Trivial zeros in the Iwasawa main conjecture

Samit Dasgupta
Mahesh Kakde

April 21, 2021

Contents

1 Introduction

Fix a prime number p. Let F be a totally real field, ψ denote a totally even character of F and ω denote the Teichmüller character. The Iwasawa main conjecture in its simplest form is an equality up to units of two power series: a power series $G(T)$ constructed from the p-adic L-function $L_p(\psi, s)$ and the characteristic power series $f(T)$ of an Iwasawa module associated to $\chi = \psi^{-1}\omega$. An application of Iwasawa's analytic class number formula shows that it is enough to prove the divisibility of any one of these power series by the other. Wiles [19] proved the Iwasawa main conjecture building on the works [15,16] by showing that $G(T)$ divides $f(T)$. This amounts to constructing, for each zero of $G(T)$ with multiplicity m, an unramified extension of the field cut out by ψ of $\mathbf{Z}_p$-rank m with a specified Galois action.

Wiles requires special arguments to handle two kinds of zeros beyond the generic case. These are the Leopoldt zeros (which conjecturally do not exist) at $s = 1$ and trivial zeros (which do exist) at $s = 0$. For the Leopoldt zeroes, the argument in [19] in the generic case only gives an extension of rank δ, the Leopoldt defect, whereas the main conjecture requires an extension of rank $\delta + 1$. If $\delta > 0$, i.e. Leopoldt's conjecture fails, then there exists a non-cyclotomic $\mathbf{Z}_p$-extension of F. Wiles constructs the required extensions by twisting by

a sequence of characters of increasing p-power order along the non-cyclotomic $\mathbf{Z}_p$-extension and a suitable limiting process. Ventullo provided an alternate direct construction of these extensions in [17].

The purpose of this note is to give a direct construction of unramified abelian extensions corresponding to trivial zeros at $s = 0$ using ideas from our recent work [5], just as Ventullo did in the setting of Leopoldt zeros at $s = 1$. For simplicity, we restrict to a special case (see Theorem 2.3). Suppose there are r primes $\mathfrak{p}$ above p in F such that $\chi(\mathfrak{p}) = 1$. There is a direct arithmetic construction of extensions associated to such primes $\mathfrak{p}$. The Gross–Kuz'min conjecture predicts that these are all the extensions corresponding to the point $s = 0$. Wiles constructs all the extensions required for the main conjecture at $s = 0$ unconditionally, even if Gross–Kuz'min fails, using an ingenious method that is now often called "horizontal Iwasawa theory."

The general argument for proving the main conjecture using Ribet's method proceeds as follows: one proves that the p-adic L-function divides the congruence ideal by constructing a cusp form congruent to an Eisenstein series modulo the p-adic L-function. The second step is to prove that the congruence ideal divides the characteristic ideal by constructing cohomology classes with appropriate local properties. This approach does not work directly in the case of trivial zeroes. More precisely, the congruence ideal is strictly smaller and hence does not divide the characteristic ideal. This occurs because the cohomology classes constructed using the congruence ideal do not have the required local properties. This phenomenon also occurs in the work of Hida–Tilouine [13] on the anticyclotomic main conjecture and they give a separate proof for the trivial zeros. The difficulty in the construction of cohomology classes with prescribed local behaviour arises from "local p-indistinguishability" i.e. the Hecke eigenvalues at primes above p are equal.

Two observations make our direct construction of extensions corresponding to trivial zeros possible. Firstly, we use the construction of a cusp form from [4] that is a slightly refined version of the method in [19]. This allows for the definition of an Eisenstein homomorphism on the cuspidal Hida Hecke algebra in weight 1 as described in Theorem 4.1. Secondly, we take a larger module adjoining all $A_{\mathfrak{p}}/C_{\mathfrak{p}}$ to the usual module of $b(\sigma)$ (see Section §5 below) in which our cohomology class takes values. This allows us to show that the cohomology class is unramified everywhere.

This note is written for the proceedings of the International Colloquium on Arithmetic Geometry organised in January 2020 at TIFR, Mumbai. We thank the organisers for inviting us to this wonderful event.

2 The main conjecture

In this section we recall the main conjecture and state our result on trivial zeroes. Let p be a prime number. For any number field F, let F_{cyc} be the cyclotomic $\mathbf{Z}_p$-extension of F.

Let F be a totally real number field and let χ be a one dimensional Artin character of

F. Put F_χ for the field cut out by χ, so χ is a faithful character of $\mathrm{Gal}(F_\chi/F)$. Following Greenberg [11], we say that χ is of type W if $F_\chi \subset F_{\mathrm{cyc}}$ and of type S if $F_\chi \cap F_{\mathrm{cyc}} = F$. There are characters that are neither of type S or W but we do not need to consider such characters in this article.

We next assume that χ is of type S and that F_χ is a CM field. Put

$$q = \begin{cases} p & \text{if } p \text{ is odd} \\ 4 & \text{if } p = 2. \end{cases}$$

Let $H = F_\chi(\mu_q)$. Let L be the maximal unramified abelian pro-p-extension of H_{cyc}. Define $X = \mathrm{Gal}(L/H_{\mathrm{cyc}})$. This is a module for $\mathrm{Gal}(H_{\mathrm{cyc}}/F)$ under the usual conjugation action. Since χ is of type S, there is a decomposition

$$\mathrm{Gal}(H_{\mathrm{cyc}}/F) \cong \mathrm{Gal}(H/F) \times \mathrm{Gal}(F_{\mathrm{cyc}}/F).$$

Let E be a sufficiently large finite extension of $\mathbf{Q}_p$ containing the pth roots of 1 and all values of the character χ. Let $X^{(\chi)} \subset X \otimes E$ be the subspace on which the first factor $\mathrm{Gal}(H/F)$ acts via χ. Fix a topological generator γ of $\mathrm{Gal}(H_{\mathrm{cyc}}/H) \cong \mathrm{Gal}(F_{\mathrm{cyc}}/F)$. Let $f_\chi(T)$ be the characteristic polynomial of $\gamma - 1$ acting on $X^{(\chi)}$.

As in §1 let $\psi = \chi^{-1}\omega$. We recall the power series $G_\psi(T)$ interpolating L-values. Let $u \in \mathbf{Z}_p^*$ be such that $\gamma(\zeta) = \zeta^u$ for every $\zeta \in \mu_{p^\infty}$. Define

$$H_\psi(T) = \begin{cases} \psi(\gamma)(T+1) - 1 & \text{if } \psi \text{ is of type } W \\ 1 & \text{otherwise} \end{cases} \tag{1}$$

Then Cassou-Noguès [1] and Deligne–Ribet [8] proved that there exists a unique power series $G_\psi(T) \in \mathbf{Z}_p[\psi][[T]]$ such that

$$\frac{G_\psi(u^n - 1)}{H_\psi(u^n - 1)} = \prod_{\mathfrak{p} \in S_p} (1 - \psi\omega^{-n}(\mathfrak{p})\mathrm{N}\mathfrak{p}^{n-1}) L(\psi\omega^{-n}, 1-n), \tag{2}$$

for every positive integer n. The following theorem is proven in Wiles [19] (following Mazur–Wiles [15] in the case when $F = \mathbf{Q}$).

Theorem 2.1 (The main conjecture)**.** *We have the equality of ideals*

$$(f_\chi(T)) = (G_\psi(u(1+T)^{-1} - 1))$$

in $\mathbf{Z}_p[[T]] \otimes E$.

Iwasawa's interpretation of the analytic class number formula implies that it is enough to prove one inclusion for deducing the equality in the theorem. More precisely, If $n_\alpha(\chi)$ and

$m_\alpha(\chi)$ denote the multiplicity of the zero α of $f_\chi(T)$ and $G_\psi(u(T+1)^{-1}-1)$, respectively, then Iwasawa's formula gives

$$\sum_\chi n_\alpha(\chi) = \sum_\chi m_\alpha(\chi)$$

for fixed α and χ running through all odd characters of a fixed extension of F. Wiles proves the inclusion $(f_\chi(T)) \subset (G_\psi(u(1+T)-1))$, i.e. the inequality $n_\alpha(\chi) \geq m_\alpha(\chi)$ for all χ and all α. Wiles proves this by constructing, for every α and χ, a subspace of $X^{(\chi)}$ on which $\gamma - 1$ has characteristic polynomial $(T-\alpha)^{m_\alpha(\chi)}$.

If $\alpha \notin \{\zeta - 1 : \zeta \in \mu_{p^\infty}\}$ (trivial zeros) and $\alpha \neq u-1$ when $\chi = \omega$ (Leopoldt zeroes), then the inequality is proven in two steps. Firstly, it is proven that $m_\alpha(\chi)$ is bounded above by the order of the zero, $n'_\alpha(\chi)$, of the characteristic polynomial of $\gamma - 1$ acting on a "congruence ideal." Secondly, it is proven that $n'_\alpha(\chi)$ is bounded above by the $n_\alpha(\chi)$.

A result of Colmez [3] shows that Leopoldt's conjecture for F_χ and p is equivalent to the statement $m_{u-1}(\omega) = 0$. If Leopolodt's conjecture fails, then Wiles' general strategy described above only shows that $n_{u-1}(\omega) \geq m_{u-1}(\omega) - 1$. Wiles proves that $n_{u-1}(\omega) \geq m_{u-1}(\omega)$ using a suitable limiting process by twisting along the non-cyclotomic $\mathbf{Z}_p$-extension arising from the failure of Leopoldt's conjecture. A direct proof of the inequality is given by Ventullo [17] using the construction in [4].

The situation for trivial zeroes is similar. The quantity $m_{\zeta-1}(\chi)$ can in general be positive, as trivial zeros do exist. If r is the number of primes of F above p that split completely in F_χ, then the Gross–Kuz'min conjecture states that $m_{\zeta-1}(\chi) = r$. Furthermore, there is an arithmetic construction due to Coates–Lichtenbaum [2, Theorem 2.1] showing that $n_{\zeta-1}(\chi) \geq r$. However, without the Gross–Kuz'min conjecture, we cannot directly deduce that $n_{\zeta-1}(\chi) \geq m_{\zeta-1}(\chi)$.

The general strategy described above does not yield enough unramified extensions as the quantity $n'_{\zeta-1}(\chi)$ may be strictly greater than $n_{\zeta-1}(\chi)$. Wiles devised the method of horizontal Iwasawa theory to construct extensions corresponding to trivial zeros by twisting by characters of increasing p-power order.

In this note we explain the recent refinement of the Ribet–Wiles method in [5] for directly constructing unramified extensions corresponding to trivial zeros. This uses the refined construction of cusp forms given in [4]. To avoid unnecessary technicalities we restrict to "Case 1" in [7], i.e. there is a prime $\mathfrak{p}$ of F above p such that $\chi(\mathfrak{p}) \neq 1$. The same ideas work in other cases described in [7]. Furthermore, using the integral constructions of cusp forms given in [5] it should be possible to give a direct proof of the equivariant main conjecture without assuming $\mu = 0$ by these methods. We note that Johnston–Nickel [14] have already proved this result using Wiles's results and the strong Brumer–Stark conjecture proven in [5]. However, the simpler situation considered here best explains the idea behind our construction of unramified classes in the locally p-indistinguishable case.

The trivial zeros are zeros of the form $\alpha = \zeta - 1$ for $\zeta \in \mu_{p^\infty}$. As the following lemma shows, we may twist by characters of type W to assume that $\alpha = 0$.

Lemma 2.2. *Let ψ be a character of type S and ρ a character of type W. Put $\rho(\gamma) = \zeta^{-1}$. Then*

$$\mathrm{ord}_{T=\zeta-1}\, G_\psi(u(T+1)^{-1}-1) = \mathrm{ord}_{T=0}\, G_{\psi\rho}(u(T+1)^{-1}-1).$$
$$\mathrm{ord}_{T=\zeta-1}\, f_\chi(T) = \mathrm{ord}_{T=0}\, f_{\chi\rho}(T).$$

Proof. Note that

$$G_{\psi\rho}(T) = G_\psi(\zeta^{-1}(T+1)-1) = G_\psi(\zeta^{-1}(T-(\zeta-1))).$$

This proves the first claim. For the second claim see Greenberg [11, Proposition 3]. □

The lemma implies that it is enough to consider the order of the zero at $T = 0$. Our main result is a simplified proof of the following special case of Wiles' theorem.

Theorem 2.3. *Assume that there is a prime $\mathfrak{p}$ of F above p such that $\chi(\mathfrak{p}) \neq 1$. Then we have*

$$\mathrm{ord}_{T=0}\, f_\chi(T) \geq \mathrm{ord}_{T=0}\, G_\psi(u(T+1)^{-1}-1).$$

To prove the theorem it is enough to show that $X^{(\chi)}$ has a subspace on which $\gamma - 1$ has characteristic polynomial $T^{r_{\mathrm{an}}}$, where

$$r_{\mathrm{an}} = \mathrm{ord}_{T=0}\, G_\psi(u(T+1)^{-1}-1).$$

We need some notation: Let $\mathcal{O}_E$ be the ring of integers of E and put $\Lambda = \mathcal{O}_E[[T]]$. Let $\Lambda_{(1)} = \mathcal{O}_E[[T]]_{(T)}$ be the localization in "weight 1". Recall the Λ-adic cyclotomic character $\varepsilon : G_F \to \Lambda^*$ given by

$$\varepsilon(\sigma) = (1+T)^{\log_p \langle \epsilon_{\mathrm{cyc}}(\sigma)\rangle / \log_p u},$$

where ϵ_{cyc} is the p-adic cyclotomic character and $\langle \varepsilon_{\mathrm{cyc}}(\sigma)\rangle$ denotes its image under the projection $\mathbf{Z}_p^* \to 1 + q\mathbf{Z}_p$.

We must prove that the E dimension of $X_{(1)}^{(\chi)} = X^{(\chi)} \otimes_\Lambda \Lambda_{(1)}$ is at least r_{an}. We follow the strategy in [6, Section 4]. We establish the desired lower bound on the dimension of $X_{(1)}^{(\chi)}$ by comparing it to an E-vector space B of dimension at least r_{an} constructed using Hilbert modular forms. The following lemma shows that such homomorphisms are classified by certain Galois cohomology classes.

Lemma 2.4. *Let r denote the number of primes of F above p that split completely in F_χ. Let B denote an $\Lambda_{(1)}$-module endowed with the continuous G_F-action in which G_F acts by $\chi\varepsilon$, and let $\kappa \in H^1(G_F, B)$ a Galois cohomology class such that*

- *κ is everywhere unramified and locally trivial at all primes above p.*
- *If B_0 is the subspace of B generated by the image of the restriction*

$$\kappa|_{G_{H_{\mathrm{cyc}}}} \in H^1(G_{H_{\mathrm{cyc}}}, B) = \mathrm{Hom}_{\mathrm{cont}}(G_{H_{\mathrm{cyc}}}, B),$$

then the E-vector space B/B_0 has dimension at most r.

Then $\dim_E(X_{(1)}^{(\chi)}) \geq \dim_E(B)$.

Proof. Let Y be the Galois group over H_{cyc} of the maximal abelian unramified p-extension of H_{cyc} in which all primes above p split completely. As before we define $Y_{(1)}^{(\chi)}$. Then $Y_{(1)}^{(\chi)}$ is a codimension r subspace of $X_{(1)}^{(\chi)}$ (see [9, Proposition 6.1]). The Gross–Kuz'min conjecture implies that $Y_{(1)}^{(\chi)} = 0$ and that the dimension of $X_{(1)}^{(\chi)}$ is r, but we do not assume this.

If we have κ as above, then the fixed field of the kernel of $\kappa|_{G_{H_{\mathrm{cyc}}}}$ is an extension of H_{cyc} that is everywhere unramified and such that the primes above p split completely. By the definition of Y, we obtain a surjective homomorphism $Y \longrightarrow B_0$. As $\kappa|_{G_{H_{\mathrm{cyc}}}}$ is restricted from a class in $H^1(G_F, B)$ and G_F acts as $\chi\varepsilon$ on B, this surjection factors through $Y_{(1)}^{(\chi)} \longrightarrow B_0$. Therefore

$$\dim_E(X_{(1)}^{(\chi)}) \geq \dim_E(Y_{(1)}^{(\chi)}) + r \geq \dim_E(B_0) + r \geq \dim_E(B).$$

□

The rest of the article is devoted to the construction of a vector space B and cohomology class κ satisfying the conditions of Lemma 2.4 such that $\dim_E B \geq r_{\mathrm{an}}$. By the lemma, we will then obtain $\dim_E X_{(1)}^{(\chi)} \geq r_{\mathrm{an}}$, i.e. Theorem 2.3.

3 Construction of modular forms

In this section we recall the construction of modular forms from [4, 7]. For the notation we refer to [7, Section 3], recalling only the essential aspects here. For each $k \in \mathbf{Z}_p$ we have the "specialization to weight k" $\mathcal{O}_E$-algebra homomorphism

$$\nu_k : \Lambda \longrightarrow \mathcal{O}_E \qquad \text{given by} \qquad T \mapsto u^{k-1} - 1.$$

Recall that $\Lambda_{(1)} = \mathcal{O}_E[[T]]_{(T)}$ is then the localization in "weight 1".

Let $\mathfrak{n}$ denote the conductor of χ. We denote by $\mathcal{M}(\mathfrak{n}, \chi)$ the Λ-module of Λ-adic Hilbert modular forms for F with level $\mathfrak{n}$ and character χ. For each $\mathcal{F} \in \mathcal{M}(\mathfrak{n}, \chi)$ and each integer $k \geq 2$, the specialization $\nu_k(\mathcal{F})$ belongs to the space $M_k(\mathfrak{n}p, \chi\omega^{1-k})$ of Hilbert modular forms for F of weight k, level $\mathfrak{n}p$ and character $\chi\omega^{1-k}$. The subspace of cusp forms in $\mathcal{M}(\mathfrak{n}, \chi)$ is denoted $\mathcal{S}(\mathfrak{n}, \chi)$. The Λ-module $\mathcal{M}(\mathfrak{n}, \chi)$ is equipped with an action of Hecke operators $T_{\mathfrak{l}}$ for primes $\mathfrak{l} \nmid \mathfrak{n}p$ and $U_{\mathfrak{l}}$ for $\mathfrak{l} \mid p$. Following Hida, we let

$$e = \lim_{n \to \infty} \left(\prod_{\mathfrak{p} \mid p} U_{\mathfrak{p}} \right)^{n!}$$

be the ordinary projector. Denote by

$$\mathcal{M}^o(\mathfrak{n}, \chi) = e\mathcal{M}(\mathfrak{n}, \chi), \qquad \mathcal{S}^o(\mathfrak{n}, \chi) = e\mathcal{S}(\mathfrak{n}, \chi)$$

the spaces of Hida families and cuspidal Hida families, respectively. we denote by $\tilde{\mathbf{T}}$ and $\mathbf{T}$ the Λ-algebras of Hecke operators acting on $\mathcal{M}^o(\mathfrak{n},\chi)$ and $\mathcal{S}^o(\mathfrak{n},\chi)$, respectively, generated by the operators $T_\mathfrak{l}$ for $\mathfrak{l}\nmid\mathfrak{n}p$ and $U_\mathfrak{l}$ for $\mathfrak{l}\mid\mathfrak{n}p$.

We put

$$R=\{\mathfrak{p}\mid p:\chi(\mathfrak{p})=1\}$$

and

$$R'=\{\mathfrak{p}\mid p:\chi(\mathfrak{p})\neq 1\}.$$

We are assuming, for simplicity, that R' is non-empty. We also introduce notation for the p-adic L-function. Let $L_p(\chi\omega)\in\Lambda_{(1)}$ such that for every even integer k we have

$$\nu_k(L_p(\chi\omega))=\frac{G_{\chi\omega}(u^k-1)}{H_{\chi\omega}(u^k-1)},$$

so that $\nu_k(L_p(\chi\omega))$ is the value usually denoted $L_p(\chi\omega,1-k)$.

Next we recall the modular form F_k from [4]. We are in "Case 1" in [7] (R' is non-empty). Define

$$F_k=E_k(1,\chi\omega^{1-k})-E_1(1,\chi_{R'})G_{k-1}\frac{L_p(\chi\omega,1-k)}{L(\chi_{R'},0)}$$

The forms $E_k(1,\chi\omega^{1-k})$ and G_{k-1} interpolate to Hida families $\mathcal{E}(1,\chi)$ and $\mathcal{G}$ with the property that

$$\nu_k(\mathcal{E}(1,\chi))=E_k(1,\chi\omega^{1-k}),\qquad \nu_k(\mathcal{G})=G_{k-1}.$$

Therefore we get Λ-adic family:

$$\tilde{\mathcal{F}}=\mathcal{E}(1,\chi)-E_1(1,\chi_{R'})\mathcal{G}\frac{L_p(\chi\omega)}{L(\chi_{R'},0)}.$$

The following theorem is proven in [4, Corollary 2.10 and Proposition 3.4].

Theorem 3.1. *There is a Hecke operator $t\in\tilde{\mathbf{T}}\otimes_\Lambda\Lambda_{(1)}$ such that $\mathcal{F}:=t\cdot e\cdot\tilde{\mathcal{F}}$ is a cuspidal Hida family and such that $t\cdot e$ fixes $\mathcal{E}(1,\chi)$.*

We remark here that we may choose t such that the family $\mathcal{F}$ is normalized. Using the notation in [4] it is clear that the Hecke operators $T_{\eta,\psi}$ and $T_{\chi,\omega^{1-k}}$ act as units in $\Lambda_{(1)}$ on $\mathcal{E}(1,\chi)$. Therefore we take t such that $\mathcal{F}$ is normalized and acts at 1 on $\mathcal{E}(1,\chi)$.

4 Hecke algebra and Hecke action

In this section we recall theorems describing the action of Hecke operators on the cusp form $\mathcal{F}$ constructed above. It is convenient to work with the uniformizer of $\Lambda_{(1)}$ given by

$$\pi=\frac{1}{\log_p u}T.$$

Recall that $r_{\mathrm{an}}(\chi)$ is the order of vanishing of $L_p(\chi\omega)$ i.e. the largest power of the ideal (π) that contains $L_p(\chi\omega)$. Whenever there is no ambiguity we denote $r_{\mathrm{an}}(\chi)$ by r_{an}.

Any Hida family is determined by its Fourier expansion; there is a canonical Λ-algebra embedding

$$c : \mathcal{S}^o(\mathfrak{n}, \chi)_{(1)} \longrightarrow \prod_{\mathfrak{a} \subset \mathcal{O}_F} \Lambda_{(1)}, \qquad \mathscr{H} \mapsto (c(\mathfrak{a}, \mathscr{H}))_{\mathfrak{a} \subset \mathcal{O}_F}.$$

Define $\mathcal{H}$ to be the image of the Hecke orbit of $\mathcal{F}$ under the reduction of c modulo $\pi^{r_{\mathrm{an}}}$. This is a finitely generated module over $\Lambda_{(1)}/(\pi^{r_{\mathrm{an}}}) = E[\pi]/(\pi^{r_{\mathrm{an}}})$. Therefore we obtain a canonical Λ-algebra homomorphism

$$\varphi : \mathbf{T} \longrightarrow \mathrm{End}_{E[\pi]/(\pi^{r_{\mathrm{an}}})} \mathcal{H}.$$

Now since $\pi^{r_{\mathrm{an}}}$ divides $L_p(\chi\omega)$, we have a congruence of Fourier expansions

$$\mathcal{F} \equiv \mathcal{E}(1, \chi) \pmod{\pi^{r_{\mathrm{an}}}}.$$

As a result we obtain the following.

Theorem 4.1. *Assume that R' is non-empty. The image of the map φ is isomorphic to $E[\pi]/(\pi^{r_{\mathrm{an}}})$. Furthermore, φ maps the Hecke operators as follows:*

$$\begin{aligned} &T_{\mathfrak{l}} \mapsto 1 + \chi\varepsilon(\mathfrak{l}) && \text{for } \mathfrak{l} \nmid \mathfrak{n}p, \\ &U_{\mathfrak{l}} \mapsto 1 && \text{for } \mathfrak{l} \mid \mathfrak{n}p. \end{aligned}$$

5 Construction of cohomology classes

Let $\mathfrak{m}$ be the unique maximal ideal containing kernel of φ. Let $\mathbf{T}_{\mathfrak{m}}$ denote the completion of $\mathbf{T}$ with respect to $\mathfrak{m}$ and set $K = \mathrm{Frac}(\mathbf{T}_{\mathfrak{m}})$. Then a theorem of Hida and Wiles [18, Theorems 2 and 4] gives a Galois representation

$$\rho : G_F \longrightarrow \mathbf{GL}_2(K)$$

such that

(1) ρ is unramified outside $\mathfrak{n}p$.

(2) For all primes $\mathfrak{l} \nmid \mathfrak{n}p$, the characteristic polynomial of $\rho(\mathrm{Frob}_{\mathfrak{l}})$ is given by

$$\mathrm{char}(\rho(\mathrm{Frob}_{\mathfrak{l}}))(x) = x^2 - T_{\mathfrak{l}}x + \chi(\mathfrak{l})\varepsilon(\mathfrak{l}).$$

(3) For $\mathfrak{q} \mid p$, let $G_{F,\mathfrak{q}} \subset G_F$ denote a decomposition group at $\mathfrak{q}$. We have

$$\rho|_{G_{F,\mathfrak{q}}} \sim \begin{pmatrix} \chi\varepsilon\eta_{\mathfrak{q}}^{-1} & * \\ 0 & \eta_{\mathfrak{q}} \end{pmatrix}, \tag{3}$$

where $\eta_{\mathfrak{q}} : G_{F,\mathfrak{q}} \to \mathbf{T}_{\mathfrak{m}}^*$ is the unramified character given by $\eta_{\mathfrak{q}}(\mathrm{rec}(\varpi^{-1})) = U_{\mathfrak{q}}$. Here ϖ denotes a uniformiser of $F_{\mathfrak{q}}^*$ and $\mathrm{rec} : F_{\mathfrak{q}}^* \to G_{F,\mathfrak{q}}^{\mathrm{ab}}$ is the local reciprocity map.

For each $\mathfrak{q} \mid p$, let $V_\mathfrak{q}$ be the eigenspace of $\rho|_{G_{F,\mathfrak{q}}}$, i.e. the span of the vector $\binom{1}{0}$ in the basis for which (3) holds. We choose an element $\tau \in G_F$ as in [7, Lemma 4.3]; hence $\chi(\tau) \neq 1$ and the subspace $V_\mathfrak{q}$ projected to each factor of K is not stable under $\rho(\tau)$. We fix a basis such that $\rho(\tau) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, where $\lambda_1 \equiv 1 \pmod{\mathfrak{m}}$ and $\lambda_2 \equiv -1 \pmod{\mathfrak{m}}$. For a general σ, we write

$$\rho(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}.$$

For each $\mathfrak{q} \mid p$, there is a change of basis matrix $M_\mathfrak{q} = \begin{pmatrix} A_\mathfrak{q} & B_\mathfrak{q} \\ C_\mathfrak{q} & D_\mathfrak{q} \end{pmatrix} \in \mathbf{GL}_2(K)$ such that

$$\begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} M_\mathfrak{q} = M_\mathfrak{q} \begin{pmatrix} \chi\varepsilon\eta_\mathfrak{q}^{-1} & * \\ 0 & \eta_\mathfrak{q} \end{pmatrix}. \tag{4}$$

The choice of τ ensures that $A_\mathfrak{q}$ and $C_\mathfrak{q}$ are invertible in K. Furthermore, equating the upper left hand entries in (4) yields:

$$b(\sigma) = \frac{A_\mathfrak{q}}{C_\mathfrak{q}}(a(\sigma) - \chi\varepsilon\eta_\mathfrak{q}^{-1}(\sigma)) \qquad \text{for all } \sigma \in G_{F,\mathfrak{q}}. \tag{5}$$

Let $\varphi_\mathfrak{m} : \mathbf{T}_\mathfrak{m} \to E[\pi]/(\pi^{r_{\mathrm{an}}})$ denote the extension of the homomorphism φ to $\mathbf{T}_\mathfrak{m}$. Put $\mathbf{I} = \ker(\varphi_\mathfrak{m})$. Then, using the choice of basis and following the proof in [7, Lemma 4.4], one can show that

$$a(\sigma) \equiv 1 \pmod{\mathbf{I}}, \qquad d(\sigma) \equiv \varepsilon(\sigma)\chi(\sigma) \pmod{\mathbf{I}}. \tag{6}$$

Now define

- $\mathbf{B} = \mathbf{T}_\mathfrak{m}$-submodule of K generated by $b(\sigma)$ for all $\sigma \in G_F$ along with $\frac{A_\mathfrak{p}}{C_\mathfrak{p}}$, for all $\mathfrak{p} \in R$.
- $\overline{\mathbf{B}} = \mathbf{B}/\mathbf{I}\mathbf{B}$.

Denote by $\overline{b}(\sigma)$ the image of $b(\sigma)$ in $\overline{\mathbf{B}}$. Since ρ is a Galois representation, we have

$$b(\sigma\sigma') = a(\sigma)b(\sigma') + b(\sigma)d(\sigma') \qquad \text{for all } \sigma, \sigma' \in G_F.$$

The congruence (6) therefore implies that the function

$$\kappa(\sigma) = \overline{b}(\sigma)\varepsilon^{-1}(\sigma)\chi^{-1}(\sigma)$$

is a 1-cocycle defining a cohomology class $[\kappa] \in H^1(G_F, \overline{\mathbf{B}}(\varepsilon^{-1}\chi^{-1}))$.

Theorem 5.1. *The class κ is unramified everywhere and locally trivial at primes above p.*

Proof. The proof that κ is unramified at primes outside R is similar to [7, Lemma 4.7] which also shows that κ is locally trivial at all primes in R'. To show that κ is unramified at primes in R we use equation (5). By definition, $A_\mathfrak{p}/C_\mathfrak{p}$ belongs to $\mathbf{B}$ for any $\mathfrak{p} \in R$

and hence $(A_\mathfrak{p}/C_\mathfrak{p})\mathbf{I} = 0$ in $\overline{\mathbf{B}}$. For any σ in the decomposition subgroup at $\mathfrak{p}$, we have $a(\sigma) \equiv \eta_\mathfrak{p}^{-1}(\sigma) \equiv 1 \pmod{\mathbf{I}}$. Hence

$$\kappa(\sigma) = (1 - \chi^{-1}\varepsilon^{-1}(\sigma))(-A_\mathfrak{p}/C_\mathfrak{p})$$

in $\overline{\mathbf{B}}$ for all σ in the decomposition subgroup $G_\mathfrak{p}$. Therefore κ is locally trivial at all primes in R. □

Theorem 5.2. *We have*

$$\mathrm{Fitt}_{E[[\pi]]}(\overline{\mathbf{B}}) \subset (\pi^{r_{\mathrm{an}}}).$$

In particular, $\dim_E(\overline{\mathbf{B}}) \geq r_{\mathrm{an}}$.

Proof. The $\mathbf{T}_\mathfrak{m}$-module $\mathbf{B}$, being a submodule of $K = \mathrm{Frac}(\mathbf{T}_\mathfrak{m})$, is faithful. It follows that $\mathrm{Fitt}_{\mathbf{T}_\mathfrak{m}}(\mathbf{B}) = 0$. Therefore $\mathrm{Fitt}_{\mathbf{T}_\mathfrak{m}/\mathbf{I}}(\overline{\mathbf{B}}) = 0$, whence $\mathrm{Fitt}_{E[[\pi]]/\pi^{r_{\mathrm{an}}}}(\overline{\mathbf{B}}) = 0$. The result follows. □

We present a second proof of the theorem that is a variant of the Fitting ideal computation in [5, Theorem 9.10]. It uses a determinant introduced in [7, Section 5] and whose refinement plays a crucial role in both [5, 6]. We first need a lemma.

Lemma 5.3. *The module* $\mathbf{B}_0 = \langle b(\sigma) : \sigma \in G_F \rangle$ *is generated by finitely many elements* $b_1, \ldots, b_m$ *that are nonzerodivisors in* K.

Proof. The finite generation of $\mathbf{B}_0$ is easy because the homomorphism ρ is continuous and hence $\mathbf{B}_0$ is compact. We must show that we can choose a generating set of nonzerodivisors. Suppose we start with an arbitrary finite generating set $b_1, \ldots, b_m$. We will modify these generators to make each one a nonzerodivisor in K. We do this by induction on the total number of zero projections of the b_i onto the factors E_j of K. Suppose that b_i has a zero projection on some E_j. Since the representation ρ_{f_j} is irreducible, some other b_k has nonzero projection onto E_j. If we replace b_i by $b_i + tb_k$for any nonzero $t \in E$, the new b_i has a nonzero projection onto E_j. Furthermore, at most finitely many t introduce a new zero projection of b_i onto some other E_j. Avoiding these finitely many t, we can choose a t that decreases the total number of zeros. Furthermore, the replacement $b_i \mapsto b_i + tb_k$ does not change the span of the set $\{b_i\}$, and hence preserves the property that they generate $\mathbf{B}_0$. □

Second proof of Theorem 5.2. Let $b_1, \ldots, b_n$ be generators of B as given by Lemma 5.3 above together with $\frac{A_{\mathfrak{p}_i}}{C_{\mathfrak{p}_i}}$ for $R = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ (therefore $n = m + r$, with m as in Lemma 5.3). Suppose we have a matrix

$$M \in M_{n\times n}(E[[\pi]])$$

such that each row of M represents a relation amongst our generators i.e. such that

$$M(b_1, \ldots, b_n)^t \equiv 0 \text{ in } \overline{\mathbf{B}}^n.$$

By the definition of Fitting ideal, the theorem will follow if we can show that $\det(M) \in (\pi^{r_{\mathrm{an}}})$. Write $M = (z_{ij})$. As the b_i's generate $\mathbf{B}$, every element of $\mathbf{IB}$ can be written as a sum of elements of the form $b_i t_i$ with $t_i \in \mathbf{I}$. Therefore each relation

$$\sum_{j=1}^{n} z_{ij} b_j \equiv 0 \text{ in } \overline{\mathbf{B}}$$

can be expressed as an equality in $\mathbf{B}$ as

$$\sum_{j=1}^{n} (z_{ij} + \mathbf{I}) b_j = 0.$$

We use the notation $a = b + \mathbf{I}$ to mean $a = b + z$ for some $z \in \mathbf{I}$. We can cancel the factors b_j scaling the columns of M, since these are non-zerodivisors in K. We obtain that $\det(M') = 0$ where

$$M' = (z_{ij} + \mathbf{I}).$$

Taking the determinant of M' and applying φ, we obtain that

$$0 = \varphi(\det(M')) = \det(M)$$

in W. By Theorem 4.1, we obtain that $\det(M) \in (\pi^{r_{\mathrm{an}}})$ as desired.

□

Theorem 2.3 now follows from Lemma 2.4, once we observe that κ has all the required properties. Indeed, we have shown in Theorem 5.1 that κ is everywhere unramified and locally trivial at all primes above p. Furthermore, if $\overline{\mathbf{B}}_0$ denotes the image of $\mathbf{B}_0$ in $\overline{\mathbf{B}}$, then $\overline{\mathbf{B}}/\overline{\mathbf{B}}_0$ is generated over $\mathbf{T}_{\mathfrak{m}}/\mathbf{I} \cong E[\pi]/(\pi^{r_{\mathrm{an}}})$ by the r elements $\left\{ \frac{A_{\mathfrak{p}}}{C_{\mathfrak{p}}} : \mathfrak{p} \in R \right\}$. We claim that π acts trivially on $\overline{\mathbf{B}}/\overline{\mathbf{B}}_0$ and thus $\left\{ \frac{A_{\mathfrak{p}}}{C_{\mathfrak{p}}} : \mathfrak{p} \in R \right\}$ generates $\overline{\mathbf{B}}/\overline{\mathbf{B}}_0$ as an E-vector space. Let σ be an element in $G_{F,\mathfrak{p}}$ such that $\langle \epsilon_{\mathrm{cyc}}(\sigma) \rangle \neq 1$. Then we have

$$1 - \varepsilon(\sigma) = \pi \cdot \text{unit}$$

and equation (5) implies that

$$b(\sigma) = \frac{A_{\mathfrak{p}}}{C_{\mathfrak{p}}} (a(\sigma) - \chi(\sigma)\varepsilon(\sigma)\eta_{\mathfrak{p}}^{-1}(\sigma)) \equiv \frac{A_{\mathfrak{p}}}{C_{\mathfrak{p}}} \cdot (1 - \varepsilon(\sigma)) \pmod{\mathbf{I}}.$$

Therefore $\frac{A_{\mathfrak{p}}}{C_{\mathfrak{p}}} \cdot \pi \in \overline{\mathbf{B}}_0$ proving our claim.

Since $\dim_E \overline{\mathbf{B}}/\overline{\mathbf{B}}_0 \leq r$, Lemma 2.4 yields the desired inequality

$$\dim_E X_{(1)}^{(\chi)} \geq \dim_E \overline{B} \geq r_{\mathrm{an}}.$$

References

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

[2] J. Coates and S. Lichtenbaum. On l-adic zeta functions. *Ann. of Math. (2)* 98:498–550, 1973.

[3] Pierre Colmez. Résidu en $s = 1$ des fonctions zêta p-adiques. *Invent. Math.* 91 (2):371–389, 1988.

[4] Samit Dasgupta, Henri Darmon, and Robert Pollack. Hilbert modular forms and the Gross-Stark conjecture. *Ann. of Math. (2)* 174 (1):439–484, 2011.

[5] Samit Dasgupta and Mahesh Kakde. On the Brumer–Stark conjecture, Preprint `https://arxiv.org/abs/2010.00657`.

[6] ———. Brumer–Stark units and Hilbert's 12th problem, Preprint `https://arxiv.org/abs/2103.02516`.

[7] Samit Dasgupta, Mahesh Kakde, and Kevin Ventullo. On the Gross-Stark conjecture. *Ann. of Math. (2)* 188 (3):833–870, 2018.

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

[9] L.J. Federer and B.H Gross. Regulators and Iwasawa modules. *Invent. Math.* 62 (3):443–457, 1981.

[10] Ralph Greenberg. On a certain l-adic representation. *Invent. Math.* 21:117–124, 1973.

[11] ———. On p-adic Artin L-functions. *Nagoya Math. J.* 89:77–87, 1983.

[12] Benedict H. Gross. p-adic L-series at $s = 0$. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 28 (3):979–994 (1982), 1981.

[13] H. Hida and J. Tilouine. On the anticyclotomic main conjecture for CM fields. *Invent. Math.* 117 (1):89–147, 1994.

[14] Henri Johnston and Andreas Nickel. An unconditional proof of the abelian equivariant Iwasawa main conjecture and applications, Preprint `https://arxiv.org/abs/2010.03186`.

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

[16] Kenneth A. Ribet. A modular construction of unramified p-extensions of $\mathbf{Q}(\mu_p)$. *Invent. Math.* 34 (3):151–162, 1976.

[17] Kevin Ventullo. On the rank one abelian Gross-Stark conjecture. *Comment. Math. Helv.* 90 (4):939–963, 2015.

[18] A. Wiles. On ordinary λ-adic representations associated to modular forms. *Invent. Math.* 94 (3):529–573, 1988.

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