph Greenberg in the AMS memoir [21] on Iwasawa theory, projective modules and modular representations.

A theorem of Iwasawa [27] (see also Proposition 1 in Greenberg's work on p-adic Artin L-functions [22]) asserts that $\mathfrak{X}$ is a torsion module over $\Lambda[G]$. When χ is totally even, Proposition 6.10 (along with the validity of the Weak Leopoldt conjecture) in Greenberg's work on the structure of Galois cohomology groups [19] asserts that $\mathfrak{X}$ has no non-zero finite Λ-submodules. See Theorem 10.3.25 in the book by Neukirch, Schmidt and Winberg [36] as to why the weak Leopoldt conjecture is valid in this setting. When χ is totally odd, the discussion in Section 4.4 of Greenberg's recent work on the structure of Selmer groups [23] asserts that $\mathfrak{X}$ has no non-zero finite Λ-submodules. These results allow us to apply the cohomological criterion developed by Greenberg (Proposition 2.4.1 in [21]).

Proposition 4.1 (Proposition 2.4.1 in [21]). *The $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one if and only if there exists a positive integer m such that*

$$H^m\left(P,\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}(L_\infty)\right)=0,\qquad H^{m+1}\left(P,\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}(L_\infty)\right)=0 \tag{31}$$

for every subgroup P of P_G. Here, P_G is some p-Sylow subgroup of G.

Remark 4.2. Though Proposition 2.4.1 in [21] requires us to verify the vanishing criterion (given in (31)) for all subgroups of G, it suffices to restrict ourselves to subgroups of a p-sylow subgroup P_G. This is because every element of the discrete module $\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}(L_\infty)$ is killed by a power of p. Furthermore, Proposition 2.4.1 in [21] establishes that $\mathfrak{X}$ has a free resolution of length one if and only if for every subgroup P of P_G

$$H^i\left(P,\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}(L_\infty)\right)=0,\qquad \forall\ i\geq 1. \tag{32}$$

Theorem 4.2.3 in Hida's book [25] allows us to deduce that the validity of (31) implies the validity of equation (32).

Remark 4.3. When p does not divide $|G|$, the cohomology groups appearing in (31) vanish. As the cohomological criterion in Proposition 4.1 illustrates, in this case, the $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one.

4.1 Global cohomology groups and Proof of Theorem 2

In this section, we want to prove the following theorem stated in the introduction.

Theorem 2. *Suppose χ is totally even. Suppose p divides $|G|$. The $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one if and only if χ is non-trivial.*

Before proving the theorem, let us introduce some notations. Let P_G denote a p-Sylow subgroup of G. Let P be a subgroup of P_G. By Galois theory, we can identify P with a Galois group $\mathrm{Gal}(L_\infty/F_\infty)$, for some field F_∞ such that $K_\infty \subset L_\infty^{P_G} \subset F_\infty \subset L_\infty$. We have

$$P \cong \mathrm{Gal}(L_\infty/F_\infty).$$

Lemma 4.4. *The differential maps in the Hochschild-Serre spectral sequence*

$$H^i\Big(\mathrm{Gal}(L_\infty/F_\infty),\ H^j\big(\mathrm{Gal}(K_\Sigma/L_\infty),\mathfrak{D}(\chi)\big)\Big) \Longrightarrow H^{i+j}\left(\mathrm{Gal}(K_\Sigma/F_\infty),\mathfrak{D}(\chi)\right),$$

yield the following isomorphism, for each $i \geq 1$:

$$H^i\Big(\mathrm{Gal}(L_\infty/F_\infty),\ H^1\big(\mathrm{Gal}(K_\Sigma/L_\infty),\mathfrak{D}(\chi)\big)\Big) \cong H^{i+2}\Big(\mathrm{Gal}(L_\infty/F_\infty),\ H^0\big(\mathrm{Gal}(K_\Sigma/L_\infty),\mathfrak{D}(\chi)\big)\Big).$$

Proof. The p-cohomological dimensions of $\mathrm{Gal}(K_\Sigma/L_\infty)$ and $\mathrm{Gal}(K_\Sigma/F_\infty)$ are less than or equal to 2. The validity of the Weak Leopoldt conjecture (Theorem 10.3.25 in the book by Neukirch, Schmidt and Winberg [36]) allows us to conclude that

$$H^2\big(\mathrm{Gal}(K_\Sigma/L_\infty),\mathfrak{D}(\chi)\big) = 0, \qquad H^2\big(\mathrm{Gal}(K_\Sigma/F_\infty),\mathfrak{D}(\chi)\big) = 0.$$

These observations combine to give us the following equalities:

$$H^i\Big(\mathrm{Gal}(L_\infty/F_\infty),\ H^j\big(\mathrm{Gal}(K_\Sigma/L_\infty),\mathfrak{D}(\chi)\big)\Big) = 0, \qquad \forall j \geq 2.$$
$$H^j\big(\mathrm{Gal}(K_\Sigma/F_\infty),\mathfrak{D}(\chi)\big) = 0, \qquad \forall j \geq 2.$$

This completes the proof of the lemma. □

Suppose that the character χ is totally odd. In this case, we have $H^0\big(\mathrm{Gal}(K_\Sigma/L_\infty),\mathfrak{D}(\chi)\big) = 0$. This observation uses the fact that L_∞ is a totally real field. As an immediate consequence of Lemma 4.4, we obtain the following result.

LEMMA 4.5. *Suppose that the character χ is totally odd. We have the following equality:*

$$H^i\Big(\mathrm{Gal}(L_\infty/F_\infty),\ H^1\big(\mathrm{Gal}(K_\Sigma/L_\infty),\mathfrak{D}(\chi)\big)\Big)=0. \tag{33}$$

We will use the following simple observation frequently in this paper.

OBSERVATION 4.6. *The finite character $\chi : G_\Sigma \to \mathbb{Z}_p^\times$ is non-trivial if and only if the residual character $\overline{\chi}\ :\ G_\Sigma \xrightarrow{\chi} \mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ associated to it is non-trivial.*

We now proceed to the proof of Theorem 2.

Proof of Theorem 2. We are working under the assumption that the character χ is totally even. In this case, note that $\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}(L_\infty) = H^1\big(\mathrm{Gal}(K_\Sigma/L_\infty),\mathfrak{D}(\chi)\big)$. If the character χ is non-trivial, we have $H^0\big(\mathrm{Gal}(K_\Sigma/L_\infty),\mathfrak{D}(\chi)\big)=0$. In this case when χ is even and non-trivial, by Lemma 4.4, for each $i\geq 1$ and every subgroup P of P_G, we have

$$\begin{aligned} &H^i\Big(P,\ H^1\big(\mathrm{Gal}(K_\Sigma/L_\infty),\mathfrak{D}(\chi)\big)\Big)\\ &\quad= H^i\Big(\mathrm{Gal}(L_\infty/F_\infty),\ H^1\big(\mathrm{Gal}(K_\Sigma/L_\infty),\mathfrak{D}(\chi)\big)\Big)=0. \end{aligned} \tag{34}$$

So by Proposition 4.1, when χ is even and non-trivial, the $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one.

Finally, let us suppose that the character χ is trivial, so that $\mathfrak{D}(\chi)=\frac{\mathbb{Q}_p}{\mathbb{Z}_p}$. In this case, we will choose P (which is isomorphic to $\mathrm{Gal}(L_\infty/F_\infty)$) so that P is a cyclic group of order p. This is possible due to our assumption that p divides the Galois group G (and due to Cauchy's theorem). Now, we have the following sequence of isomorphisms for each $i\geq 1$ (the second isomorphism uses the fact that we have chosen $\mathrm{Gal}(L_\infty/F_\infty)$ to be cyclic):

$$\begin{aligned} &H^{2i-1}\left(\mathrm{Gal}(L_\infty/F_\infty),\ H^1\left(\mathrm{Gal}(K_\Sigma/L_\infty),\mathfrak{D}(\chi)\right)\right)\\ &\cong H^{2i+1}\left(\mathrm{Gal}(L_\infty/F_\infty),\ H^0\left(\mathrm{Gal}(K_\Sigma/L_\infty),\frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)\right)\\ &\cong H^1\left(\mathrm{Gal}(L_\infty/F_\infty),\ H^0\left(\mathrm{Gal}(K_\Sigma/L_\infty),\frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)\right)\\ &\cong \mathrm{Hom}\left(\mathrm{Gal}(L_\infty/F_\infty),\frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)\cong\frac{\mathbb{Z}}{p\mathbb{Z}}. \end{aligned}$$

The isomorphisms given in the equation above and Proposition 4.1 let us conclude that if the character χ is even and trivial, the $\Lambda[G]$-module $\mathfrak{X}$ does not have a free resolution of length one. This completes the proof of Theorem 2. □

4.2 Local cohomology groups and Proof of Theorem 3

The whole of Section 4.2 will be devoted to the proof of Theorem 3, which we state below.

Theorem 3. *Suppose χ is totally odd. Suppose p divides $|G|$. The $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one if and only if one of the two following conditions holds for every prime $\omega \in \Sigma_p(L_\infty)$:*

(I) $H^0\left(G_\omega, \mathfrak{D}(\chi)\right) = 0$

(II) *ω is tamely ramified in the extension L_∞/K_∞.*

Let P_G denote a p-Sylow subgroup of G. Let P denote a subgroup of P_G. By Galois theory, we can identify P with $\mathrm{Gal}(L_\infty/F_\infty)$, for some field F_∞ such that $K_\infty \subset L_\infty^{P_G} \subset F_\infty \subset L_\infty$. We have

$$P \cong \mathrm{Gal}(L_\infty/F_\infty).$$

Fix a prime ν in $\Sigma_p(F_\infty)$. Suppose $\omega_1, \ldots, \omega_n$ denote all the primes in L_∞ lying above the prime ν in F. Let $\omega(\nu)$ equal ω_1. Let $P_{\omega(\nu)}$ denote the decomposition group inside P, corresponding to the prime $\omega(\nu)$ lying above ν. We have the following isomorphism:

$$\prod_{\omega_i|\nu} H^1\left(I_{\omega_i}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega_i}} \cong \mathrm{Ind}_{P_{\omega(\nu)}}^{P}\left(H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega(\nu)}}\right)$$

Shapiro's lemma then lets us deduce the following isomorphism:

$$H^i\left(P, \prod_{\omega_i|\nu} H^1\left(I_{\omega_i}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega_i}}\right) \cong H^i\left(P_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega(\nu)}}\right). \quad (35)$$

Corollary 3.2.3 in Greenberg's work [20], along with the observation that $H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega(\nu)}}$ is a quotient of the local cohomology group $H^1\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right)$ and the fact that Σ contains primes above a finite prime number ν not lying above p, let us conclude that the map $\phi^{\Sigma_0}_{\mathfrak{D}(\chi),\mathrm{odd}}$ is surjective. The fact that the map $\phi^{\Sigma_0}_{\mathfrak{D}(\chi),\mathrm{odd}}$ is surjective crucially relies on the fact that it is a global-to-local map defining the non-primitive Selmer group. We have the short exact sequence

$$\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}(L_\infty) \hookrightarrow H^1\left(\mathrm{Gal}(K_\Sigma/L_\infty), \mathfrak{D}(\chi)\right) \xrightarrow{\phi^{\Sigma_0}_{\mathfrak{D}(\chi),\mathrm{odd}}} \prod_{\eta \in \Sigma_p(L_\infty),} H^1\left(I_\eta, \mathfrak{D}(\chi)\right)^{\Gamma_\eta}$$

of $\Lambda[G]$-modules. Let us apply the long exact sequence in Galois cohomology, for the group P. Lemma (4.5) let us obtain the following isomorphism, for each $i \geq 1$:

$$\prod_{\eta \in \Sigma_p(L_\infty)} H^i\left(P, H^1(I_\eta, \mathfrak{D}(\chi))^{\Gamma_\eta}\right) \cong H^{i+1}\left(P, \mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}(L_\infty)\right) \quad (36)$$

The product in equation (36) is indexed by the primes lying above p in L_∞. Equation (35) allows us to rewrite the isomorphism in (36) as follows (where the product is now indexed by the primes lying above p in F_∞), for each $i \geq 1$:

$$\prod_{\nu \in \Sigma_p(F_\infty)} H^i\left(P_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega(\nu)}}\right) \cong H^{i+1}\left(P,\ \mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}\left(L_\infty\right)\right). \quad (37)$$

Let $G_{\omega(\nu)}$ (and G_ν respectively) denote the decomposition group lying inside $\mathrm{Gal}(K_\Sigma/L_\infty)$ (and $\mathrm{Gal}(K_\Sigma/F_\infty)$ respectively) corresponding to the prime $\omega(\nu)$ (and ν respectively). Let $I_{\omega(\nu)}$ (and I_ν respectively) denote the inertia subgroup inside $G_{\omega(\nu)}$ (and G_ν respectively). Let $\Gamma_{\omega(\nu)}$ (and Γ_ν respectively) denote the quotient $\frac{G_{\omega(\nu)}}{I_{\omega(\nu)}}$ (and $\frac{G_\nu}{I_\nu}$ respectively). We have the following natural maps:

$$G_{\omega(\nu)} \hookrightarrow G_\nu, \qquad P_{\omega(\nu)} \cong \frac{G_\nu}{G_{\omega(\nu)}}. \quad (38)$$

The p-cohomological dimensions of both the groups G_ν and $G_{\omega(\nu)}$ equal one (see the discussion on Page 25 of [18]). As a result,

$$H^j\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right) = 0, \quad H^j\left(G_\nu, \mathfrak{D}(\chi)\right) = 0, \quad \forall j \geq 2.$$

An argument (similar to the one used to establish Lemma 4.4) involving the spectral sequence

$$H^i\left(P_{\omega(\nu)}, H^j\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) \implies H^{i+j}\left(G_\nu, \mathfrak{D}(\chi)\right)$$

then allows us obtain the following natural isomorphism for all $i \geq 1$ (via the differential maps):

$$H^i\left(P_{\omega(\nu)}, H^1\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) \cong H^{i+2}\left(P_{\omega(\nu)}, H^0\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right). \quad (39)$$

We will now complete the proof of Theorem 3 by considering the following cases:

- (Condition I) When $H^0\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right) = 0$.
- (Condition II) When $\omega(\nu)$ is tamely ramified in the extension L_∞/K_∞.
- There exists a prime $\omega \in \Sigma_p(L_\infty)$ that doesn't satisfy both conditions I and II.

These cases are considered in Sections 4.2.1, 4.2.2 and 4.2.3. The headings in each of these sections highlight the assumption which we will be working with.

4.2.1 When $H^0\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right) = 0$

Consider the following inflation-restriction short exact sequence that is $P_{\omega(\nu)}$-equivariant:

$$H^1\Big(\Gamma_{\omega(\nu)}, H^0\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\Big) \hookrightarrow H^1\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right) \twoheadrightarrow H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega(\nu)}}.$$

We first claim that $H^1\Big(\Gamma_{\omega(\nu)}, H^0\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\Big)$ equals zero. It suffices to prove the claim when $H^0\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right) \neq 0$. The reasoning for this is similar to the one given in Observation 4.6. If $H^0\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right) \neq 0$, then

$$H^0\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right) \cong \mathfrak{D}(\chi) = \frac{\mathbb{Q}_p(\chi)}{\mathbb{Z}_p(\chi)}.$$

The group $\Gamma_{\omega(\nu)}$ is topologically generated by Frobenius (denoted by $\mathrm{Frob}_{\omega(\nu)}$). We have the following exact sequence:

$$\begin{aligned} 0 \to H^1\Big(\Gamma_{\omega(\nu)}, H^0\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\Big)^\vee \to \\ \to \underbrace{H^0\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^\vee}_{\mathbb{Z}_p(\chi^{-1})} \xrightarrow{\mathrm{Frob}_{\omega(\nu)}-1} \underbrace{H^0\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^\vee}_{\mathbb{Z}_p(\chi^{-1})} \\ \to \underbrace{H^0\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^\vee}_{=0} \to 0. \end{aligned}$$

A surjective endomorphism of a finitely generated free $\mathbb{Z}_p$-module must be an isomorphism. We can now conclude that $H^1\Big(\Gamma_{\omega(\nu)}, H^0\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\Big) = 0$. So, we have the following isomorphism that is $P_{\omega(\nu)}$-equivariant:

$$H^1\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right) \cong H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega(\nu)}}. \tag{40}$$

This lets us obtain the following isomorphism for all $i \geq 0$:

$$H^i\Big(P_{\omega(\nu)},\ H^1\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\Big) \cong H^i\Big(P_{\omega(\nu)},\ H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega(\nu)}}\Big). \tag{41}$$

Equation (39) lets us conclude that for all $i \geq 1$,

$$H^i\left(P_{\omega(\nu)}, H^1\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) \cong H^{i+2}\left(P_{\omega(\nu)}, H^0\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) = 0. \tag{42}$$

Combining (41), (42), we obtain the following equality for all $i \geq 1$:

$$\begin{aligned} H^i\Big(P_{\omega(\nu)},\ H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega(\nu)}}\Big) &\cong H^i\left(P_{\omega(\nu)}, H^1\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) \\ &\cong H^{i+2}\left(P_{\omega(\nu)}, H^0\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) = 0. \end{aligned} \tag{43}$$

4.2.2 When $\omega(\nu)$ is tamely ramified in the extension L_∞/K_∞

We would like to start with the following observation. The Galois group $\mathrm{Gal}(L_\infty/F_\infty)$ is a p-group. If $\omega(\nu)$ is tamely ramified in the extension L_∞/K_∞, then prime $\omega(\nu)$ in L_∞ (lying over the prime ν in F_∞) must remain unramified in the extension L_∞/F_∞. Therefore, in addition to the maps in (38), we have the natural isomorphisms:

$$I_{\omega(\nu)} \xhookrightarrow{\cong} I_\nu, \qquad \Gamma_\nu \cong \frac{\Gamma_\omega}{P_\omega}.$$

Note that the p-cohomological dimensions of the groups $\Gamma_{\omega(\nu)}$ and Γ_ν equal one (these groups are isomorphic to $\hat{\mathbb{Z}}$). For any Γ_ν-module $\mathcal{M}$, an argument involving the spectral sequence (which is similar to the one used to establish Lemma 4.4),

$$H^i\Big(P_{\omega(\nu)}, H^j\left(\Gamma_{\omega(\nu)}, \mathcal{M}\right)\Big) \implies H^{i+j}\left(\Gamma_\nu, \mathcal{M}\right)$$

allows us obtain the following natural isomorphism (via the differential maps):

$$H^i\Big(P_{\omega(\nu)}, H^1\left(\Gamma_{\omega(\nu)}, \mathcal{M}\right)\Big) \cong H^{i+2}\Big(P_{\omega(\nu)}, H^0\left(\Gamma_{\omega(\nu)}, \mathcal{M}\right)\Big), \qquad \forall\ i \geq 1. \tag{44}$$

Furthermore, the p-cohomological dimension of the inertia group $I_{\omega(\nu)}$ (in addition to the decomposition group $G_{\omega(\nu)}$ and the quotient group $\Gamma_{\omega(\nu)}$) also equals one. See the discussion on Page 25 of [18]. Analysing the spectral sequence

$$H^i\Big(\Gamma_{\omega(\nu)}, H^j\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\Big) \implies H^{i+j}\left(G_{\omega(\nu)}, \mathfrak{D}(\chi)\right)$$

now lets us deduce that

$$H^1\Big(\Gamma_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\Big) = 0. \tag{45}$$

To deduce equation (45), we do not use the condition that $\omega(\nu)$ is tamely ramified in the extension L_∞/K_∞.
Let $\mathcal{M}$ equal $H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)$. Combining (44) and (45), we obtain the following isomorphisms for all $i \geq 3$:

$$\begin{aligned} H^i\Big(P_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega(\nu)}}\Big) \\ \cong H^{i-2}\left(P_{\omega(\nu)}, H^1\left(\Gamma_{\omega(\nu)},\ H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right)\right) = 0. \end{aligned} \tag{46}$$

The arguments in Sections 4.2.1 and 4.2.2 have the following implications towards Theorem 3. Suppose every prime ω in $\Sigma_p(L_\infty)$ satisfies one of the following conditions:

(I) $H^0\left(G_\omega, \mathfrak{D}(\chi)\right) = 0$

(II) ω is tamely ramified in the extension L_∞/K_∞.

Combining (37), (43) and (46), we obtain the following equality for all $i \geq 4$:

$$H^i\left(P,\ \mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}\left(L_\infty\right)\right) \cong \prod_{\nu \in \Sigma_p(F_\infty)} H^{i-1}\left(P_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega(\nu)}}\right) = 0. \tag{47}$$

As a result, Proposition 4.1 now lets us conclude that the $\Lambda[G]$-module $\mathfrak{X}$ has a free resolution of length one if every prime $\omega \in \Sigma_p(L_\infty)$ satisfies Condition I or II.

4.2.3 There exists a prime $\omega \in \Sigma_p(L_\infty)$ that doesn't satisfy both conditions I and II

For the rest of this section, we will work under the assumption given in the heading of this subsection. Under this assumption, we will establish that the $\Lambda[G]$-module $\mathfrak{X}$ does not have a free resolution of length one.
Since the prime ω doesn't satisfy Condition I, we have $H^0\left(G_\omega, \mathfrak{D}(\chi)\right) \neq 0$. As we argued earlier (see Observation 4.6), this leads us to assert that the restriction of the character χ to G_ω is trivial and that

$$H^0\left(I_\omega, \mathfrak{D}(\chi)\right) \cong H^0\left(G_\omega, \mathfrak{D}(\chi)\right) \cong \frac{\mathbb{Q}_p}{\mathbb{Z}_p}. \tag{48}$$

Furthermore, since the prime ω doesn't satisfy Condition II, the prime ω is wildly ramified in the extension L_∞/K_∞. As a result, p divides the order of the inertia subgroup inside $\mathrm{Gal}(L_\infty/K_\infty)$, corresponding to the prime ω. We choose P to be a cyclic subgroup of order p inside this inertia subgroup (this is possible due to Cauchy's theorem). As we did in the earlier sections, we will identify P with $\mathrm{Gal}(L_\infty/F_\infty)$, for some field F_∞ satisfying $K_\infty \subset F_\infty \subset L_\infty$. We let ν denote the prime in F_∞ lying below ω. To be consistent with our notations in the earlier sections, we let $\omega(\nu)$ denote the prime ω. We have the following natural maps:

$$P_{\omega(\nu)} \xhookrightarrow{=} P \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$$

Since the prime $\omega(\nu)$ is totally ramified in the extension L_∞/F_∞, we have a natural inclusion of inertia groups $I_{\omega(\nu)} \hookrightarrow I_\nu$. We also have the following natural isomorphisms:

$$P_{\omega(\nu)} \cong \frac{I_\nu}{I_\omega(\nu)}, \qquad \Gamma_{\omega(\nu)} \cong \Gamma_\nu. \tag{49}$$

The short exact sequences

$$0 \to \underbrace{\frac{I_\nu}{I_{\omega(\nu)}}}_{\cong P_{\omega(\nu)}} \to \frac{G_\nu}{I_{\omega(\nu)}} \to \underbrace{\frac{G_\nu}{I_\nu}}_{\cong \Gamma_\nu} \to 0, \qquad 0 \to \underbrace{\frac{G_{\omega(\nu)}}{I_{\omega(\nu)}}}_{\cong \Gamma_{\omega(\nu)}} \to \frac{G_\nu}{I_{\omega(\nu)}} \to \underbrace{\frac{G_\nu}{G_{\omega(\nu)}}}_{\cong P_{\omega(\nu)}} \to 0,$$

allow us to view both $P_{\omega(\nu)}$ and $\Gamma_{\omega(\nu)}$ as normal subgroups of $\frac{G_\nu}{I_{\omega(\nu)}}$. As a result,

$$\frac{G_\nu}{I_{\omega(\nu)}} \cong P_{\omega(\nu)} \times \Gamma_{\omega(\nu)}.$$

Equation (45) tells us that $H^1\left(\Gamma_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) = 0$. So, the following exact sequence

$$H^0\left(\Gamma_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) \hookrightarrow H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right) \xrightarrow{\mathrm{Frob}_{\omega(\nu)}-1} H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)$$

is $P_{\omega(\nu)} \times \Gamma_{\omega(\nu)}$-equivariant. Consider the following long exact sequence in group cohomology (for the group $P_{\omega(\nu)}$):

$$\begin{aligned} &\to H^i\left(P_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega(\nu)}}\right) \to \\ &\quad \to H^i\left(P_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) \xrightarrow{\mathrm{Frob}_{\omega(\nu)}-1} H^i\left(P_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) \to \end{aligned} \tag{50}$$

For each $i \geq 1$, we have the following commutative diagram:

$$\begin{array}{ccc} H^i\left(P_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) & \xrightarrow{\mathrm{Frob}_{\omega(\nu)}-1} & H^i\left(P_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) \\ \downarrow \cong & & \downarrow \cong \\ H^{i+2}\left(P_{\omega(\nu)}, H^0\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) & \xrightarrow{\mathrm{Frob}_{\omega(\nu)}-1} & H^{i+2}\left(P_{\omega(\nu)}, H^0\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)\right) \end{array} \tag{51}$$

Equation (48) tells us that $H^0\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right) \cong \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$. Note that the group $\Gamma_{\omega(\nu)}$, which is topologically generated by $\mathrm{Frob}_{\omega(\nu)}$, acts trivially on both $P_{\omega(\nu)}$ and $\frac{\mathbb{Q}_p}{\mathbb{Z}_p}$. As a result, for each $i \geq 1$, the horizontal maps in the commutative diagram (51) (given by $\mathrm{Frob}_{\omega(\nu)} - 1$) are the zero maps. Since $P_{\omega(\nu)}$ is a cyclic group of order p, for all $i \geq 1$,

$$H^{2i-1}\left(P_{\omega(\nu)}, \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cong \mathrm{Hom}\left(P_{\omega(\nu)}, \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \cong \frac{\mathbb{Z}}{p\mathbb{Z}}, \qquad H^{2i}\left(P_{\omega(\nu)}, \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) = 0.$$

Combining these observations pertaining to the long exact sequence (50) and the commutative diagram (51) with the fact that $P_{\omega(\nu)}$ is a cyclic group leads us to conclude that

$$H^i\left(P_{\omega(\nu)}, H^1\left(I_{\omega(\nu)}, \mathfrak{D}(\chi)\right)^{\Gamma_{\omega(\nu)}}\right) \cong \frac{\mathbb{Z}}{p\mathbb{Z}}, \qquad \forall\ i \geq 1.$$

Equation (37) now let us deduce that for all $i \geq 2$, we have the following surjection:

$$H^i\left(P,\ \mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi)}\left(L_\infty\right)\right) \twoheadrightarrow \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

As a result, Proposition 4.1 lets us make the following deduction: the $\Lambda[G]$-module $\mathfrak{X}$ does not have a free resolution of length one if there exists a prime $\omega \in \Sigma_p(L_\infty)$ that does not satisfiy both Condition I and II.
Our observations in Sections 4.2.1, 4.2.2 and 4.2.3 now complete the proof of Theorem 3.

5 Elliptic curve with a cyclic p^2 isogeny and proof of Theorem 4

5.1 Setup of Theorem 4

Let E be an elliptic curve defined over $\mathbb{Q}$ with good ordinary or split multiplicative reduction at p. Let $\Phi : E \to E'$ be a cyclic isogeny, defined over $\mathbb{Q}$, of degree p^2. Let $\tilde{\Phi} : E' \to E$ denote the dual isogeny (which is also a cyclic isogeny over $\mathbb{Q}$ of degree p^2). Let us enlarge the set Σ to contain all the primes of bad reduction for E. The non-primitive Selmer group $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)$ associated to E (introduced in the work of Greenberg and Vatsal [24]) is given below:

$$\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty) = \ker\left(H^1\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty), E[p^\infty]\right) \to H^1(I_\eta, \mathfrak{A})^{G_\eta/I_\eta}\right).$$

Here, G_η and I_η denote the decomposition and inertia subgroup for the unique prime η in $\mathbb{Q}_\infty$ lying above p. If E has good reduction at p then we let $\mathfrak{A}$ equal the $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module $\overline{E}[p^\infty]$, the p-power torsion points on the reduced elliptic curve $\overline{E}$. If E has split multiplicative reduction at p, then $\mathfrak{A}$ is defined to be $\mathbb{Q}_p/\mathbb{Z}_p$ with the trivial action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Both $\ker(\Phi)$ and $\ker(\tilde{\Phi})$ are cyclic groups of order p^2. Without loss of generality, we shall henceforth assume that the action of $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$ on $\ker(\Phi)$ is even (otherwise we could simply consider the curve E' and the dual isogeny). We have the following natural characters:

$$\begin{aligned}
\phi &: \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}) \to \mathrm{Aut}\left(\ker(\Phi)\right) \cong \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times, \\
\tilde{\phi} &: \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}) \to \mathrm{Aut}\left(\ker\left(\tilde{\Phi}\right)\right) \cong \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times \\
\chi_\phi &: \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}) \to \mathrm{Aut}\left(\ker(\Phi)[p]\right) \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^\times, \\
\chi_{\tilde{\phi}} &: \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}) \to \mathrm{Aut}\left(\ker\left(\tilde{\Phi}\right)[p]\right) \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^\times,
\end{aligned}$$

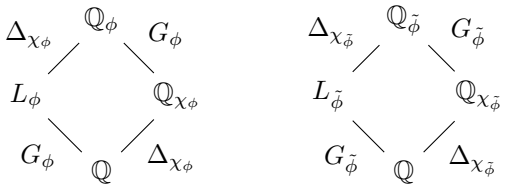
The Weil pairing gives us the following equality of characters:

$$\phi\tilde{\phi} = \chi_p \pmod{p^2}, \qquad \chi_\phi\chi_{\tilde{\phi}} = \chi_p \pmod{p}. \tag{52}$$

Here $\chi_p : \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}) \to \mathbb{Z}_p^\times$ denotes the p-adic cyclotomic character. Consider the following fields and the associated Galois groups:

$$\mathbb{Q}_\phi := \overline{\mathbb{Q}}^{\ker(\phi)}, \quad \mathbb{Q}_{\tilde{\phi}} := \overline{\mathbb{Q}}^{\ker(\tilde{\phi})}, \quad \mathbb{Q}_{\chi_\phi} := \overline{\mathbb{Q}}^{\ker(\chi_\phi)}, \quad \mathbb{Q}_{\chi_{\tilde{\phi}}} := \overline{\mathbb{Q}}^{\ker(\chi_{\tilde{\phi}})}.$$
$$\Delta_{\chi_\phi} := \mathrm{Gal}(\mathbb{Q}_{\chi_\phi}/\mathbb{Q}), \quad \Delta_{\chi_{\tilde{\phi}}} := \mathrm{Gal}(\mathbb{Q}_{\chi_{\tilde{\phi}}}/\mathbb{Q}).$$

Let G_ϕ and $G_{\tilde{\phi}}$ denote the p-Sylow subgroups of $\mathrm{Gal}(\mathbb{Q}_\phi/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}_{\tilde{\phi}}/\mathbb{Q})$ respectively. Note that the groups G_ϕ and $G_{\tilde{\phi}}$ are of order dividing p. Also note that the groups Δ_{χ_ϕ} and $\Delta_{\chi_{\tilde{\phi}}}$ are of order dividing $p-1$. One can view G_ϕ and $G_{\tilde{\phi}}$ as quotients of $\mathrm{Gal}(\mathbb{Q}_\phi/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}_{\tilde{\phi}}/\mathbb{Q})$, respectively, as well. We can consider the following field diagrams:



$G_\phi \cong \mathrm{Gal}(L_\phi/\mathbb{Q})$.

$G_{\tilde{\phi}} \cong \mathrm{Gal}(L_{\tilde{\phi}}/\mathbb{Q})$.

We will need to impose the following condition (similar to (1)):

(Non-DG) $L_\phi \cap \mathbb{Q}_\infty = \mathbb{Q}$.

As we shall see in Corollary 5.2, the condition given in (1) is automatically satisfied for $L_{\tilde{\phi}}$. That is, $L_{\tilde{\phi}} \cap \mathbb{Q}_\infty = \mathbb{Q}$. To verify (Non-DG) in practice, one can use, for example, Velu's formula ([50]) to explicitly find a generating polynomial for the field extension L_ϕ over $\mathbb{Q}$.

For our application, we shall consider the Selmer groups $\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi_\phi)}(L_{\phi,\infty})$ and $\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi_{\tilde{\phi}})}(L_{\tilde{\phi},\infty})$ whose Pontryagin duals are finitely generated torsion modules over the completed group rings $\Lambda[G_\phi]$ and $\Lambda[G_{\tilde{\phi}}]$ respectively. The Pontryagin dual of these Selmer groups are non-primitive Iwasawa modules; they can be denoted by $\mathfrak{X}_{\mathfrak{D}(\chi_\phi)}(L_{\phi,\infty})$ and $\mathfrak{X}_{\mathfrak{D}(\chi_{\tilde{\phi}})}(L_{\tilde{\phi},\infty})$, following the notations of the introduction. For this section, we will use the notation involving the Selmer group (instead of using the notations involving $\mathfrak{X}$).

The restriction of the group homomorphisms

$$\phi\,|_{G_\phi} \colon G_\phi \to \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times, \qquad \tilde{\phi}\,|_{G_{\tilde{\phi}}} \colon G_{\tilde{\phi}} \to \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times \tag{53}$$

allow us to consider the following ring homomorphisms:

$$\sigma_\phi : \Lambda[G_\phi] \to \left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)[[\Gamma]] \cong \frac{\Lambda}{(p^2)}, \qquad \sigma_{\tilde{\phi}} : \Lambda[G_{\tilde{\phi}}] \to \left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)[[\Gamma]] \cong \frac{\Lambda}{(p^2)}. \tag{54}$$

As stated above, we shall work with the following assumption:

The even character χ_ϕ is ramified at p.

Keep in mind that the elliptic curve E has either good ordinary reduction or split multiplicative reduction at p. As a result, the semi-simplification of the $\mathbb{F}_p[I_p]$-representation $E[p]$ is a sum of two distinct characters; one of which coincides with the Teichmüller character (which is ramified at p) and one of which is trivial. Here, $E[p]$ denotes the p-power torsion points on the elliptic curve E and I_p denotes the inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. So, our assumption on the even character is valid if and only if we place the following assumption on the odd character:

The odd character $\chi_{\tilde{\phi}}$ is unramified at p.

Lemma 5.1. *The action of* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ *on* $\ker(\Phi)$ *is totally ramified. The action of* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ *on* $\ker\left(\tilde{\Phi}\right)$ *is unramified. In fact, we have the following isomorphism of* $\frac{\mathbb{Z}}{p^2\mathbb{Z}}[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$*-modules:*

$$\mathfrak{A}[p^2] \cong \ker\left(\tilde{\Phi}\right).$$

Proof. Observe that the semi-simplification of the $\frac{\mathbb{Z}}{p^2\mathbb{Z}}[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$-module $E[p^2]$ is the direct sum

$$\ker(\Phi) \oplus \ker\left(\tilde{\Phi}\right).$$

Our assumptions tell us that the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $\ker\left(\tilde{\Phi}\right)[p]$ is unramified and the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $\ker(\Phi)[p]$ is ramified. The natural surjection $E[p^2] \twoheadrightarrow \mathfrak{A}[p^2]$ of free $\frac{\mathbb{Z}}{p^2\mathbb{Z}}$-modules, that is $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-equivariant, tells us that $\mathfrak{A}[p^2]$ is one of the components appearing in the semi-simplification of $E[p^2]$ over $\frac{\mathbb{Z}}{p^2\mathbb{Z}}[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$. Since the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\overline{\mathbb{Q}}_p)$ on $\mathfrak{A}[p]$ is unramified, we must have the following isomorphism of $\frac{\mathbb{Z}}{p^2\mathbb{Z}}[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$-modules:

$$\mathfrak{A}[p^2] \cong \ker(\tilde{\Phi}),$$

The fact that the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $\ker(\Phi)$ is totally ramified now follows from equality of characters obtained in (52) using the Weil pairing. □

As an immediate corollary to Lemma 5.1 (in particular, since the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $\ker\left(\tilde{\Phi}\right)$ is unramified), we have the following corollary:

Corollary 5.2. $L_{\tilde{\phi}} \cap \mathbb{Q}_\infty = \mathbb{Q}$.

The hypotheses of Theorems 3 and 2 are satisfied for the $\Lambda[G_\phi]$-module $\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi_\phi)}(L_{\phi,\infty})^\vee$ and the $\Lambda[G_{\tilde{\phi}}]$-module $\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi_{\tilde{\phi}})}(L_{\tilde{\phi},\infty})^\vee$. They let us deduce

that we have the following short exact sequences of $\Lambda[G_\phi]$-modules and $\Lambda[G_{\tilde{\phi}}]$-modules respectively:

$$\begin{aligned} &0 \to \Lambda[G_\phi]^n \xrightarrow{A_\phi} \Lambda[G_\phi]^n \to \mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi_\phi)}(L_{\phi,\infty})^\vee \to 0, \qquad && A_\phi \in M_n\left(\Lambda[G_\phi]\right). \\ &0 \to \Lambda[G_{\tilde{\phi}}]^m \xrightarrow{A_{\tilde{\phi}}} \Lambda[G_{\tilde{\phi}}]^m \to \mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi_{\tilde{\phi}})}(L_{\tilde{\phi},\infty})^\vee \to 0, \qquad && A_{\tilde{\phi}} \in M_m\left(\Lambda[G_{\tilde{\phi}}]\right). \end{aligned} \tag{55}$$

One can naturally view Λ as a subring of $\Lambda[G_\phi]$ and $\Lambda[G_{\tilde{\phi}}]$. Since the groups G_ϕ and $G_{\tilde{\phi}}$ are finite, the ring extensions $\Lambda \hookrightarrow \Lambda[G_{\tilde{\phi}}]$ and $\Lambda \hookrightarrow \Lambda[G_{\tilde{\phi}}]$ are integral. One has the following natural maps:

$$\Lambda \hookrightarrow \Lambda[G_\phi] \xrightarrow{\sigma_\phi} \frac{\Lambda}{(p^2)}, \qquad \Lambda \hookrightarrow \Lambda[G_{\tilde{\phi}}] \xrightarrow{\sigma_{\tilde{\phi}}} \frac{\Lambda}{(p^2)}. \tag{56}$$

The rings $\mathbb{Z}_p[G_\phi]$ and $\mathbb{Z}_p[G_{\tilde{\phi}}]$ are local rings, each of which has a unique maximal ideal containing p. The ring $\frac{\Lambda}{(p^2)}$ has a unique minimal prime ideal (which corresponds to the prime ideal (p) in the ring Λ and the prime ideal lying above (p) in $\Lambda[G_\phi]$ and $\Lambda[G_{\tilde{\phi}}]$ respectively). Since the fields L_ϕ and $L_{\tilde{\phi}}$ are abelian over $\mathbb{Q}$, a theorem of Ferrero and Washington ([10]) asserts that the μ-invariants of the Λ-modules $\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi_\phi)}(L_{\phi,\infty})^\vee$ and $\mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi_{\tilde{\phi}})}(L_{\tilde{\phi},\infty})^\vee$ equal zero. As a result, $\det\left(A_\phi\right)$ and $\det\left(A_{\tilde{\phi}}\right)$ do not belong to the prime ideal lying above (p) in the rings $\Lambda[G_\phi]$ and $\Lambda[G_{\tilde{\phi}}]$ respectively. Note that every zero-divisor in the ring $\frac{\Lambda}{(p^2)}$ is also nilpotent. So, the elements $\det\left(\sigma_\phi\left(A_\phi\right)\right)$ and $\det\left(\sigma_{\tilde{\phi}}\left(A_{\tilde{\phi}}\right)\right)$ in the ring $\frac{\Lambda}{(p^2)}$ are non-zero divisors. By applying Proposition 6 in Chapter III, §8 of [3], one can conclude that tensoring the short exact sequences in (55) with $\frac{\Lambda}{(p^2)}$, via the maps σ_ϕ and $\sigma_{\tilde{\phi}}$ respectively, will give us the following short exact sequences:

$$\begin{aligned} &0 \to \left(\frac{\Lambda}{(p^2)}\right)^n \xrightarrow{\sigma_\phi(A_\phi)} \left(\frac{\Lambda}{(p^2)}\right)^n \to \mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi_\phi)}(L_{\phi,\infty})^\vee \otimes_{\Lambda[G_\phi]} \frac{\Lambda}{(p^2)} \to 0. \\ &0 \to \left(\frac{\Lambda}{(p^2)}\right)^m \xrightarrow{\sigma_{\tilde{\phi}}(A_{\tilde{\phi}})} \left(\frac{\Lambda}{(p^2)}\right)^m \to \mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi_{\tilde{\phi}})}(L_{\tilde{\phi},\infty})^\vee \otimes_{\Lambda[G_{\tilde{\phi}}]} \frac{\Lambda}{(p^2)} \to 0. \end{aligned} \tag{57}$$

In a rather ad-hoc manner, we define the following Selmer groups (which, as one observes, turn out to be $\frac{\Lambda}{(p^2)}$-modules):

$$\begin{aligned} \mathrm{Sel}^{\Sigma_0}_{\ker(\Phi)}(\mathbb{Q}_\infty) &:= H^1\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty), \ker(\Phi)\right), \\ \mathrm{Sel}^{\Sigma_0}_{\ker(\tilde{\Phi})}(\mathbb{Q}_\infty) &:= \ker\left(H^1\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty), \ker(\tilde{\Phi})\right) \to H^1(I_\eta, \ker(\tilde{\Phi}))\right). \end{aligned}$$

Here, η denotes the unique prime in $\mathbb{Q}_\infty$ lying above p and I_η denotes the corresponding inertia subgroup. We now state a "control theorem".

Proposition 5.3. *We have the following isomorphism of $\frac{\Lambda}{(p^2)}$-modules:*

$$\mathrm{Sel}^{\Sigma_0}_{\ker(\Phi)}(\mathbb{Q}_\infty)^\vee \cong \mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}(\chi_\phi)}\left(L_{\phi,\infty}\right)^\vee \otimes_{\Lambda[G_\phi]} \frac{\Lambda}{(p^2)}, \tag{58}$$

$$\mathrm{Sel}^{\Sigma_0}_{\ker\left(\tilde{\Phi}\right)}(\mathbb{Q}_\infty)^\vee \cong \mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}\left(\chi_{\tilde{\phi}}\right)}\left(L_{\tilde{\phi},\infty}\right)^\vee \otimes_{\Lambda[G_{\tilde{\phi}}]} \frac{\Lambda}{(p^2)}. \tag{59}$$

Proof. We will show that equation (59) holds. The validity of equation (58) follows similarly. Let us choose a generator, say $g_{\tilde{\phi}}$, of the cyclic group $G_{\tilde{\phi}}$. Let ϑ equal the element $g_{\tilde{\phi}} - \sigma_{\tilde{\phi}}(g_{\tilde{\phi}})$ in the ring $\Lambda[G_{\tilde{\phi}}]$. One can easily show that ϑ generates the ideal $\ker\left(\sigma_{\tilde{\phi}}\right)$. To prove (59), one needs to establish the following isomorphism:

$$\mathrm{Sel}^{\Sigma_0}_{\ker\left(\tilde{\Phi}\right)}(\mathbb{Q}_\infty) \overset{?}{\cong} \mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}\left(\chi_{\tilde{\phi}}\right)}(L_{\tilde{\phi},\infty})[\vartheta].$$

Consider the tautological character $\kappa : \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty) \twoheadrightarrow \mathrm{Gal}(L_{\tilde{\phi},\infty}/\mathbb{Q}_\infty) \cong G_{\tilde{\phi}} \hookrightarrow \mathrm{GL}_1\left(\mathbb{Z}_p[G_{\tilde{\phi}}]\right)$. We obtain the following short exact sequence of $\mathbb{Z}_p[G_{\tilde{\phi}}]$-modules that is $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$-equivariant:

$$0 \to \mathbb{Z}_p[G_{\tilde{\phi}}]\left(\kappa^{-1}\chi_{\tilde{\phi}}^{-1}\right) \xrightarrow{\vartheta} \mathbb{Z}_p[G_{\tilde{\phi}}]\left(\kappa^{-1}\chi_{\tilde{\phi}}^{-1}\right) \to \frac{\mathbb{Z}}{p^2\mathbb{Z}}\left(\tilde{\phi}^{-1}\right) \to 0. \tag{60}$$

Here, $\mathbb{Z}_p[G_{\tilde{\phi}}]\left(\kappa^{-1}\chi_{\tilde{\phi}}^{-1}\right)$ denotes a free $\mathbb{Z}_p[G_{\tilde{\phi}}]$-module of rank 1 on which $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$ acts via the character $\kappa^{-1}\chi_{\tilde{\phi}}^{-1}$. Note that the group $G_{\tilde{\phi}}$ is isomorphic to the quotient $\frac{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}{\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty})}$. Let us keep in mind the following isomorphisms that are $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$-invariant:

$$\begin{aligned}
\mathrm{Ind}_{\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty})}^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}\left(\frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right) &\cong \frac{\mathbb{Q}_p[G_{\tilde{\phi}}]\left(\kappa\chi_{\tilde{\phi}}\right)}{\mathbb{Z}_p[G_{\tilde{\phi}}]\left(\kappa\chi_{\tilde{\phi}}\right)} \\
&\cong \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G_{\tilde{\phi}}]\left(\kappa\chi_{\tilde{\phi}}\right) \\
&\cong \mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p, \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G_{\tilde{\phi}}]\left(\kappa\chi_{\tilde{\phi}}\right) \\
&\cong \mathrm{Hom}_{\mathbb{Z}_p[G_{\tilde{\phi}}]}\left(\mathbb{Z}_p[G_{\tilde{\phi}}], \frac{\mathbb{Q}_p[G_{\tilde{\phi}}]}{\mathbb{Z}_p[G_{\tilde{\phi}}]}\right)\left(\kappa\chi_{\tilde{\phi}}\right) \\
&\cong \mathrm{Hom}_{\mathbb{Z}_p}\left(\mathbb{Z}_p[G_{\tilde{\phi}}]\left(\kappa^{-1}\chi_{\tilde{\phi}}^{-1}\right), \frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right).
\end{aligned}$$

The fourth isomorphism follows from Theorem 7.11 in Matsumura's book [33]. The last isomorphism follows since $\mathrm{Ind}_{\{1\}}^{G_{\tilde{\phi}}}$ is right adjoint to $\mathrm{Res}_{\{1\}}^{G_{\tilde{\phi}}}$.

Considering the Pontryagin duals of all the modules appearing in the exact sequence (60), we obtain the following exact sequence of discrete modules that is $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$-equivariant:

$$\ker\left(\tilde{\Phi}\right) \hookrightarrow \mathrm{Ind}_{\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty})}^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}\left(\frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right) \xrightarrow{\vartheta} \mathrm{Ind}_{\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty})}^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}\left(\frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right). \quad (61)$$

Let $G_{\Sigma,\infty}$ denote $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$. Shapiro's Lemma along with the observations that $\chi_{\tilde{\phi}}$ is odd and $L_{\tilde{\phi},\infty}$ is a totally real field, tells us that

$$\begin{aligned} H^0\left(G_{\Sigma,\infty}, \mathrm{Ind}_{\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty})}^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}\left(\frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right)\right) &\cong H^0\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty}), \frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right) \\ &= 0. \\ H^1\left(G_{\Sigma,\infty}, \mathrm{Ind}_{\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty})}^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}\left(\frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right)\right) &\cong H^1\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty}), \frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right). \end{aligned} \quad (62)$$

Let η be the unique prime in $\mathbb{Q}_\infty$ lying above p. Observe that since the extension $L_{\tilde{\phi},\infty}/\mathbb{Q}_\infty$ is abelian of order p, there either exists exactly one prime or p distinct primes in the field $L_{\tilde{\phi},\infty}$ lying above η. The extension must be unramified by Lemma 5.1. Using Shapiro's lemma, we obtain the following isomorphism:

$$H^1\left(I_\eta,\ \mathrm{Ind}_{\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty})}^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}\left(\frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right)\right) \cong \begin{cases} \bigoplus\limits_{\omega_i|\eta} H^1\left(I_{\omega_i}, \frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right), \\ \qquad \text{if } \eta \text{ splits completely.} \\ \bigoplus\limits_{p \text{ copies}} H^1\left(I_\omega, \frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right), \\ \qquad \text{if } \omega \mid \eta \text{ remains inert.} \end{cases} \quad (63)$$

The discussions in section 4.2 (in particular, see Observation 4.6) also tell us that $H^0\left(I_\omega, \frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right)$ is either 0 or isomorphic to $\frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ as a group, for each $\omega \mid \eta$. In either case, it is a divisible group. As a result, using Shapiro's lemma, one can conclude that $H^0\left(I_\eta,\ \mathrm{Ind}_{\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty})}^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}\left(\frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right)\right)$ is also a divisible group. Since the kernel of the map

$$H^0\left(I_\eta, \mathrm{Ind}_{\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty})}^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}\left(\frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right)\right) \xrightarrow{\vartheta} H^0\left(I_\eta, \mathrm{Ind}_{\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty})}^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}\left(\frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right)\right)$$

being a subgroup of $\ker\left(\tilde{\Phi}\right)$, is finite, the map must also be surjective. Consider the long exact sequence in group cohomology obtained from the short exact

sequence (61), for both groups $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$ and I_η. Combining our various observations lets us obtain the following commutative diagram:

$$\begin{array}{ccc} H^1\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty), \ker\left(\tilde{\Phi}\right)\right) & \xrightarrow{\cong} & H^1\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty}), \frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right)[\vartheta] \\ \downarrow & & \downarrow \\ H^1\left(I_\eta, \ker\left(\tilde{\Phi}\right)\right) & \xrightarrow{\cong} & H^1\left(I_\eta,\ \mathrm{Ind}_{\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty})}^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}\left(\frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right)\right)[\vartheta] \end{array}$$

Considering the kernels of the vertical maps and the description of $H^1\left(I_\eta,\ \mathrm{Ind}_{\mathrm{Gal}(\mathbb{Q}_\Sigma/L_{\tilde{\phi},\infty})}^{\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)}\left(\frac{\mathbb{Q}_p(\chi_{\tilde{\phi}})}{\mathbb{Z}_p(\chi_{\tilde{\phi}})}\right)\right)$ given in (63), we obtain the desired isomorphism

$$\mathrm{Sel}^{\Sigma_0}_{\ker\left(\tilde{\Phi}\right)}(\mathbb{Q}_\infty) \cong \mathrm{Sel}^{\Sigma_0}_{\mathfrak{D}\left(\chi_{\tilde{\phi}}\right)}(L_{\tilde{\phi},\infty})[\vartheta].$$

The proposition follows. □

We will now recall some results of Greenberg-Vatsal [24] concerning $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)$. Note that a finitely generated module over a 2-dimensional regular local ring has no non-trivial pseudo-null submodules if and only if its projective dimension is less than or equal to 1. The following proposition is proved in [24]:

Proposition 5.4 (Proposition 2.5 in [24]). *The* Λ*-module* $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee$ *has no non-zero pseudo-null submodules. As a result,*

$$proj\ dim_\Lambda\left(\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee\right) \leq 1.$$

Note that over a commutative local ring, every finitely generated projective module is free. We can consider a free resolution of $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee$ as a Λ-module:

$$0 \to \Lambda^r \xrightarrow{A_E} \Lambda^r \to \mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty) \to 0. \tag{64}$$

Here, A_E is an $r \times r$ matrix with entries in Λ. Note that the characteristic ideal $\mathrm{Char}_\Lambda\left(\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee\right)$ equals the ideal generated by $\det(A_E)$ in Λ. By Proposition 5.10 in Greenberg's work [17], the μ-invariant of the Λ-module $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee$ is zero. So, the prime number p, viewed as an irreducible in the regular local ring Λ, does not divide $\det(A_E)$. We have the following natural ring homomorphism:

$$\sigma_{p^2} : \Lambda \to \frac{\Lambda}{(p^2)}.$$

By applying Proposition 6 in Chapter III, §8 of [3] as we did earlier, one can conclude that tensoring the short exact sequence (64) with $\frac{\Lambda}{(p^2)}$ gives us the following short exact sequence:

$$0 \to \left(\frac{\Lambda}{(p^2)}\right)^r \xrightarrow{\sigma_{p^2}(A_E)} \left(\frac{\Lambda}{(p^2)}\right)^r \to \mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee \otimes_\Lambda \frac{\Lambda}{(p^2)} \to 0. \tag{65}$$

Once again, in a rather ad-hoc manner, we define a Selmer group $\mathrm{Sel}^{\Sigma_0}_{E[p^2]}(\mathbb{Q}_\infty)$ for the Galois module $E[p^2]$ over $\mathbb{Q}_\infty$. It turns out to be a module over the ring $\frac{\Lambda}{(p^2)}$.

$$\mathrm{Sel}^{\Sigma_0}_{E[p^2]}(\mathbb{Q}_\infty) := \ker\left(H^1\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty), E[p^2]\right) \to H^1(I_\eta, \mathfrak{A}[p^2])^{G_\eta/I_\eta}\right).$$

Note that if E has good ordinary reduction at p, then $\mathfrak{A}[p^2]$ is isomorphic to $\overline{E}[p^2]$, the p^2-torsion points on the reduced elliptic curve $\overline{E}$. If E has split multiplicative reduction at p, then $\mathfrak{A}[p^2]$ is isomorphic to $\frac{\mathbb{Z}}{p^2\mathbb{Z}}$ with the trivial action of $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$. The following "control theorem" is essentially proved in the work of Greenberg and Vatsal [24], relating the $\frac{\Lambda}{(p^2)}$-module $\mathrm{Sel}^{\Sigma_0}_{E[p^2]}(\mathbb{Q}_\infty)^\vee$ with the $\frac{\Lambda}{(p^2)}$-module $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee \otimes_\Lambda \frac{\Lambda}{(p^2)}$:

PROPOSITION 5.5 (Proposition 2.8 in [24]). *We have the following isomorphism of $\frac{\Lambda}{(p^2)}$-modules:*

$$\mathrm{Sel}^{\Sigma_0}_{E[p^2]}(\mathbb{Q}_\infty)^\vee \cong \mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee \otimes_\Lambda \frac{\Lambda}{(p^2)}. \tag{66}$$

5.2 PROOF OF THEOREM 4

We would like to prove the following theorem stated in the introduction:

THEOREM 4. *Suppose the even character χ_ϕ is ramified at p. Suppose the condition (Non-DG) holds. We have the following equality of ideals in $\frac{\Lambda}{(p^2)}$:*

$$\sigma_{p^2}\left(\mathrm{Char}_\Lambda\left(\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee\right)\right) = \sigma_\phi\left(\left(\det\left(A_\phi\right)\right)\right)\sigma_{\tilde{\phi}}\left(\left(\det\left(A_{\tilde{\phi}}\right)\right)\right). \tag{4}$$

Proof. Recall, from the introduction, that we have the following short exact sequence of modules over $\frac{\mathbb{Z}}{p^2\mathbb{Z}}$ that is $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$-equivariant:

$$0 \to \ker(\Phi) \to E[p^2] \to \ker\left(\tilde{\Phi}\right) \to 0.$$

Let $G_{\Sigma,\infty}$ denote $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$. Consider the long exact sequence in group cohomology, for both $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$ and I_η (here once again, η is the unique

prime above p in $\mathbb{Q}_\infty$). We have the following commutative diagram whose rows are exact:

$$\begin{array}{ccccc} H^1\left(G_{\Sigma,\infty}, \ker(\Phi)\right) & \hookrightarrow & H^1\left(G_{\Sigma,\infty}, E[p^2]\right) & \twoheadrightarrow & H^1\left(G_{\Sigma,\infty}, \ker\left(\tilde{\Phi}\right)\right) \\ & & \downarrow & & \downarrow \\ & & H^1\left(I_\eta, \mathfrak{A}[p^2]\right) & \xrightarrow{\cong} & H^1\left(I_\eta, \ker\left(\tilde{\Phi}\right)\right) \end{array}$$

To see why the top row is exact, it suffices to show that (i) $H^0\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty), \ker\left(\tilde{\Phi}\right)\right) = 0$ and (ii) $H^2\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty), \ker(\Phi)\right) = 0$. The first assertion follows from our assumption that the character $\tilde{\phi}$ is odd. For the second assertion, notice that one obtains an exact sequence,

$$H^2\left(G_{\Sigma,\infty}, \ker(\Phi)[p]\right) \to H^2\left(G_{\Sigma,\infty}, \ker(\Phi)\right) \to H^2\left(G_{\Sigma,\infty}, \ker(\Phi)[p]\right),$$

as part of the long exact sequence in group cohomology (for the group $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$) using the short exact sequence $0 \to \ker(\Phi)[p] \to \ker(\Phi) \to \ker(\Phi)[p] \to 0$; the existence of this short exact sequence uses the fact that $\ker(\Phi)$ is cyclic. The arguments given on Page 30 in the work of Greenberg and Vatsal [24] establish that $H^2\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty), \ker(\Phi)[p]\right)$ equals zero. This forces $H^2\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty), \ker(\Phi)\right)$ to equal zero too.

As for the bottom row in the commutative diagram above, it turns out that, by Lemma 5.1, $\mathfrak{A}[p^2] \cong \ker\left(\tilde{\Phi}\right)$, as modules for the group ring $\frac{\mathbb{Z}}{p^2\mathbb{Z}}[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$ (and hence for the action of inertia subgroup I_η of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p,\infty})$ too).

Considering the Snake Lemma for the commutative diagram given earlier, we obtain the short exact sequence $0 \to \mathrm{Sel}^{\Sigma_0}_{\ker(\Phi)}(\mathbb{Q}_\infty) \to \mathrm{Sel}^{\Sigma_0}_{E[p^2]}(\mathbb{Q}_\infty) \to \mathrm{Sel}^{\Sigma_0}_{\ker(\tilde{\Phi})} \to 0$. Taking Pontryagin duals, we obtain the following short exact sequence of $\frac{\Lambda}{(p^2)}$-modules:

$$0 \to \mathrm{Sel}^{\Sigma_0}_{\ker(\tilde{\Phi})}(\mathbb{Q}_\infty)^\vee \to \mathrm{Sel}^{\Sigma_0}_{E[p^2]}(\mathbb{Q}_\infty)^\vee \to \mathrm{Sel}^{\Sigma_0}_{\ker(\ker(\Phi))}(\mathbb{Q}_\infty)^\vee \to 0. \tag{67}$$

By (57) and (65), all the $\frac{\Lambda}{(p^2)}$-modules, appearing in (67), have projective dimensions less than or equal to one. Using Lemma 3 in [7], we have the following equality of (first) Fitting ideals in $\frac{\Lambda}{(p^2)}$:

$$\mathrm{Fitt}\left(\mathrm{Sel}^{\Sigma_0}_{E[p^2]}(\mathbb{Q}\infty)^\vee\right) = \mathrm{Fitt}\left(\mathrm{Sel}^{\Sigma_0}_{\ker(\Phi)}(\mathbb{Q}_\infty)^\vee\right) \mathrm{Fitt}\left(\mathrm{Sel}^{\Sigma_0}_{\ker(\tilde{\Phi})}(\mathbb{Q}_\infty)^\vee\right). \tag{68}$$

Using (57) and (65), we have the following equality of (first) Fitting ideals in $\frac{\Lambda}{(p^2)}$:

$$\begin{aligned}
\text{Fitt}\left(\text{Sel}^{\Sigma_0}_{E[p^2]}(\mathbb{Q}_\infty)^\vee\right) &= \sigma_{p^2}\left(\text{Char}_\Lambda\left(\text{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee\right)\right),\\
\text{Fitt}\left(\text{Sel}^{\Sigma_0}_{\ker(\Phi)}(\mathbb{Q}_\infty)^\vee\right) &= \sigma_{\phi}\left(\left(\det\left(A_\phi\right)\right)\right),\\
\text{Fitt}\left(\text{Sel}^{\Sigma_0}_{\ker(\tilde{\Phi})}(\mathbb{Q}_\infty)^\vee\right) &= \sigma_{\tilde{\phi}}\left(\left(\det\left(A_{\tilde{\phi}}\right)\right)\right). \qquad (69)
\end{aligned}$$

Combining (68) and (69), we obtain the following equality of ideals in $\frac{\Lambda}{(p^2)}$:

$$\sigma_{p^2}\left(\text{Char}_\Lambda\left(\text{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee\right)\right) = \sigma_{\phi}\left(\left(\det\left(A_\phi\right)\right)\right)\sigma_{\tilde{\phi}}\left(\left(\det\left(A_{\tilde{\phi}}\right)\right)\right). \quad (70)$$

This completes the proof of Theorem 4. □

ACKNOWLEDGEMENTS

Both authors thank Ralph Greenberg for his guidance in graduate school, and for his steadfast encouragement to write this paper. The second author thanks Ted Chinburg for indicating to him the works of Reiner and Ullom. We also thank Andreas Nickel for many helpful comments. We are also grateful to the anonymous referees for their feedback and providing many thoughtful suggestions.

REFERENCES

[1] M. Auslander and O. Goldman. Maximal orders. Trans. Amer. Math. Soc., 97:1–24, 1960.

[2] D. Barsky. Fonctions zeta p-adiques d'une classe de rayon des corps de nombres totalement réels. In Groupe d'Etude d'Analyse Ultramétrique (5e année: 1977/78), pages Exp. No. 16, 23. Secrétariat Math., Paris, 1978.

[3] N. Bourbaki. Elements of mathematics. Algebra, Part I: Chapters 1-3. Hermann, Paris; Addison-Wesley Publishing Co., Reading Mass., 1974. Translated from the French.

[4] P. Cassou-Noguès. p-adic L-functions for totally real number field. In Proceedings of the Conference on p-adic Analysis (Nijmegen, 1978), volume 7806 of Report, pages 24–37. Katholieke Univ., Nijmegen, 1978.

[5] J. Coates, T. Fukaya, K. Kato, R. Sujatha, and O. Venjakob. The GL_2 main conjecture for elliptic curves without complex multiplication. Publ. Math. Inst. Hautes Études Sci., (101):163–208, 2005.

[6] P. M. Cohn. Free ideal rings and localization in general rings, volume 3 of New Mathematical Monographs. Cambridge University Press, Cambridge, 2006.

[7] P. Cornacchia and C. Greither. Fitting ideals of class groups of real fields with prime power conductor. J. Number Theory, 73(2):459–471, 1998.

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

[9] D. Eisenbud. Commutative algebra, volume 150 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[10] B. Ferrero and L. C. Washington. The Iwasawa invariant μ_p vanishes for abelian number fields. Ann. of Math. (2), 109(2):377–395, 1979.

[11] A. Fröhlich. Local fields. In Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), pages 1–41. Thompson, Washington, DC, 1967.

[12] T. Fukaya and K. Kato. A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory. In Proceedings of the St. Petersburg Mathematical Society. Vol. XII, volume 219 of Amer. Math. Soc. Transl. Ser. 2, pages 1–85. Amer. Math. Soc., Providence, RI, 2006.

[13] K. R. Goodearl and R. B. Warfield, Jr. An introduction to noncommutative Noetherian rings, volume 61 of London Mathematical Society Student Texts. Cambridge University Press, Cambridge, second edition, 2004.

[14] R. Greenberg. On p-adic L-functions and cyclotomic fields. II. Nagoya Math. J., 67:139–158, 1977.

[15] R. Greenberg. On p-adic Artin L-functions. Nagoya Math. J., 89:77–87, 1983.

[16] R. Greenberg. Iwasawa theory for p-adic representations. Advanced Studies in Pure Math., 17:97–137, 1989.

[17] R. Greenberg. Iwasawa theory for elliptic curves. In Arithmetic theory of elliptic curves (Cetraro, 1997), volume 1716 of Lecture Notes in Math., pages 51–144. Springer, Berlin, 1999.

[18] R. Greenberg. Introduction to Iwasawa theory for elliptic curves. In Arithmetic algebraic geometry (Park City, UT, 1999), volume 9 of IAS/Park City Math. Ser., pages 407–464. Amer. Math. Soc., Providence, RI, 2001.

[19] R. Greenberg. On the structure of certain Galois cohomology groups. Doc. Math., (Extra Vol.):335–391 (electronic), 2006.

[20] R. Greenberg. Surjectivity of the global-to-local map defining a Selmer group. Kyoto J. Math., 50(4):853–888, 2010.

[21] R. Greenberg. Iwasawa Theory, projective modules, and modular representations. Mem. Amer. Math. Soc., no. 992, 2011. Available at http://www.math.washington.edu/~greenber/NewMod.pdf.

[22] R. Greenberg. On p-adic Artin L-functions. II. In Iwasawa Theory 2012, pages 227–245. Springer, 2014.

[23] R. Greenberg. On the Structure of Selmer Groups. In Elliptic Curves, Modular Forms and Iwasawa Theory: In Honour of John H. Coates' 70th Birthday, Cambridge, UK, March 2015, pages 225–252. Springer International Publishing, 2016.

[24] R. Greenberg and V. Vatsal. On the Iwasawa invariants of elliptic curves. Inventiones Mathematicae, 142(1):17–63, 2000. Available at http://www.math.washington.edu/~greenber/IWINV.ps.

[25] H. Hida. Modular forms and Galois cohomology, volume 69 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2000.

[26] Y. Hirano. Congruences of Hilbert modular forms over real quadratic fields and the special values of L-functions: an announcement. In Algebraic number theory and related topics 2013, RIMS Kôkyûroku Bessatsu, B53, pages 65–86. Res. Inst. Math. Sci. (RIMS), Kyoto, 2015.

[27] K. Iwasawa. On $\mathbf{Z}_l$-extensions of algebraic number fields. Ann. of Math. (2), 98:246–326, 1973.

[28] N. Jacobson. The Theory of Rings. American Mathematical Society Mathematical Surveys, vol. II. American Mathematical Society, New York, 1943.

[29] H. Johnston and A. Nickel. Hybrid Iwasawa algebras and the equivariant Iwasawa main conjecture. Amer. J. Math., 140(1):245–276, 2018.

[30] M. Kakde. The main conjecture of Iwasawa theory for totally real fields. Invent. Math., 193(3):539–626, 2013.

[31] Y. Kida. l-extensions of CM-fields and cyclotomic invariants. J. Number Theory, 12(4):519–528, 1980.

[32] T. Y. Lam. A first course in noncommutative rings, volume 131 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 2001.

[33] H. Matsumura. Commutative ring theory, volume 8 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[34] J. C. McConnell and J. C. Robson. Noncommutative Noetherian rings, volume 30 of Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, revised edition, 2001. With the cooperation of L. W. Small.

[35] T. Nakayama and Y. Matsushima. Über die multiplikative Gruppe einer p-adischen Divisionsalgebra. Proc. Imp. Acad. Tokyo, 19:622–628, 1943.

[36] J. Neukirch, A. Schmidt, and K. Wingberg. Cohomology of number fields, volume 323 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, second edition, 2008.

[37] A. Nichifor. Iwasawa theory for elliptic curves with cyclic isogenies. PhD thesis, University of Washington, 2004. Available at http://www.math.washington.edu/~nichifor/Thesis.pdf.

[38] A. Nickel. On the equivariant Tamagawa number conjecture in tame CM-extensions. Math. Z., 268(1-2):1–35, 2011.

[39] A. Nickel. On the equivariant Tamagawa number conjecture in tame CM-extensions, II. Compos. Math., 147(4):1179–1204, 2011.

[40] R. Oliver. Whitehead groups of finite groups, volume 132 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1988.

[41] V. P. Platonov. Algebraic groups and reduced K-theory. In Proceedings of the International Congress of Mathematicians (Helsinki, 1978), pages 311–317. Acad. Sci. Fennica, Helsinki, 1980.

[42] M. Ramras. Maximal orders over regular local rings of dimension two. Trans. Amer. Math. Soc., 142:457–479, 1969.

[43] I. Reiner. Maximal orders. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1975. London Mathematical Society Monographs, No. 5.

[44] I. Reiner and S. Ullom. Class groups of integral group rings. Trans. Amer. Math. Soc., 170:1–30, 1972.

[45] I. Reiner and S. Ullom. A Mayer-Vietoris sequence for class groups. J. Algebra, 31:305–342, 1974.

[46] J. Ritter and A. Weiss. Toward equivariant Iwasawa theory. Manuscripta Math., 109(2):131–146, 2002.

[47] J. Ritter and A. Weiss. Toward equivariant Iwasawa theory. II. Indag. Math. (N.S.), 15(4):549–572, 2004.

[48] J. Ritter and A. Weiss. On the "main conjecture" of equivariant Iwasawa theory. J. Amer. Math. Soc., 24(4):1015–1050, 2011.

[49] L. N. Vaserstein. On the Whitehead determinant for semi-local rings. J. Algebra, 283(2):690–699, 2005.

[50] J. Vélu. Isogénies entre courbes elliptiques. C. R. Acad. Sci. Paris Sér. A-B, 273:A238–A241, 1971.

[51] O. Venjakob. A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory. With an appendix by Denis Vogel. J. Reine Angew. Math., 559:153–191, 2003.

[52] C. A. Weibel. The K-book, volume 145 of Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2013. An introduction to algebraic K-theory.

[53] M. Witte. Non-Commutative Iwasawa Theory for Global Fields. Habilitation thesis, University of Heidelberg, 2017. Available at https://www.mathi.uni-heidelberg.de/∼witte/docs/....

Alexandra Nichifor
Department of Mathematics
University of Washington
Seattle WA 98195-4350
USA
nichifor@uw.edu

Bharathwaj Palvannan
Department of Mathematics
University of Pennsylvania
Philadelphia PA 19104-6395
USA
pbharath@math.upenn.edu