

Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 87 (2012)

Artikel: Anticyclotomic Iwasawa's main conjecture for Hilbert modular forms
Autor: Longo, Matteo
DOI: <https://doi.org/10.5169/seals-283481>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 29.01.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

Anticyclotomic Iwasawa’s Main Conjecture for Hilbert modular forms

Matteo Longo

Abstract. Let F/\mathbb{Q} be a totally real extension and f an Hilbert modular cusp form of level \mathfrak{n} , with trivial central character and parallel weight 2, which is an eigenform for the action of the Hecke algebra. Fix a prime $\wp \mid \mathfrak{n}$ of F of residual characteristic p . Let K/F be a quadratic totally imaginary extension and K_{\wp^∞} be the \wp -anticyclotomic \mathbb{Z}_p -extension of K . The main result of this paper, generalizing the analogous result [5] of Bertolini and Darmon, states that, under suitable arithmetic assumptions and some technical restrictions, the characteristic power series of the Pontryagin dual of the Selmer group attached to (f, K_{\wp^∞}) divides the p -adic L -function attached to (f, K_{\wp^∞}) , thus proving one direction of the Anticyclotomic Main Conjecture for Hilbert modular forms. Arithmetic applications are given.

Mathematics Subject Classification (2010). 11G10, 11G18, 11G40.

Keywords. Hilbert modular forms, Iwasawa theory.

Contents

1	Introduction	303
2	Anticyclotomic \mathbb{Z}_p -extensions	308
3	CM points on quaternion algebras	310
4	p -adic L -functions	312
5	Selmer groups attached to Hilbert modular forms	315
6	Iwasawa’s Main Conjecture	321
7	The proof	325
	References	350

1. Introduction

Let F/\mathbb{Q} be a totally real extension of degree $d := [F : \mathbb{Q}]$ and \mathfrak{n} a square-free integral ideal of the ring of integers \mathcal{O}_F of F . Let $f \in S_2(\mathfrak{n})$ be a Hilbert modular cusp form for the $\Gamma_0(\mathfrak{n})$ level structure with trivial central character and parallel

weight 2. Let \mathbb{T}_n be the Hecke algebra generated over \mathbb{Z} by the Hecke operators acting on $S_2(n)$. Assume that f is a normalized eigenform for the action of \mathbb{T}_n and denote by $\phi_f: \mathbb{T}_n \rightarrow \bar{\mathbb{Q}}$ the morphism corresponding to f . Let $a_q(f) := \phi_f(T_q)$ (respectively, $a_q(f) := \phi_f(U_q)$) be the eigenvalue of the Hecke operator at prime ideals $q \nmid n$ (respectively, $q \mid n$). Define

$$K_f := \mathbb{Q}(a_q(f), q \text{ a prime ideal of } \mathcal{O}_F)$$

to be the field generated (over \mathbb{Q}) by the eigenvalues of the Hecke algebra acting on f and denote by \mathcal{O}_f its ring of integers. Since the character of f is trivial, K_f is totally real by [44], Proposition 2.5.

Fix $p \geq 5$ a rational prime and assume for simplicity that p does not ramify in F/\mathbb{Q} and K_f/\mathbb{Q} . Fix an embedding $\iota_p: \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$. Denote by π the prime ideal of \mathcal{O}_f corresponding to ι_p and denote by $\mathcal{O}_{f,\pi}$ the completion of \mathcal{O}_f at π .

Say that f is *ordinary* at a prime ideal $\mathfrak{p} \mid p$ if there exists a root $\alpha_{\mathfrak{p}}$ of the Hecke polynomial at \mathfrak{p} such that $\iota_p(\alpha_{\mathfrak{p}})$ is a unit. In this paper we assume that f is ordinary at all prime ideals $\mathfrak{p} \mid p$.

Suppose that there exists a prime ideal $\wp \mid p$ such that $\wp \mid n$. Suppose that either f is a newform or it comes from a newform of level n/\wp which is ordinary at all primes \mathfrak{p} dividing p via the procedure of p -stabilization. In the totally real case, see Section 12.5.2 in [35] for this procedure; see also Nekovář [35] (Chapter 12), [36], [37], Zhang [48], [49], [50], Cornut–Vatsal [9], [8], Howard [21] and Goren [16] for references on recent developments and results on the arithmetic theory of Hilbert modular forms.

Let K/F be a totally imaginary quadratic extension. Assume that the discriminant of K/F and $p\mathfrak{n}$ are prime to each other. Then K determines a factorization

$$\mathfrak{n} = \wp \mathfrak{n}^+ \mathfrak{n}^-$$

where a prime ideal \mathfrak{q} divides \mathfrak{n}^+ if and only if \mathfrak{q} is split in K/F while divides \mathfrak{n}^- if and only if it is inert in K/F . We also assume that the number of prime ideals $\mathfrak{q} \subseteq \mathcal{O}_F$ dividing \mathfrak{n}^- has the same parity as $d = [F : \mathbb{Q}]$. Finally, if d is even, we assume that $\mathfrak{n}^- \neq \mathcal{O}_F$.

Remark 1.1. The condition $d \text{ even} \Rightarrow \mathfrak{n}^- \neq \mathcal{O}_F$ is assumed to obtain the isomorphism (10). See Remark 7.15. For the case of d even and $\mathfrak{n}^- = \mathcal{O}_F$, see the discussions and the results of [29] and [30].

As a consequence of the assumption on the parity of the number of ideals dividing \mathfrak{n}^- , the special value at 1 of the complex L -function $L_K(f, \chi, s)$ of f over K twisted by χ is non zero for infinitely many ramified ring class characters χ of conductor \wp^m (see [8], Theorem 1.4).

Using the notion of Gross points it is possible to associate to f a p -adic L -function $L_{\wp,\pi}(f/K)$ relative to \wp and π . This is an element of the Iwasawa algebra

$$\Lambda_{\wp,\pi} := \mathcal{O}_{f,\pi} \llbracket G_{\wp^\infty} \rrbracket,$$

where

$$G_{\wp^\infty} := \text{Gal}(K_{\wp^\infty}/K) \simeq \mathbb{Z}_p^{[F_\wp:\mathbb{Q}_p]}$$

is the Galois group of the anticyclotomic \mathbb{Z}_p -extension K_{\wp^∞}/K associated to \wp . See Section 2 for the definition of K_{\wp^∞} and Section 4 for the construction of $L_{\wp,\pi}(f/K)$. The p -adic L function $L_{\wp,\pi}(f/K)$ is characterized by its interpolation properties of the complex L -functions $L_K(f, \chi, s)$, where χ is as above: see Section 4.4 for details.

On the other hand, there is a notion of *Selmer group* attached to f . Denote by

$$\rho_{f,\pi^\infty} : G_F := \text{Gal}(\bar{F}/F) \longrightarrow \text{GL}_2(\mathcal{O}_{f,\pi})$$

the π -adic Galois representation attached to f and define $\rho_{f,\pi^n} := \rho_{f,\pi^\infty} \pmod{\pi^n}$. Denote by T_{f,π^∞} the G_F -module associated to the representation ρ_{f,π^∞} . Let

$$V_{f,\pi^\infty} := T_{f,\pi^\infty} \otimes_{\mathcal{O}_{f,\pi}} K_{f,\pi}$$

(where $K_{f,\pi} := \text{Frac}(\mathcal{O}_{f,\pi})$). Define finally $A_{f,\pi^\infty} := V_{f,\pi^\infty}/T_{f,\pi^\infty}$ and $A_{f,\pi^n} := A_{f,\pi^\infty}[\pi^n]$ for all $n \geq 1$. The Selmer group

$$\text{Sel}_{\pi^\infty}(f/K_{\wp^\infty}) \subseteq H^1(K_{\wp^\infty}, A_{f,\pi^\infty})$$

is defined in Section 5 by imposing suitable local conditions on global cohomology classes. Its Pontryagin dual $\text{Sel}_{\pi^\infty}^\vee(f/K_{\wp^\infty})$ is a finitely generated $\Lambda_{\wp,\pi}$ -module. Denote by

$$\text{Char}_{\wp,\pi}(f/K) \in \Lambda_{\wp,\pi}$$

the characteristic power series of $\text{Sel}_{\pi^\infty}^\vee(f/K_{\wp^\infty})$. This element is well-defined only up to units, while the ideal $(\text{Char}_{\wp,\pi}(f/K))$ of $\Lambda_{\wp,\pi}$ generated by $\text{Char}_{\wp,\pi}(f/K)$ depends only on $\text{Sel}_{\pi^\infty}^\vee(f/K_{\wp^\infty})$.

The Anticyclotomic Iwasawa Main Conjecture relates the ideals of $\Lambda_{\wp,\pi}$ generated by $L_{\wp,\pi}(f/K)$ and $\text{Char}_{\wp,\pi}(f/K)$; it can be stated as follows:

Conjecture 1.2 (Anticyclotomic Iwasawa's Main Conjecture). *The ideals of $\Lambda_{\wp,\pi}$ generated by $L_{\wp,\pi}(f/K)$ and by $\text{Char}_{\wp,\pi}(f/K)$ are equal.*

For any prime ideal $\mathfrak{q} \subseteq \mathcal{O}_F$, choose

$$G_{F_{\mathfrak{q}}} = \text{Gal}(\bar{F}_{\mathfrak{q}}/F_{\mathfrak{q}}) \subseteq \text{Gal}(\bar{F}/F)$$

a decomposition group and denote by $I_{F_{\mathfrak{q}}}$ its inertia subgroup. To state the main result, suppose that the following technical conditions are verified:

Assumption 1.3. (1) $\rho_{f,\pi}$ is surjective.

(2) The morphism $\phi_f: \mathbb{T}_\pi \rightarrow \mathcal{O}_f$ is surjective.

(3) Define $\mathfrak{m}_{f,\pi}$ to be kernel of the morphism $\mathbb{T}_\pi \rightarrow \mathcal{O}_{f,\pi}/\pi$ associated to f . The completion \mathbb{T}_f of \mathbb{T}_π at $\mathfrak{m}_{f,\pi}$ is isomorphic to $\mathcal{O}_{f,\pi}$ (we say that f is π -isolated if this condition holds).

(4) Let $\mathfrak{q} \mid \pi$ and $\mathfrak{q} \nmid p$ be a prime ideal. The maximal $I_{F_{\mathfrak{q}}}$ -invariant submodule of A_{f,π^∞} is free of rank one over $K_{f,\pi}/\mathcal{O}_{f,\pi}$.

(5) If $p = 5$ then $[F(\zeta_5) : F] \neq 2$, where ζ_5 is a 5-th root of unity.

(6) The prime number p does not divide the class number h_K of K and the index $[\mathcal{O}_K^\times : \mathcal{O}_F^\times]$ of \mathcal{O}_F^\times in \mathcal{O}_K^\times . Further, p does not ramify in F and K_f .

Remark 1.4. Some of the conditions in Assumption 1.3 could probably be relaxed. In particular, (1) could be replaced by a less strong condition as in [38]. Condition (2) also could be relaxed by using arguments in [39]. Condition (3) will be used in Lemma 7.7 to control a certain Selmer group associated to the adjoint representation of $\rho_{f,\pi}$ and to obtain the isomorphism (10). Condition (4) will be used in § 5.2 to describe the local conditions at primes $\mathfrak{q} \mid \pi$, $\mathfrak{q} \nmid p$ appearing in the definition of $\text{Sel}_{\pi^\infty}(f/K_{\varphi^\infty})$. In the case of a modular abelian variety A defined over F , whose associated Hilbert modular form is f (in the sense of Definition 6.3), these conditions will be compared in § 6.2 with the image of the local Kummer map at the primes dividing π but not dividing p . Condition (5) is used in § 7.3 to apply a result by Fujiwara [15]. Finally, (6) could certainly be relaxed and is assumed mainly to get a simpler description of the extension K_{φ^∞} in Section 2 and, consequently, a simpler construction of $L_{\varphi,\pi}(f/K)$ in Section 4.

The main result, corresponding to Theorem 6.1, can be formulated under the technical conditions in Assumption 1.3 as follows:

Theorem 1.5. *Suppose that Ihara's Lemma for Shimura curves over totally real fields, as stated in Assumption 7.18, holds. Then the characteristic power series $\text{Char}_{\varphi,\pi}(f/K)$ divides the p -adic L -function $L_{\varphi,\pi}(f/K)$.*

Under our arithmetic assumptions, the p -adic L -function does not vanish identically by Theorem 1.4 of [8]: see Section 4.4. This shows that (see Corollary 6.2):

Corollary 1.6. *Assumptions as in Theorem 1.5. Then $\text{Sel}_{\pi^\infty}^\vee(f/K_{\varphi^\infty})$ is pseudo-isomorphic to a torsion $\Lambda_{\varphi,\pi}$ -module.*

Remark 1.7. Unlike the conditions in Assumption 1.3, Ihara's Lemma in the statement of Theorem 1.5 seems to be considerably harder to remove. This is the most substantial obstruction to an unconditional result. It consists in a version of Ihara's Lemma for Shimura curves over totally real fields. It will be used in the proof of

Lemma 7.20 below. If $F = \mathbb{Q}$, the result we need is Theorem 2 in [12]. The results contained in [12] and successively refined in [13] are partially generalized to the totally real case in [25]. However, [25] does not cover the full generalization of [12], Theorem 2. In this paper we follow [15], which assumes the generalization of Ihara's Lemma as an hypothesis in [15] (Hypothesis 5.9). Similar results for Hilbert modular varieties hold thanks to [14]. For further discussions, see Remark 7.19.

The proof of the main result is a generalization of the methods in [5], where the case of $F = \mathbb{Q}$ and $\mathcal{O}_{f,\pi} = \mathbb{Z}_p$ is considered. In Section 7 the main steps of the proof are recalled and the necessary technical adaptations are performed. Among the difficulties arising in the totally real context is that we work with an Iwasawa algebra isomorphic to a power series ring in several (not just one) variables. In particular, we need to generalize the divisibility criterion in [5] (Proposition 3.1) to this more general setting. The needed generalization is provided by Proposition 7.4, which might be viewed as an algebraic result of independent interest in the context of Iwasawa theory. An other technical difficulty arises from the fact that we deal with normalized newforms f with arbitrary (non necessarily integers) Fourier coefficients and we need to discuss the local conditions defining Selmer groups in order to relate them to the usual description of Selmer groups via classical Kummer map when f is associated to an abelian variety (in the sense of Definition 6.3). See § 6.2 for details.

Remark 1.8. If the above condition on the number of primes dividing π^- is not satisfied (excluding from this discussion the case $[F : \mathbb{Q}]$ even and $\pi = \mathcal{O}_F$ for simplicity), then $\text{Sel}_{\pi^\infty}^\vee(f/K_{\varphi^\infty})$ is not pseudo-isomorphic to a torsion $\Lambda_{\varphi,\pi}$ -module and the growth of $\text{Sel}_{\pi^\infty}(f/K_{\varphi^\infty})$ is forced by the presence of Heegner points coming from a Shimura curve parametrization of the abelian variety A_f associated to f (see Remark 6.4 for details on A_f and its parametrization by the Jacobian variety of a suitable Shimura curve). For precise statements and results in this case, see [1] (over \mathbb{Q}), [21] and [36] (over totally real number fields).

Remark 1.9. Using the techniques announced by Skinner–Urban, it should be possible to prove the opposite divisibility $L_{\varphi,\pi}(f/K) \mid \text{Char}_{\varphi,\pi}(f/K)$. Thus, combining with Theorem 1.5, it may be possible to obtain a proof of Conjecture 1.2. An other application of the methods of Skinner–Urban concerns the full p -adic L -function (and not just its anticyclotomic part as in Conjecture 1.2). It should be possible to prove that the p -adic L -function of the maximal \mathbb{Z}_p -extension of K divides the characteristic ideal of the Pontryagin dual of the π -Selmer module attached to f and this extension. If this were the case, one could combine such a result with Theorem 1.5 to prove the main conjecture for the full p -adic L -function and therefore for the *cyclotomic* p -adic L -function. Such a result would generalise work of Kato over \mathbb{Q} to the case of totally real fields. (Kato's construction of an Euler system does not generalize.)

Theorem 1.5 can be used to study the arithmetic of abelian varieties of GL_2 -type. The simplest case is that of an elliptic curve. Let A be an elliptic curve defined over F , of conductor \mathfrak{n} , without complex multiplication, which is ordinary at each prime ideal $\mathfrak{p} \mid p$. Suppose also that A is *modular* in the sense that there exists a Hilbert modular form f for the $\Gamma_0(\mathfrak{n})$ -structure, of parallel weight 2 and trivial central character, such that the ℓ -adic representation of A is isomorphic to the ℓ -adic representation associated to f , where ℓ is a rational prime. In this case, $\mathcal{O}_f = \mathbb{Z}$, $\pi = p$ and $\mathcal{O}_{f,\pi} = \mathbb{Z}_p$. Suppose finally that f satisfies all the above assumptions. Note in particular that, since A does not have complex multiplication, there are only a finite number of primes ℓ such that the Galois representation on the ℓ -torsion points of A is not surjective. Theorem 1.5 can be used to study the characteristic power series of the Pontryagin dual $\text{Sel}_{p^\infty}^\vee(A/K_{\wp^\infty})$ of the p -primary Selmer group $\text{Sel}_{p^\infty}(A/K_{\wp^\infty})$ of A over K_{\wp^∞} . Theorem 1.5 and the non-vanishing of $L_\wp(f/K)$ established in Theorem 1.4 of [8] show that $\text{Sel}_{p^\infty}^\vee(A/K_{\wp^\infty})$ is always pseudo-isomorphic to a torsion $\Lambda_{\wp,p}$ -module. The first application, corresponding to Corollary 6.11, is the following:

Corollary 1.10. *Assumptions as in Theorem 1.5. Moreover, suppose $[F_\wp : \mathbb{Q}_p] = 1$ and let A/F be a modular elliptic curve as above. Then $A(K_{\wp^\infty})$ is finitely generated.*

For any $\Lambda_{\wp,p}$ -module M and any finite order character $\chi: G_{\wp^\infty} \rightarrow \mathcal{O}$, where \mathcal{O} is the ring of integers of a finite extension of \mathbb{Q}_p , extend χ to a homomorphism, denoted by the same symbol, $\chi: \Lambda_{\wp,p} \rightarrow \mathcal{O}$ and set $M^\chi := M \otimes_\chi \mathcal{O}$, the tensor product being taken over $\Lambda_{\wp,p}$ via χ . Let $\text{III}_{p^\infty}(A/K_{\wp^\infty})$ be the p -primary part of the Shafarevich–Tate group of A over K_{\wp^∞} . The second application, corresponding to Corollary 6.9, is the following:

Corollary 1.11. *Assumptions as in Theorem 1.5. Moreover, suppose $[F_\wp : \mathbb{Q}_p] = 1$ and let A/F be a modular elliptic curve as above. If $L_K(A, \chi, 1) \neq 0$, then $A(K_{\wp^\infty})^\chi$ and $\text{III}_{p^\infty}(A/K_{\wp^\infty})^\chi$ are finite.*

Acknowledgements. The author thanks the referee for the careful reading of the manuscript and for useful comments which led to some corrections and an improvement of the exposition.

2. Anticyclotomic \mathbb{Z}_p -extensions

Let the assumptions and notations be fixed as in Section 1. In particular, recall that p does not divide the class number of K and the index of \mathcal{O}_F^\times in \mathcal{O}_K^\times . For any integral ideal $\mathfrak{c} \subseteq \mathcal{O}_F$, let

$$\mathcal{O}_{\mathfrak{c}} := \mathcal{O}_F + \mathfrak{c}\mathcal{O}_K$$

be the order of conductor c in K and define the *ring class field* \tilde{K}_c/K of K of conductor c to be the Galois extension of K such that the Artin map induces an isomorphism:

$$\mathrm{Gal}(\tilde{K}_c/K) \simeq \mathrm{Pic}(\mathcal{O}_c) \simeq \hat{K}^\times / \hat{\mathcal{O}}_c^\times K^\times.$$

Denote by $|\cdot|$ the norm on ideals of \mathcal{O}_F and set $h_c := \#\mathrm{Pic}(\mathcal{O}_c)$, so that $h_K := h_{(1)}$ is the class number of K . By the Dedekind formula:

$$h_c = \frac{h_K |c| \prod_{\mathfrak{q}|c} \left(1 - \left(\frac{K}{\mathfrak{q}}\right) |\mathfrak{q}|^{-1}\right)}{[\mathcal{O}_K^\times : \mathcal{O}_c^\times]}, \quad (1)$$

where \mathfrak{q} denotes a prime ideal of \mathcal{O}_F and $\left(\frac{K}{\mathfrak{q}}\right) = 1$ (respectively, $-1, 0$) if \mathfrak{q} is split (respectively, inert, ramified) in K/F . The extension \tilde{K}_{\wp^m}/K is unramified outside the places dividing \wp . Thanks to the fact that p does not ramify in K and does not divide $h_K[\mathcal{O}_K^\times : \mathcal{O}_F^\times]$, it follows from (1), that $[\tilde{K}_{\wp^m} : \tilde{K}_{\wp^{m-1}}] = |\wp|$ for all integers $m \geq 2$ and that $p \nmid [\tilde{K}_{\wp} : K]$. Define $\tilde{K}_{\wp^\infty} := \varinjlim_m \tilde{K}_{\wp^m}$.

Definition 2.1. The \wp -anticyclotomic \mathbb{Z}_p -extension K_{\wp^∞}/K is defined to be the unique subfield K_{\wp^∞} of \tilde{K}_{\wp^∞} such that

$$G_{\wp^\infty} := \mathrm{Gal}(K_{\wp^\infty}/K) \simeq \mathbb{Z}_p^{[F_{\wp}:\mathbb{Q}_p]}.$$

The extension K_{\wp^∞}/F is Galois and non abelian. More precisely, the quotient $\mathrm{Gal}(K/F)$ acts by conjugation on the normal subgroup $\mathrm{Gal}(K_{\wp^\infty}/K)$ by the formula $\sigma \mapsto \tau \sigma \tau = \sigma^{-1}$, where τ is the choice of a complex conjugation raising the non trivial automorphism of $\mathrm{Gal}(K/F)$. For any integer $m \geq 1$, define the extension K_{\wp^m}/K by requiring that

$$G_{\wp^m} := \mathrm{Gal}(K_{\wp^m}/K) \simeq (\mathbb{Z}/p^m\mathbb{Z})^{[F_{\wp}:\mathbb{Q}_p]}.$$

It follows from the above assumptions on p that K_{\wp^m} is the maximal p -power sub-extension of \tilde{K}_{\wp^m}/K . Denote by $\Lambda_{\wp,\pi}$ the Iwasawa algebra of G_{\wp^∞} :

$$\Lambda_{\wp,\pi} := \mathcal{O}_{f,\pi}[[G_{\wp^\infty}]] = \varprojlim_m \mathcal{O}_{f,\pi}[G_{\wp^m}]$$

where the inverse limit is with respect to the canonical projection maps $G_{\wp^m} \rightarrow G_{\wp^{m-1}}$.

Remark 2.2. There are other definitions of ring class fields of conductor c in the literature. Nekovář [36], Section 2.6 (see also Zhang [50]), defines the *ring class field of conductor* c to be the Galois extension K_c^* corresponding via class field theory to

$\widehat{K}^\times/K^\times\widehat{\mathcal{O}}_c^\times\widehat{F}^\times$. On the other hand, [8] uses the definition given in this paper for the ring class field \widetilde{K}_{\wp^n} , denoted $K[P^n]$ therein. However, note that the quotient $\widehat{K}^\times/K^\times\widehat{\mathcal{O}}_c^\times\widehat{F}^\times$ is isomorphic to $\text{Pic}(\mathcal{O}_c)/\text{Pic}(\mathcal{O}_F)$, so, since $p \nmid h_K$, the maximal \mathbb{Z}_p -extension contained in $\bigcup_{n=1}^\infty K_{\wp^n}^*$ is exactly the extension K_{\wp^∞} in Definition 2.1.

3. CM points on quaternion algebras

This section is devoted to fixing the notation for CM-points on quaternion algebras. Since we will need this notions both for totally definite quaternion algebras (in Section 4) and for quaternion algebras which are split in exactly one archimedean place (in Section 7.4), we will adopt a quite general view-point.

3.1. Optimal embeddings and CM-points. Let k denote a global or local field and D/k a quaternion algebra. Let O be an Eichler order of D . Let k'/k be a quadratic extension and denote by r an order in k' . Say that ψ is an *optimal embedding* of r into O if $\psi: k' \hookrightarrow D$ is an injective homomorphism of k -algebras such that

$$\psi(r) = \psi(k') \cap O.$$

Two optimal embeddings ψ_1 and ψ_2 of r into O are said to be *equivalent* if there exists $\alpha \in O^\times$ such that $\psi_1(x) = \alpha^{-1}\psi_2(x)\alpha$ for all $x \in r$. The *conductor* of an optimal embedding ψ is the conductor of the order r . For more details, see [47], Chapitre II, when k is a local field and [47], Chapitre III, when k is a global field.

Suppose now that k is a global field and, for any valuation v of k , let k_v, k'_v, r_v, D_v and O_v denote the completions of k, k', r, D and O , respectively, at v . In the following, by an abuse of notation, we will identify v with the integral prime ideal of k corresponding to it. Let d denote the discriminant of k'/k , c the conductor of the quadratic order r , n the discriminant of the quaternion algebra D and m the level of the Eichler order O , and assume that m is square-free, c is prime to n and d is prime to cmn . Suppose that if $v \mid n$ then v is inert in k' . Suppose also that if $v \mid m$ and $v \nmid c$ (so r_v is maximal) then v is split in k'/k . These conditions ensure that the set of optimal embeddings of r into O is non-empty: see [47], page 94.

Following [17] and [3], define

$$X(k') := D^\times \backslash \widehat{D}^\times \times \text{Hom}(k', D) / \widehat{O}^\times$$

where the action of $b \in D^\times$ and $x \in \widehat{O}^\times$ on a pair (g, ψ) is $b(g, \psi)x := (bgx, b\psi b^{-1})$. Say that a point $(x, \psi) \in X(k')$ is a *CM-point of conductor c* if ψ is an optimal embedding of r into $O_x := xOx^{-1} \cap D$. Write $\text{CM}(c)$ for the set of CM-points of conductor c in $X(k')$.

Fix an embedding $\bar{\psi}: k' \hookrightarrow D$ which allows to view k' as a subfield of D . Following [8], the set $\text{CM}(c)$ can also be described as follows. Define

$$Y(k') := \bar{\psi}(k')^\times \backslash \hat{D}^\times / \hat{O}^\times.$$

Say that a point $x \in Y(k')$ has conductor c if $k' \cap O_x = r$. The set $\text{CM}(c)$ can be identified with the set of points in $Y(k')$ of conductor c . To see this, note that there is a map from the set of points in $Y(k')$ of conductor c to $X(k')$ defined by $x \mapsto (x, \bar{\psi})$. This map is a bijection. Injectivity: Suppose $(x_1, \bar{\psi}) = (x_2, \bar{\psi})$. Then there exists $b \in D^\times$ and $x \in \hat{O}^\times$ such that $x_1 = bx_2x$ and $\bar{\psi} = b\bar{\psi}b^{-1}$. Since $\bar{\psi}(k')$ is a maximal commutative subfield of D , it follows that $b \in \bar{\psi}(k')$ and so x_1 and x_2 represent the same element in $\bar{\psi}(k')^\times \backslash \hat{D}^\times / \hat{O}^\times$. Surjectivity: Fix $(x, \psi) \in X(k')$ of conductor c . By the Skolem–Noether theorem, there exists $b \in D^\times$ such that $\psi(k') = b^{-1}\bar{\psi}(k')b$. It follows that $b^{-1}\bar{\psi}(r)b = b^{-1}\bar{\psi}(k')b \cap x\hat{O}x^{-1}$, so $\bar{\psi}(r) = \bar{\psi}(k') \cap bx\hat{O}(bx)^{-1}$. Hence, $(bx, \bar{\psi})$ belongs to the image of the set of points in CM of conductor c . Finally, note that $(bx, \bar{\psi}) = (x, b^{-1}\bar{\psi}b) = (x, \psi)$.

The Galois group

$$G(c) = \text{Pic}(r) = \hat{k}^\times / k'^\times \hat{r}^\times$$

acts on $\text{CM}(c)$ by left translation: for every $g \in G(c)$ and $(x, \psi) \in \text{CM}(c)$, the action is given by $x \mapsto (gx, \psi)$. Equivalently, if $x \in Y(k')$ has conductor c , the Galois action is given by $x \mapsto gx$.

3.2. The trace formula. Fix representatives $g_1 = 1, \dots, g_h$ of $D^\times \backslash \hat{D}^\times / \hat{O}^\times$ and define $O_j := g_j \hat{O} g_j^{-1} \cap D$, so that $O_1 = O$. Note that the number of CM -points of $X(k')$ is equal to the number of non-equivalent optimal embeddings of r into one of the Eichler orders O_j . Write $\text{Emb}(r, O_j)$ for the set of equivalence classes of optimal embeddings of r into O_j .

For any place v of k , let m_v be the number of non-equivalent local optimal embeddings of r_v into O_v . Then m_v is finite and $m_v = 1$ for those v which do not divide mn . The following *trace formula* holds ([47], Chapitre III, Théorème 5.11 and page 94):

$$|\text{CM}(c)| = \sum_{j=1}^h |\text{Emb}(r, O_j)| = h(r) \prod_{v|mn} m_v, \quad (2)$$

where $h(r)$ is the class number of r .

3.3. Orientations and Gross points. An *orientation* at v of a local optimal embedding $\psi: k_v \rightarrow D_v$ of r_v into O_v is the choice of an equivalence class of optimal embeddings. This can be made precise as follows.

If $v \mid nm$ and $v \nmid c$, then $m_v = 2$. The choice of an orientation can be performed as follows. For $v \mid nm$ and $v \nmid c$, define

$$U_v(r, O) := \text{Hom}(r_v, O_v)/O_v^\times.$$

The choice of an *orientation* o_v at the primes $v \mid nm$ and $v \nmid c$ is the choice of an element in $U_v(r, O)$. Say that a point $(x, \psi) \in \text{CM}(c)$ is *oriented* at a prime $v \mid nm$ and $v \nmid c$ (with respect to the chosen orientation o_v) if $x^{-1}\psi x$ and o_v define the same element in $U_v(r, O)$. For more details, see Section 2.1.1 in [48].

Let now $v \mid m$ and $v \mid c$, so r_v is not maximal. In this case too, $m_v = 2$ (see [47], page 94). The choice of an orientation can be performed as follows. The set of maximal orders (respectively, Eichler orders of level v) of $\text{GL}_2(k_v)$ can be identified with the set of vertices \mathcal{V}_v (respectively, unoriented edges \mathcal{E}_v) of the homogeneous tree \mathcal{T}_v of degree $|v|$. Let v_0 (respectively, e_0) denote the vertex (respectively, the edge) corresponding to the maximal order $\text{GL}_2(r_v)$ (respectively, the Eichler order $\Gamma_0(v) \subseteq \text{GL}_2(r_v)$ of level v consisting of matrices which are upper triangular modulo v). Say that a vertex v is *even* (respectively, *odd*) if its distance from v_0 is even (respectively, odd) and define an *orientation* $s, t: \mathcal{E}_v \rightarrow \mathcal{V}_v$ by requiring that for any edge e , $s(e) = v_{\text{even}}$ and $t(e) = v_{\text{odd}}$, where e is the edge joining v_{even} and v_{odd} and v_{even} and v_{odd} are even and odd, respectively.

Let $(x, \psi) \in \text{CM}(c)$. Then $\psi: k_v \rightarrow D_v$ is an optimal embedding of r_v into O_x . Fix an isomorphism $\iota_v: D_v \rightarrow M_2(k_v)$. Then O_x can be identified with an edge $e_{O_x} = (s(e_{O_x}), t(e_{O_x}))$ in such a way that O_x is the intersection of the two maximal orders represented by $s(e_{O_x})$ and $t(e_{O_x})$. Finally, let r' be the quadratic order containing r of conductor c/v . Say that (x, ψ) is *oriented* (with respect to the chosen orientations s, t) if the v -component ψ_v of ψ is an optimal embedding of r'_v into the maximal order corresponding to $s(e_{O_x})$. Note that, in this case, ψ must be an optimal embedding of r_v into the maximal order corresponding to $t(e_{O_x})$.

Fix orientations $o_v \in U_v(r, O)$ for $v \mid mn$ and $v \nmid c$ and orientations $s, t: \mathcal{E}_v \rightarrow \mathcal{V}_v$ for $v \mid m$ and $v \mid c$. A *Gross point* of conductor c is a CM-point $(x, \psi) \in \text{CM}(c)$ which is oriented at all $v \mid mn$.

4. p -adic L -functions

4.1. Modular forms on definite quaternion algebras. Let B/F be the quaternion algebra of discriminant \mathfrak{n}^- which is ramified at all archimedean places. Fix an Eichler order $R \subseteq B$ of level \mathfrak{n}^+ .

Let $f \in S_2(\mathfrak{n})$ be a Hilbert modular cuspform of parallel weight 2 and trivial central character with respect to the $\Gamma_0(\mathfrak{n})$ -level structure. Let $\mathbb{T}_{\mathfrak{n}}$ be the Hecke algebra acting faithfully on $S_2(\mathfrak{n})$ (see Section 3.1 in [48] for precise definitions).

Denote by $S_2^B(\wp\mathfrak{n}^+)$ the \mathbb{C} -vector space of functions

$$B^\times \backslash \widehat{B}^\times / \widehat{R}^\times \longrightarrow \mathbb{C}.$$

There is an action of the Hecke algebra $\mathbb{T}_{\mathfrak{n}}$ on $S_2^B(\wp\mathfrak{n}^+)$ defined as usual via double cosets. The Jacquet–Langlands correspondence implies that (up to scaling) there is a unique modular form $f^B \in S_2^B(\wp\mathfrak{n}^+)$ having the same eigenvalues as f under the action of the Hecke algebra. If the Hecke eigenvalues on a Hilbert modular form f are contained in a ring \mathcal{O} , then f^B can be normalized to take values in \mathcal{O} .

4.2. CM points on definite quaternion algebras. Since all primes dividing the discriminant of B are inert in K , there exists an embedding $K \hookrightarrow B$, so that K can be regarded as a subfield of B via this fixed embedding $\bar{\Psi}$. Following the notation in Section 3, define the set of CM-points by R to be

$$\mathrm{CM}_R := \bar{\Psi}(K)^\times \backslash \widehat{B}^\times / \widehat{R}^\times$$

and say that a point $x \in \mathrm{CM}_R$ has *conductor* \mathfrak{c} if

$$\bar{\Psi}(K) \cap x \widehat{R} x^{-1} = \mathcal{O}_{\mathfrak{c}}.$$

Denote by $\mathrm{CM}_R(\mathfrak{c})$ the set of CM points of conductor \mathfrak{c} . Following Section 3, the set $\mathrm{CM}_R(\mathfrak{c})$ can also be described as the set of points in

$$X_R(K) := B^\times \backslash (\widehat{B}^\times \times \mathrm{Hom}(K, B)) / \widehat{R}^\times$$

such that Ψ is an optimal embedding of $\mathcal{O}_{\mathfrak{c}}$ into the Eichler order $B \cap x \widehat{R}^\times x^{-1}$; explicitly,

$$\Psi(K) \cap x \widehat{R}^\times x^{-1} = \Psi(\mathcal{O}_{\mathfrak{c}}).$$

Since all primes dividing \mathfrak{n}^+ are split in K , $\mathrm{CM}_R(\wp^m)$ is non empty for all $m \geq 1$. The group $\tilde{G}_{\wp^m} \simeq \widehat{K}^\times / K^\times \widehat{\mathcal{O}}_{\wp^m}^\times$ acts on $\mathrm{CM}_R(\wp^m)$ by left translation, as described in Section 3.

Fix a positive integer m . Choose orientations for the optimal embeddings of \mathcal{O}_{\wp^m} into R as in Section 3 for all primes \mathfrak{q} dividing \mathfrak{n} : this amounts to choose orientations $o_{\mathfrak{q}} \in U_{\mathfrak{q}}(\mathcal{O}_{\wp^m}, R)$ for all primes $\mathfrak{q} \mid \mathfrak{n}^+ \mathfrak{n}^-$ and an orientation $s, t: \mathcal{E}_{\wp} \rightarrow \mathcal{V}_{\wp}$ at the prime \wp . Let $\mathrm{Gr}(\wp^m)$ denote the set of Gross points of conductor \wp^m with respect to these orientations and define

$$\mathrm{Gr}(\wp^\infty) := \bigcup_{m=1}^{\infty} \mathrm{Gr}(\wp^m).$$

If $P = (x, \Psi) \in \mathrm{Gr}(\wp^m)$, then the local component $\Psi_{\wp}: K_{\wp} \rightarrow B_{\wp}$ of Ψ is an optimal embedding of the completion $\mathcal{O}_{\wp^m, \wp}$ of \mathcal{O}_{\wp^m} at \wp into $x R_{\wp} x^{-1}$, where R_{\wp} is the completion of R at \wp . Let $e_P = (s(e_P), t(e_P)) \in \mathcal{E}_{\wp}$ be the edge corresponding to $x R_{\wp} x^{-1}$ as described in Section 3. Say that a sequence $(P_m)_{m \geq 1}$ of points in $\mathrm{Gr}(\wp^\infty)$, with $P_m \in \mathrm{Gr}(\wp^m)$, is *compatible* if $t(e_{P_m}) = s(e_{P_{m+1}})$ for all integers $m \geq 1$.

Remark 4.1. If $P = (x, \Psi) \in \text{Gr}(\mathfrak{g}^m)$ with $m \geq 1$, then the pair (x, Ψ) also defines a CM-point of conductor \mathfrak{g}^{m-1} in $X_{R_0}(K)$, where $R_0 \supset R$ is an Eichler order of B of level π^+ chosen in such a way that $R_{0,\mathfrak{p}}$ corresponds to $s(e_P)$.

4.3. Anticyclotomic \mathfrak{p} -adic L functions. Let f^B be the modular form on the quaternion algebra B associated to f via the Jacquet–Langlands correspondence and define the following map:

$$\eta: \bar{\psi}(K)^\times \backslash \widehat{B}^\times / \widehat{R}^\times \xrightarrow{\mu} B^\times \backslash \widehat{B}^\times / \widehat{R}^\times \xrightarrow{f^B} \mathcal{O}_f,$$

where μ is the canonical projection. Choose points $x_m \in \text{CM}_R(\mathfrak{g}^m)$ in such a way that the sequence $(x_m)_m$ is compatible. The orientation $s, t: \mathcal{E}_\mathfrak{p} \rightarrow \mathcal{V}_\mathfrak{p}$ being fixed as above, the action of $U_\mathfrak{p}$ on an edge $e \in \mathcal{E}_\mathfrak{p}$ can be described as $U_\mathfrak{p}(e) = \sum_{e'} e'$, where the sum is over all edges e' such that $s(e') = t(e)$. The choice of the compatible sequence of Gross points made before shows then that for $m \geq 2$,

$$\sum_{g \in \text{Gal}(\tilde{K}_{\mathfrak{p}^m} / \tilde{K}_{\mathfrak{p}^{m-1}})} \mu(gx_m) = U_\mathfrak{p}(\mu(x_{m-1})). \quad (3)$$

Define the *theta elements* for $m \geq 1$:

$$\tilde{\theta}_{f,m} := \sum_{g \in \tilde{G}_{\mathfrak{p}^m}} \alpha_\mathfrak{p}^{-m} \eta(gx_m) g \in \mathcal{O}_{f,\pi}[\tilde{G}_{\mathfrak{p}^m}].$$

Denote by $v_{m+1,m}: \mathcal{O}_{f,\pi}[\tilde{G}_{\mathfrak{p}^{m+1}}] \rightarrow \mathcal{O}_{f,\pi}[\tilde{G}_{\mathfrak{p}^m}]$ the homomorphisms induced by the projection maps $\tilde{G}_{\mathfrak{p}^{m+1}} \rightarrow \tilde{G}_{\mathfrak{p}^m}$. By Equation (3), the elements $\tilde{\theta}_{f,m}$ verify the following relation:

$$v_{m+1,m}(\tilde{\theta}_{f,m}) = \tilde{\theta}_{f,m-1}.$$

Taking the inverse limit with respect to the projection maps $v_{m+1,m}$ yields an element

$$\tilde{\theta}_f := \varprojlim_m \tilde{\theta}_{f,m} \in \mathcal{O}_{f,\pi}[\tilde{G}_{\mathfrak{p}^\infty}] := \varprojlim_m \mathcal{O}_{f,\pi}[\tilde{G}_{\mathfrak{p}^m}].$$

The group ring $\mathcal{O}_{f,\pi}[\tilde{G}_{\mathfrak{p}^\infty}]$ is endowed with a canonical involution $x \mapsto x^*$ defined to be the extension by $\mathcal{O}_{f,\pi}$ -linearity of the involution $\sigma \mapsto \sigma^{-1}$ of $\tilde{G}_{\mathfrak{p}^\infty}$. Define

$$\tilde{L}_{\mathfrak{p},\pi}(f/K) := \tilde{\theta}_f \tilde{\theta}_f^* \in \mathcal{O}_{f,\pi}[\tilde{G}_{\mathfrak{p}^\infty}].$$

Since $\tilde{\theta}_f$ is well defined up to multiplication by an element of $\tilde{G}_{\mathfrak{p}^\infty}$, the definition of $\tilde{L}_{\mathfrak{p},\pi}(f/K)$ is independent on the choice of the Gross points x_m . Set $\tilde{\Lambda}_{\mathfrak{p},\pi} := \mathcal{O}_{f,\pi}[\tilde{G}_{\mathfrak{p}^\infty}]$ and denote by $\lambda: \tilde{\Lambda}_{\mathfrak{p},\pi} \rightarrow \Lambda_{\mathfrak{p},\pi}$ the projection induced by the inclusion $K_{\mathfrak{p}^\infty} \subseteq \tilde{K}_{\mathfrak{p}^\infty}$.

Definition 4.2. Define the *anticyclotomic \wp -adic L -function* attached to f and K to be the element

$$L_{\wp,\pi}(f/K) := \lambda(\tilde{L}_{\wp,\pi}(f/K)) \in \Lambda_{\wp,\pi}.$$

Furthermore, define $\theta_{f,n} := \lambda(\tilde{\theta}_{f,n})$ and $\theta_f := \lambda(\tilde{\theta}_f)$, so that $L_{\wp,\pi}(f/K) = \theta_f \theta_f^*$ and $\theta_f = \varprojlim_n \theta_{f,n}$.

4.4. Interpolation properties. Let $\chi: \tilde{G}_{\wp^\infty} \rightarrow \mathcal{O}^\times$ be a ramified finite order character, where \mathcal{O} is the ring of integers of a finite extension of \mathbb{Q}_p . Extend χ to an homomorphism, denoted by the same symbol, $\chi: \mathcal{O}_{f,\pi}[\tilde{G}_{\wp^\infty}] \rightarrow \mathcal{O}$. Zhang, generalizing [17], proves in Theorem 1.3.2 of [49] the following interpolation formula:

$$L(f, \chi, 1) = C \cdot |\ell(\chi)|^2$$

where

$$\ell(\chi) := \chi(\tilde{L}_{\wp,\pi}(f/K)) \quad \text{and} \quad C := 2^g d_{K/F}^{-1/2} (\|f^\sharp\| / \|f^B\|)^2.$$

In the above formulas we use a fixed embedding $\bar{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$ to view $\ell(\chi)$ as a complex number; furthermore, $d_{K/F}$ is the discriminant of K over F , the symbol $\|\cdot\|$ denotes the L^2 -norm in $S_2^B(\wp n^+)$ with respect to a suitable measure (defined in [49], Theorem 1.3.2) on the idele ring $B_{\mathbb{A}}^\times$ of B and, finally, f^\sharp is the *quasi newform* associated to f defined in [49], §1.1. In particular, $C \neq 0$ and we obtain (see also Theorem 6.4 in [46]):

$$\ell(\chi) \neq 0 \text{ if and only if } L_K(f, \chi, 1) \neq 0.$$

The arithmetic assumptions we are working with imply that the sign of the functional equation of $L_K(f, \chi, 1)$ is $+1$ and, by [8], Theorem 1.4, that $L_K(f, \chi, 1) \neq 0$ for infinitely many characters χ as above. Hence $\tilde{L}_{\wp,\pi}(f/K) \neq 0$. Since $\tilde{G}_{\wp^\infty} \simeq G_{\wp^\infty} \times \Delta_\wp$ and Δ_\wp is finite, it follows that $L_{\wp,\pi}(f/K) \neq 0$.

5. Selmer groups attached to Hilbert modular forms

5.1. Galois cohomology groups

5.1.1. Galois representations. Let T_{f,π^∞} be the $G_F = \text{Gal}(\bar{F}/F)$ -module, free of rank 2 over $\mathcal{O}_{f,\pi}$, associated to the representation $\rho_{f,\pi^\infty}: \text{Gal}(\bar{F}/F) \rightarrow \text{GL}_2(\mathcal{O}_{f,\pi})$; define $K_{f,\pi} := \text{Frac}(\mathcal{O}_{f,\pi})$ and

$$V_{f,\pi^\infty} := T_{f,\pi^\infty} \otimes_{\mathcal{O}_{f,\pi}} K_{f,\pi}; \quad A_{f,\pi^\infty} := V_{f,\pi^\infty} / T_{f,\pi^\infty};$$

$$T_{f,\pi^n} := T_{f,\pi^\infty} / \pi^n T_{f,\pi^\infty}; \quad A_{f,\pi^n} = A_{f,\pi^\infty}[\pi^n].$$

As $\mathcal{O}_{f,\pi}$ -modules, $A_{f,\pi^\infty} \simeq (K_{f,\pi}/\mathcal{O}_{f,\pi})^2$ while both T_{f,π^n} and A_{f,π^n} are $\mathcal{O}_{f,\pi}/\pi^n$ -modules free of rank 2 and there is an isomorphism of G_F -modules $T_{f,\pi^n} \simeq A_{f,\pi^n}$. Furthermore,

$$A_{f,\pi^\infty} \simeq \varinjlim_n A_{f,\pi^n} \quad \text{and} \quad T_{f,\infty} \simeq \varprojlim_n T_{f,\pi^n}$$

with respect to the canonical maps.

5.1.2. Global cohomology groups. Let v denote a positive integer or ∞ . Define the following groups:

$$H^1(K_{\wp^\infty}, A_{f,\pi^v}) := \varinjlim_m H^1(K_{\wp^m}, A_{f,\pi^v}),$$

where the direct limit is with respect to the restriction maps, and

$$\hat{H}^1(K_{\wp^\infty}, T_{f,\pi^v}) := \varprojlim_m H^1(K_{\wp^m}, T_{f,\pi^v}),$$

where the inverse limit is with respect to the corestriction maps.

5.1.3. Local cohomology groups. For each prime $\mathfrak{q} \subseteq \mathcal{O}_F$, let $K_{\wp^m, \mathfrak{q}} := K_{\wp^m} \otimes_F F_{\mathfrak{q}} = \bigoplus_{\mathfrak{q}'|\mathfrak{q}} K_{\wp^m, \mathfrak{q}'}$ where the sum is over the prime ideals $\mathfrak{q}' \mid \mathfrak{q}$ of the ring of integers $\mathcal{O}_{K_{\wp^m}}$ of K_{\wp^m} and $K_{\wp^m, \mathfrak{q}'}$ is the completion of K_{\wp^m} at \mathfrak{q}' . For any $\text{Gal}(\bar{K}/K_{\wp^m})$ -module M , define $H^1(K_{\wp^m, \mathfrak{q}}, M) := \bigoplus_{\mathfrak{q}'|\mathfrak{q}} H^1(K_{\wp^m, \mathfrak{q}'}, M)$. Then define as above for v a positive integer or ∞ ,

$$H^1(K_{\wp^\infty, \mathfrak{q}}, A_{f,\pi^v}) := \varinjlim_m H^1(K_{\wp^m, \mathfrak{q}}, A_{f,\pi^v}),$$

where the direct limit is with respect to the restriction maps, and

$$\hat{H}^1(K_{\wp^\infty, \mathfrak{q}}, T_{f,\pi^v}) := \varprojlim_m H^1(K_{\wp^m, \mathfrak{q}}, T_{f,\pi^v}),$$

where the inverse limit is with respect to the corestriction maps.

5.2. Selmer groups. The definitions of $\text{Sel}_{\pi^n}(f/K_{\wp^\infty})$ and $\text{Sel}_{\pi^\infty}(f/K_{\wp^\infty})$ require the introduction of the following finite/singular and ordinary structures. For any prime ideal \mathfrak{q} of \mathcal{O}_F and any prime ideal \mathfrak{q}' of $\mathcal{O}_{K_{\wp^m}}$ above \mathfrak{q} , choose a decomposition subgroup $G_{m, \mathfrak{q}'} \subseteq G_{K_{\wp^m}}$ at \mathfrak{q}' and let $I_{m, \mathfrak{q}'} \subseteq G_{m, \mathfrak{q}'}$ denote the inertia subgroup.

5.2.1. Primes $\mathfrak{q} \nmid \mathfrak{n}p$. Let M denote A_{f,π^n} or T_{f,π^n} . Fix $\mathfrak{q} \subseteq \mathcal{O}_F$ a prime ideal such that $\mathfrak{q} \nmid \mathfrak{n}p$. The *singular part* of $H^1(K_{\wp^m,\mathfrak{q}}, M)$ is

$$H_{\text{sing}}^1(K_{\wp^m,\mathfrak{q}}, M) := \bigoplus_{\mathfrak{q}'|\mathfrak{q}} H^1(I_{m,\mathfrak{q}'}, M)^{\text{Gal}(K_{\wp^m,\mathfrak{q}'}^{\text{unr}}/K_{\wp^m,\mathfrak{q}'})},$$

where the sum is over all prime ideals \mathfrak{q}' of $\mathcal{O}_{K_{\wp^m}}$ dividing \mathfrak{q} . The kernel of the *residue map* $\partial_{\mathfrak{q}}: H^1(K_{\wp^m,\mathfrak{q}}, M) \rightarrow H_{\text{sing}}^1(K_{\wp^m,\mathfrak{q}}, M)$ is the *finite part* of $H^1(K_{\wp^m,\mathfrak{q}}, M)$ and is denoted by $H_{\text{fin}}^1(K_{\wp^m,\mathfrak{q}}, M)$. Define

$$H_{\text{fin}}^1(K_{\wp^\infty,\mathfrak{q}}, A_{f,\pi^n}) := \varinjlim_m H_{\text{fin}}^1(K_{\wp^m,\mathfrak{q}}, A_{f,\pi^n}),$$

$$H_{\text{sing}}^1(K_{\wp^\infty,\mathfrak{q}}, A_{f,\pi^n}) := \varinjlim_m H_{\text{sing}}^1(K_{\wp^m,\mathfrak{q}}, A_{f,\pi^n}),$$

where the direct limits are with respect to restriction maps, and

$$\hat{H}_{\text{fin}}^1(K_{\wp^\infty,\mathfrak{q}}, T_{f,\pi^n}) := \varprojlim_m H_{\text{fin}}^1(K_{\wp^m,\mathfrak{q}}, T_{f,\pi^n}),$$

$$\hat{H}_{\text{sing}}^1(K_{\wp^\infty,\mathfrak{q}}, T_{f,\pi^n}) := \varprojlim_m H_{\text{sing}}^1(K_{\wp^m,\mathfrak{q}}, T_{f,\pi^n}),$$

where the inverse limits are with respect to the corestriction maps. The cohomology groups $H_{\text{fin}}^1(K_{\wp^\infty,\mathfrak{q}}, A_{f,\pi^n})$ and $\hat{H}_{\text{fin}}^1(K_{\wp^\infty,\mathfrak{q}}, T_{f,\pi^n})$ are the exact annihilators of each other under the local Tate pairing $\langle \cdot, \cdot \rangle_{\mathfrak{q}}$ (for a proof, see [34], Theorem 2.6). If $\mathfrak{q} = \mathfrak{q}_1\mathfrak{q}_2$ is split in K/F , the Frobenius element at \mathfrak{q}_i topologically generates a finite index subgroup in G_{\wp^∞} . Hence there are only a finite number of prime ideals \mathfrak{q}' of K_{\wp^∞} over \mathfrak{q} and for each of them, $K_{\wp^\infty,\mathfrak{q}'}$ is the unramified \mathbb{Z}_p -extension of $K_{\mathfrak{q}}$. It follows that any unramified class of $H^1(K_{\wp^m,\mathfrak{q}}, A_{f,\pi^n})$ becomes trivial after restriction to $H^1(K_{\wp^r,\mathfrak{q}}, A_{f,\pi^n})$ for r sufficiently large. Hence, if \mathfrak{q} is split in K/F ,

$$H_{\text{fin}}^1(K_{\wp^\infty,\mathfrak{q}}, A_{f,\pi^n}) = 0 \text{ and } \hat{H}_{\text{sing}}^1(K_{\wp^\infty,\mathfrak{q}}, T_{f,\pi^n}) = 0,$$

where the second assertion follows from the non-degeneracy of the local Tate pairing. If \mathfrak{q} is inert in K/F , then it splits completely in K_{\wp^∞} (this observation is due to Iwasawa [23]). It follows that, if \mathfrak{q} is inert in K/F ,

$$\hat{H}_{\text{sing}}^1(K_{\wp^\infty,\mathfrak{q}}, T_{f,\pi^n}) \simeq H_{\text{sing}}^1(K_{\mathfrak{q}}, T_{f,\pi^n}) \otimes \Lambda_{\wp,\pi}$$

and

$$H_{\text{fin}}^1(K_{\wp^\infty,\mathfrak{q}}, A_{f,\pi^n}) \simeq \text{Hom}(H_{\text{sing}}^1(K_{\mathfrak{q}}, T_{f,\pi^n}) \otimes \Lambda_{\wp,\pi}, K_{f,\pi}/\mathcal{O}_{f,\pi}).$$

Remark 5.1. To explain the above definitions, let ℓ be a prime number, K/\mathbb{Q}_ℓ a finite extension and A/K an abelian variety with good reduction. Let $p \neq \ell$ a prime

and denote by G_K and I_K the absolute Galois group of K and its inertia subgroup, respectively. Finally, let

$$\kappa: A(K) \longrightarrow H^1(K, A[p^n])$$

denote the Kummer map, where n is a non-negative integer. Then

$$\text{Im}(\kappa) = H^1(G_K/I_K, A[p^n]) = \ker(H^1(G_K, A[p^n]) \longrightarrow H^1(I_K, A[p^n])^{G_K/I_K}).$$

For a proof, see [34] (Chapter 1, Proposition 3.8) or Lemma 7 in [18].

5.2.2. Primes $\mathfrak{q} \mid \mathfrak{n}$ and $\mathfrak{q} \nmid p$. Fix a prime $\mathfrak{q} \nmid p$ which divides \mathfrak{n} . By Assumption 1.3,

$$A_{f,\pi^n}^{(\mathfrak{q})} := A_{f,\pi^n}^{I_{F\mathfrak{q}}} \simeq K_{f,\pi}/\mathcal{O}_{f,\pi}.$$

The *ordinary part* of the group $H^1(K_{\wp^m,\mathfrak{q}}, A_{f,\pi^n})$ is defined to be the unramified cohomology

$$H_{\text{ord}}^1(K_{\wp^m,\mathfrak{q}}, A_{f,\pi^n}) := H^1(G_{K_{\wp^m,\mathfrak{q}}}/I_{K_{\wp^m,\mathfrak{q}}}, A_{f,\pi^n}^{(\mathfrak{q})}).$$

Define

$$H_{\text{ord}}^1(K_{\wp^\infty,\mathfrak{q}}, A_{f,\pi^n}) := \varinjlim_m H_{\text{ord}}^1(K_{\wp^m,\mathfrak{q}}, A_{f,\pi^n}),$$

where the direct limit is with respect to the restriction maps. Note that if $\mathfrak{q} \mid \mathfrak{n}^+$ and $\mathfrak{q} \nmid p$, then, by an argument similar to that of Section 5.2.1, $H_{\text{ord}}^1(K_{\wp^\infty,\mathfrak{q}}, A_{f,\pi^n}) = 0$.

Remark 5.2. To explain the above definitions, let ℓ be a prime number, K/\mathbb{Q}_ℓ a finite extension and A/K an abelian variety with purely toric reduction. Suppose that there exists an extension E/\mathbb{Q} such that $[E:\mathbb{Q}] = \dim(A)$ and an embedding $\mathcal{O}_E \hookrightarrow \text{End}(A)$, where \mathcal{O}_E is the ring of integers of E . Let $p \neq \ell$ a prime and \mathfrak{p} a prime ideal of \mathcal{O}_E of residual characteristic p . Denote by G_K and I_K the absolute Galois group of K and its inertia subgroup, respectively. Suppose that the inertia invariants $A[\mathfrak{p}^n]^{I_K}$ of $A[\mathfrak{p}^n]$ are one-dimensional over the field $\mathcal{O}_E/\mathfrak{p}$. Finally, let

$$\kappa: A(K) \longrightarrow H^1(K, A[\mathfrak{p}^n])$$

denote the Kummer map, where n is a non-negative integer. Then

$$\text{Im}(\kappa) = H^1(G_K/I_K, A[\mathfrak{p}^n]^{I_K}).$$

For a proof in the case $n = 1$, see Lemma 4, Lemma 6 and Section 3.3 in [18]. The general case ($n > 1$) can be obtained by a direct generalization of the arguments used in the case $n = 1$.

5.2.3. Primes $\mathfrak{p} \mid p$. Let $\mathfrak{p} \mid p$ be a prime ideal. Let $I_{F_{\mathfrak{p}}} \subseteq G_{F_{\mathfrak{p}}} := \text{Gal}(\bar{F}_{\mathfrak{p}}/F_{\mathfrak{p}})$ denote the inertia subgroup. Since f is ordinary at \mathfrak{p} , there is an exact sequence of $I_{F_{\mathfrak{p}}}$ -modules

$$0 \longrightarrow A_{f,\pi\infty}^{(\mathfrak{p})} \longrightarrow A_{f,\pi\infty} \longrightarrow A_{f,\pi\infty}^{(1)} \longrightarrow 0 \quad (4)$$

such that the submodule $A_{f,\pi\infty}^{(\mathfrak{p})}$ and the quotient $A_{f,\pi\infty}^{(1)}$ are both isomorphic to $K_{f,\pi}/\mathcal{O}_{f,\pi}$ as groups and $I_{F_{\mathfrak{p}}}$ acts on $A_{f,\pi\infty}^{(\mathfrak{p})}$ via the cyclotomic character

$$\epsilon_p: \text{Gal}(\bar{F}/F) \rightarrow \text{Aut}(\mu_{p^\infty})$$

describing the action of $\text{Gal}(\bar{F}/F)$ on the group μ_{p^∞} of p -power roots of unity, and acts trivially on $A_{f,\pi\infty}^{(1)}$. Let

$$\lambda_{\mathfrak{p},m}: H^1(K_{\wp^m,\mathfrak{p}}, A_{f,\pi\infty}^{(\mathfrak{p})}) \longrightarrow H^1(K_{\wp^m,\mathfrak{p}}, A_{f,\pi\infty})$$

be the map of cohomology groups induced by the inclusion $A_{f,\pi\infty}^{(\mathfrak{p})} \subseteq A_{f,\pi\infty}$. Define the *ordinary part* $H_{\text{ord}}^1(K_{\wp^m,\mathfrak{p}}, A_{f,\pi\infty})$ of $H^1(K_{\wp^m,\mathfrak{p}}, A_{f,\pi\infty})$ to be the maximal divisible subgroup of $\text{Im}(\lambda_{\mathfrak{p},m})$. Then define

$$H_{\text{ord}}^1(K_{\wp^\infty,\mathfrak{p}}, A_{f,\pi\infty}) := \varinjlim_m H_{\text{ord}}^1(K_{\wp^m,\mathfrak{p}}, A_{f,\pi\infty}),$$

where the direct limit is with respect to the restriction maps.

Remark 5.3. To justify the above definition, let $A[p^\infty]$ be the maximal p -divisible group of $A(\bar{K})$, where A/K is an ordinary abelian variety defined over a finite extension K of \mathbb{Q}_p . Let \mathcal{F} be the formal group over \mathcal{O}_K attached to the Néron model for A over \mathcal{O}_K and define $C := \mathcal{F}(\bar{\mathfrak{m}})[p^\infty]$, where $\bar{\mathfrak{m}}$ is the maximal ideal of the algebraic closure of K . Finally, define the map: $\lambda: H^1(K, C) \rightarrow H^1(K, A[p^\infty])$ induced by the inclusion $C \hookrightarrow A[p^\infty]$. Then the image of the Kummer map $\kappa: A(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(K, A[p^\infty])$ is equal to the maximal divisible subgroup $(\text{Im}(\lambda))_{\text{div}}$ of $\text{Im}(\lambda)$. For proofs, see [7], Proposition 4.5. Moreover, if K_∞/K is a deeply ramified extension (see [7], Section 2, for definitions), then the image of the Kummer map $A(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(K_\infty, A[p^\infty])$ coincides with the image of $\lambda: H^1(K_\infty, C) \rightarrow H^1(K_\infty, A[p^\infty])$ by [7], Proposition 4.3.

Note that for each prime \mathfrak{p}' of K_{\wp^∞} over \mathfrak{p} , the extension $K_{\wp^\infty,\mathfrak{p}'}/K_{\mathfrak{p}}$ is deeply ramified. The last lines of Remark 5.3 show that one could equivalently define $H_{\text{ord}}^1(K_{\wp^\infty,\mathfrak{p}}, A_{f,\pi\infty})$ to be the image of

$$\lambda_{\mathfrak{p},\infty}: H^1(K_{\wp^\infty,\mathfrak{p}}, A_{f,\pi\infty}^{(\mathfrak{p})}) \longrightarrow H^1(K_{\wp^\infty,\mathfrak{p}}, A_{f,\pi\infty}).$$

Define

$$\mathcal{H}(\mathfrak{p}, m, n) := H_{\text{ord}}^1(K_{\wp^m,\mathfrak{p}}, A_{f,\pi\infty}) \cap H^1(K_{\wp^m,\mathfrak{p}}, A_{f,\pi^n}).$$

For any subgroup $\mathcal{H} \subseteq H^1(K_{\wp^m, \mathfrak{p}}, A_{f, \pi^n})$, use the isomorphism $A_{f, \pi^n} \simeq T_{f, \pi^n}$ to define a subgroup $\mathcal{H}^* \subseteq H^1(K_{\wp^m, \mathfrak{p}}, T_{f, \pi^n})$ such that $\mathcal{H} \simeq \mathcal{H}^*$. Then define $H_{\text{ord}}^1(K_{\wp^m, \mathfrak{p}}, A_{f, \pi^n})$ to be the maximal subgroup of $H^1(K_{\wp^m, \mathfrak{p}}, A_{f, \pi^n})$ containing $\mathcal{H}(\mathfrak{p}, m, n)$ and such that $H_{\text{ord}}^1(K_{\wp^m, \mathfrak{p}}, A_{f, \pi^n})$ and $H_{\text{ord}}^1(K_{\wp^m, \mathfrak{p}}, A_{f, \pi^n})^*$ are the exact annihilators of each other under the local Tate pairing at \mathfrak{p} . Finally, set

$$H_{\text{ord}}^1(K_{\wp^\infty, \mathfrak{p}}, A_{f, \pi^n}) := \varinjlim_m H_{\text{ord}}^1(K_{\wp^m, \mathfrak{p}}, A_{f, \pi^n}),$$

where the direct limit is with respect to the restriction maps.

Remark 5.4. Let $A[p^n]$ be the p^n -torsion of an abelian variety A/K as in Remark 5.3. The image of the Kummer map $\kappa: A(K)/p^n \hookrightarrow H^1(K, A[p^n])$ contains the subgroup $\mathcal{H} := \text{Im}(\lambda)_{\text{div}} \cap H^1(K, A[p^n])$, where λ is the map defined in Remark 5.3. Since $\text{Im}(\kappa)$ is maximal isotropic for the local Tate pairing, then it coincides with the maximal isotropic subgroup of $H^1(K, A[p^n])$ containing \mathcal{H} .

5.2.4. Selmer groups. Let M_{f, π^n} denote A_{f, π^n} or T_{f, π^n} . For any prime \mathfrak{q} , let

$$\text{res}_{\mathfrak{q}}: H^1(K_{\wp^\infty}, M_{f, \pi^n}) \longrightarrow H^1(K_{\wp^\infty, \mathfrak{q}}, M_{f, \pi^n})$$

denote the restriction map. For a prime $\mathfrak{q} \subseteq \mathcal{O}_F$ not dividing $\mathfrak{n}p$, let $\partial_{\mathfrak{q}}$ denote the residue map

$$\partial_{\mathfrak{q}}: H^1(K_{\wp^\infty, \mathfrak{q}}, M_{f, \pi^n}) \longrightarrow H_{\text{sing}}^1(K_{\wp^\infty, \mathfrak{q}}, M_{f, \pi^n})$$

and, by an abuse of notation, denote also by $\partial_{\mathfrak{q}}$ the map obtained by composing $\text{res}_{\mathfrak{q}}$ with $\partial_{\mathfrak{q}}$. If $s \in H^1(K_{\wp^\infty}, M_{f, \pi^n})$ satisfies $\partial_{\mathfrak{q}}(s) = 0$, write $v_{\mathfrak{q}}(s)$ for the image of s in $H_{\text{fin}}^1(K_{\wp^\infty}, M_{f, \pi^n})$.

Definition 5.5. The *Selmer group* $\text{Sel}_{\pi^n}(f/K_{\wp^\infty})$ attached to f, n and K_{\wp^∞} is the group of elements $s \in H^1(K_{\wp^\infty}, A_{f, \pi^n})$ satisfying

- (1) for primes $\mathfrak{q} \nmid \mathfrak{n}p$: $\text{res}_{\mathfrak{q}}(s) \in H_{\text{fin}}^1(K_{\wp^\infty, \mathfrak{q}}, A_{f, \pi^n})$;
- (2) for primes $\mathfrak{q} \mid \mathfrak{n}^-$ and $\mathfrak{q} \nmid p$: $\text{res}_{\mathfrak{q}}(s) \in H_{\text{ord}}^1(K_{\wp^\infty, \mathfrak{p}}, A_{f, \pi^n})$;
- (3) for primes $\mathfrak{q} \mid \mathfrak{n}^+$ and $\mathfrak{q} \nmid p$: $\text{res}_{\mathfrak{q}}(s) = 0$;
- (4) for primes $\mathfrak{p} \mid p$: $\text{res}_{\mathfrak{p}}(s) \in H_{\text{ord}}^1(K_{\wp^\infty, \mathfrak{p}}, A_{f, \pi^n})$.

The Selmer group $\text{Sel}_{\pi^\infty}(f/K_{\wp^\infty})$ is defined to be the direct limit

$$\text{Sel}_{\pi^\infty}(f/K_{\wp^\infty}) := \varinjlim_n \text{Sel}_{\pi^n}(f/K_{\wp^\infty})$$

with respect to the inclusion maps.

Let $\mathfrak{s} \subseteq \mathcal{O}_F$ be a square free ideal prime to \mathfrak{n} . The *compactified Selmer group* $\hat{H}_{\mathfrak{s}}^1(K_{\wp^\infty}, T_{f, \pi^n})$ attached to f, n and K_{\wp^∞} is the groups of elements $\kappa \in \hat{H}^1(K_{\wp^\infty}, T_{f, \pi^n})$ such that

$$\langle \text{res}_{\mathfrak{q}}(\kappa), \text{res}_{\mathfrak{q}}(s) \rangle_{\mathfrak{q}} = 0$$

for all $s \in \text{Sel}_{\pi^n}(f/K_{\wp^\infty})$ and all $\mathfrak{q} \nmid \mathfrak{s}$, where $\langle \cdot, \cdot \rangle_{\mathfrak{q}}$ is the local Tate pairing. The *global reciprocity law of class field theory* implies that for any $s \in \text{Sel}_{\pi^n}(f/K_{\wp^\infty})$ and any $\kappa \in \hat{H}_{\mathfrak{s}}^1(K_{\wp^\infty}, T_{f, \pi^n})$,

$$\sum_{\mathfrak{q} \mid \mathfrak{s}} \langle \partial_{\mathfrak{q}}(\kappa), v_{\mathfrak{q}}(s) \rangle_{\mathfrak{q}} = 0. \quad (5)$$

In the above equation, by an abuse of notation, the symbol $\partial_{\mathfrak{q}}$ denotes the map obtained from $\partial_{\mathfrak{q}}$ by passing to the inverse limit.

6. Iwasawa's Main Conjecture

6.1. The main result. Let

$$\text{Sel}_{\pi^\infty}^\vee(f/K_{\wp^\infty}) := \text{Hom}(\text{Sel}_{\pi^\infty}(f/K_{\wp^\infty}), K_{f, \pi}/\mathcal{O}_{f, \pi})$$

be the Pontryagin dual of $\text{Sel}_{\pi^\infty}(f/K_{\wp^\infty})$. Since $\text{Sel}_{\pi^\infty}^\vee(f/K_{\wp^\infty})$ has a structure of finitely generated $\Lambda_{\wp, \pi}$ -module, there is an exact sequence:

$$0 \longrightarrow M \longrightarrow \text{Sel}_{\pi^\infty}^\vee(f/K_{\wp^\infty}) \longrightarrow \Lambda_{\wp, \pi}^r \oplus_{i=1}^s \Lambda_{\wp, \pi}/(f_i) \longrightarrow N \longrightarrow 0, \quad (6)$$

where $f_i \neq 0$ and M and N are pseudo-null $\Lambda_{\wp, \pi}$ -modules (for definitions of *pseudo-null* $\Lambda_{\wp, \pi}$ -modules, as well as for the notion of *pseudo-isomorphism* of $\Lambda_{\wp, \pi}$ -modules, we refer to Section 7.1). Define the *characteristic power series* of $\text{Sel}_{\pi^\infty}^\vee(f/K_{\wp^\infty})$ to be:

$$\text{Char}_{\wp}(f/K) := \begin{cases} 0, & \text{if } r \neq 0 \\ \prod_{i=1}^s f_i, & \text{if } r = 0. \end{cases}$$

The main result which will be proved in Section 7 is the following:

Theorem 6.1. *Suppose that the assumptions listed in the Introduction are satisfied. The characteristic power series $\text{Char}_{\wp, \pi}(f/K)$ of the Pontryagin dual $\text{Sel}_{\pi^\infty}^\vee(f/K_{\wp^\infty})$ of $\text{Sel}_{\pi^\infty}(f/K_{\wp^\infty})$ divides the p -adic L -function $L_{\wp, \pi}(f/K)$.*

Corollary 6.2. *Suppose that the assumptions listed in the Introduction are satisfied. Then $\text{Sel}_{\pi^\infty}^\vee(f/K_{\wp^\infty})$ is pseudo-isomorphic to a torsion $\Lambda_{\wp, \pi}$ -module.*

Proof. By Theorem 1.4 of [8], $L_{\wp, \pi}(A/K)$ is not identically zero, and therefore $\text{Char}_{\wp, \pi}(f/K) \neq 0$. \square

The proof of this result is based on a generalization of the argument in [5]. In Section 7 a sketch of the argument with the necessary adaptations to the totally real case will be presented.

6.2. Applications to modular abelian varieties

6.2.1. Modular abelian varieties. Let A/F be an abelian variety. Denote by $\text{End}(A)$ its endomorphism ring and define

$$E := \text{End}_{\mathbb{Q}}(A) = \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Say that A is of GL_2 -type if E is a field such that $[E : \mathbb{Q}] = \dim(A)$ and $\text{End}(A)$ is the ring of integers \mathcal{O}_E of E . For any ideal $I \subseteq \mathcal{O}_E$, denote by $A[I]$ the I -torsion in A , by $A[I^\infty]$ the I -primary subgroup of A and by $T_I(A)$ the I -adic Tate module of A . Finally, let

$$\rho_{A,I} : \text{Gal}(\bar{F}/F) \longrightarrow \text{Aut}(T_I(A))$$

be the representation of $\text{Gal}(\bar{F}/F)$ on $T_I(A)$.

Definition 6.3. Say that an abelian variety of GL_2 -type A/F as above is *modular* if there exists a cuspidal Hilbert modular form f of $\Gamma_0(\mathfrak{n})$ -level for some ideal $\mathfrak{n} \subseteq \mathcal{O}_F$, parallel weight 2, trivial central character, which is an eigenform for the Hecke algebra $\mathbb{T}_{\mathfrak{n}}$, such that $E \simeq K_f$ and the ℓ -adic representation $\rho_{A,\ell}$ of $\text{Gal}(\bar{F}/F)$ on the ℓ -adic Tate module $T_\ell(A)$ of A is equivalent to the ℓ -adic representation $\rho_{f,\ell}$ attached to f , where ℓ is a prime number.

Remark 6.4. Since $\mathfrak{n}^- \neq \mathcal{O}_F$ when d is even, Shimura's construction generalized to this context (see [48], Theorem B and Section 3) shows that for f as above there is a modular abelian variety A/F whose associated eigenform is f . Note that Definition 6.3 applies also to the case of $\mathfrak{n}^- = \mathcal{O}_F$ and d even, which however is not considered in this paper. For results in this important case, see [29] and [30].

Assume that the abelian variety A/F satisfies the following:

Assumption 6.5. (1) A/F is a modular abelian variety in the sense of Definition 6.3.

(2) The modular form f associated to A by Definition 6.3 satisfies the assumptions listed in the Introduction.

(3) A/F has *good reduction* at all primes $\mathfrak{q} \nmid \mathfrak{n}$.

(4) A/F has *purely toric reduction* at all primes $\mathfrak{q} \mid \mathfrak{n}$ and $\mathfrak{q} \nmid p$.

(5) A/F has *ordinary reduction* at all prime ideals $\mathfrak{p} \mid p$.

Remark 6.6. If A is ordinary at $\mathfrak{p} \mid p$, then the associated Hilbert modular form is also ordinary at \mathfrak{p} (see [16], Chapter 3, Section 6.2).

Let A/F satisfy Assumption 6.5 above. Define the Selmer groups:

$$\mathrm{Sel}_{\pi^n}(A/K_{\wp^m}) := \ker \left(H^1(K_{\wp^m}, A[\pi^n]) \longrightarrow \prod_{\mathfrak{q}} H^1(K_{\wp^m, \mathfrak{q}}, A(\overline{K_{\wp^m, \mathfrak{q}}})) \right),$$

where the product is over all prime ideals \mathfrak{q} of K_{\wp^m} ,

$$\mathrm{Sel}_{\pi^n}(A/K_{\wp^\infty}) := \varinjlim_m \mathrm{Sel}_{\pi^n}(A/K_{\wp^m})$$

where the direct limit is with respect to the restriction maps, and

$$\mathrm{Sel}_{\pi^\infty}(A/K_{\wp^\infty}) := \varinjlim_n \mathrm{Sel}_{\pi^n}(A/K_{\wp^\infty})$$

where the direct limit is with respect to the maps induced by $A[\pi^n] \subseteq A[\pi^{n+1}]$.

Lemma 6.7. *There are isomorphisms*

$$\mathrm{Sel}_{\pi^n}(f/K_{\wp^\infty}) \simeq \mathrm{Sel}_{\pi^n}(A/K_{\wp^\infty}) \quad \text{and} \quad \mathrm{Sel}_{\pi^\infty}(A/K_{\wp^\infty}) \simeq \mathrm{Sel}_{\pi^\infty}(f/K_{\wp^\infty}).$$

In particular, the characteristic power series of their Pontryagin duals are the same.

Proof. To show the first isomorphism it is necessary to compare the local conditions used in the definition of $\mathrm{Sel}_{\pi^n}(f/K_{\wp^\infty})$ with the image of the local Kummer map

$$\kappa_{\mathfrak{q}'} : A(K_{\wp^\infty, \mathfrak{q}'})/\pi^n \hookrightarrow H^1(K_{\wp^\infty, \mathfrak{q}'}, A[\pi^n])$$

for all prime ideals \mathfrak{q}' in the ring of integers of K_{\wp^∞} . The equality of the local conditions follows from Remark 5.1 for primes $\mathfrak{q}' \nmid \mathfrak{n}p$, from Remark 5.2 for primes $\mathfrak{q}' \mid \mathfrak{n}$, $\mathfrak{q}' \nmid p$ and from Remark 5.4 for primes $\mathfrak{p} \mid p$. The second isomorphism follows by taking the direct limit over n . \square

6.2.2. Arithmetic applications of the main result. Let A/F satisfy Assumption 6.5 above. Define the \wp -adic L -function associated to A/K to be $L_{\wp, \pi}(A/K) := L_{\wp, \pi}(f/K)$. Then Theorem 6.1 and Corollary 6.2 can be restated as follows:

Theorem 6.8. *The characteristic power series $\mathrm{Char}_{\wp, \pi}(A/K)$ of the Pontryagin dual $\mathrm{Sel}_{\pi^\infty}^\vee(A/K_{\wp^\infty})$ of the π -primary Selmer group $\mathrm{Sel}_{\pi^\infty}(A/K_{\wp^\infty})$ of A over K_{\wp^∞} divides the \wp -adic L -function $L_{\wp, \pi}(A/K)$ of A over K . In particular, $\mathrm{Sel}_{\pi^\infty}^\vee(A/K_{\wp^\infty})$ is pseudo-isomorphic to a torsion $\Lambda_{\wp, \pi}$ -module.*

This result on the abelian variety A/F can be used to deduce the following corollaries. Denote by $L_K(A, s)$ and $L_K(A, \chi, s)$ the complex L -function of A over K and its twist by finite order characters $\chi: G_{\wp^\infty} \rightarrow \mathbb{C}^\times$. For any character $\chi: G_{\wp^\infty} \rightarrow \mathcal{O}^\times$, where \mathcal{O} is the valuation ring of a finite extension of \mathbb{Q}_p , denote by the same symbol $\chi: \Lambda_{\wp, \pi} \rightarrow \mathcal{O}$ its extension. Choose an embedding $\overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$ such that χ can also be considered as a complex-valued character. For any $\Lambda_{\wp, \pi}$ -module M , let $M^\chi := M \otimes_\chi \mathcal{O}_{f, \pi}$. Finally, let $\text{III}_{\pi^\infty}(A/K_{\wp^\infty})$ denote the π -primary Tate–Shafarevich group of A/K_{\wp^∞} which is defined by the exactness of the following sequence:

$$0 \longrightarrow A(K_{\wp^\infty}) \otimes (E_\pi/\mathcal{O}_{E, \pi}) \longrightarrow \text{Sel}_{\pi^\infty}(A/K_{\wp^\infty}) \longrightarrow \text{III}_{\pi^\infty}(A/K_{\wp^\infty}) \longrightarrow 0,$$

where E_π and $\mathcal{O}_{E, \pi}$ are the completions of $E = \text{End}_{\mathbb{Q}}(A)$ and $\mathcal{O}_E = \text{End}(A)$ at π .

Corollary 6.9. *Suppose that $[F_\wp : \mathbb{Q}_p] = 1$. If $L_K(A, \chi, 1) \neq 0$, then $A(K_{\wp^\infty})^\chi$ and $\text{III}_{\pi^\infty}(A/K_{\wp^\infty})^\chi$ are finite.*

Proof. In this case the Iwasawa algebra $\Lambda_{\wp, \pi}$ is isomorphic to a power series ring over $\mathcal{O}_{f, \pi}$ in one variable and all pseudo-null $\Lambda_{\wp, \pi}$ -modules are finite. By the interpolation formula, $\chi(L_\wp(f/K)) \neq 0$. By Theorem 6.8, $\chi(\text{Char}_{\wp, \pi}(A, K)) \neq 0$. Hence $\text{Sel}_{\pi^\infty}(A/K_{\wp^\infty})^\chi$ is finite and the result follows. \square

Corollary 6.10. *Suppose $[F_\wp : \mathbb{Q}_p] = 1$ and the torsion subgroup $A(K_{\wp^\infty})_{\text{tors}}$ of $A(K_{\wp^\infty})$ is finite. Then $A(K_{\wp^\infty})$ is finitely generated.*

Proof. As in the proof of Corollary 6.9, note that all pseudo-null $\Lambda_{\wp, \pi}$ -modules are finite. By Theorem 6.8, $\text{Sel}_{\pi^\infty}^\vee(A/K_{\wp^\infty})$ is a torsion $\Lambda_{\wp, \pi}$ -module. The result follows from the classification of torsion $\Lambda_{\wp, \pi}$ -modules because $A(K_{\wp^\infty})_{\text{tors}}$ is finite. \square

Corollary 6.11. *Suppose $[F_\wp : \mathbb{Q}_p] = 1$ and A an elliptic curve. Then $A(K_{\wp^\infty})$ is finitely generated.*

Proof. By definition, A does not have complex multiplication, hence by [32], Proposition 6.12 (ii), $A(K_{\wp^\infty})_{\text{tors}}$ is finite and Corollary 6.10 applies. \square

Remark 6.12. The finiteness of $A(K_{\wp^\infty})_{\text{tors}}$ for more general abelian varieties of GL_2 -type is proved for example in [32], Proposition 6.12 (i), under the condition that the \mathbb{Z}_p -extension is the cyclotomic one. This explains the finiteness assumption added in Corollary 6.10.

7. The proof

7.1. The divisibility criterion. The argument of the proof of Theorem 6.1 is based on the generalization of Proposition 3.1 in [5], which will be obtained in the next Proposition 7.4. For its proof, we need two preliminary results which, for lack of precise references, are stated in the following as Lemma 7.1, Lemma 7.2 and Lemma 7.3.

Let $\Lambda := R[[T_1, \dots, T_m]]$ be a ring of formal power series in $m \geq 1$ variables, where R is the ring of integers of a finite extension of \mathbb{Q}_p and p is a prime number. Choose an uniformizer ϖ of R . Recall that the Noetherian integral domain Λ is a UFD (see for example [42]), so every height one prime ideal of Λ is principal (see for example [31], Theorem 20.1). A finitely generated Λ -module X is said to be *pseudo-null* if its support $\text{Supp}_\Lambda(X)$ contains only prime ideals of height greater than or equal to 2. Two Λ -modules X and Y are said to be *pseudo-isomorphic* if there exist two pseudo-null Λ -modules A and B and an exact sequence of Λ -modules:

$$0 \longrightarrow A \longrightarrow X \longrightarrow Y \longrightarrow B \longrightarrow 0.$$

Let X be a finitely generated Λ -module. By Section 4.4, Théorèmes 4, 5 in [6], X is pseudo-isomorphic to a Λ -module of the form $\Lambda^r \oplus_{i=1}^s \Lambda/(g_i)$, that is, there exists an exact sequence of Λ -modules

$$0 \longrightarrow A \longrightarrow X \longrightarrow \Lambda^r \oplus_{i=1}^s \Lambda/(g_i) \longrightarrow B \longrightarrow 0, \quad (7)$$

where r, s are non-negative integers, A, B are pseudo-null Λ -modules and $g_i \in \Lambda$. By definition the *characteristic power series* $\text{Char}_\Lambda(X)$ attached to the Λ -module X is $\text{Char}_\Lambda(X) := \prod_{i=1}^s g_i$ if $r = 0$ and 0 otherwise. The characteristic power series $\text{Char}_\Lambda(X)$ is well-defined only up to units in Λ ; the *characteristic ideal* $(\text{Char}_\Lambda(X))$ of Λ that it generates is then well defined.

Lemma 7.1. *Let F, G be elements of Λ . Then F divides G if and only if for all morphisms $\varphi: \Lambda \rightarrow \mathcal{O}$, where \mathcal{O} is the ring of integers of a finite extension of \mathbb{Q}_p , $\varphi(F)$ divides $\varphi(G)$.*

Proof. One direction is obvious. For the other direction, we prove the following equivalent statement: If F does not divide G , then there exists a homomorphism $\varphi: \Lambda \rightarrow \mathcal{O}$, where \mathcal{O} is the ring of integers of a finite extension of \mathbb{Q}_p , such that $\varphi(F)$ does not divide $\varphi(G)$. The proof is by induction.

The case $m = 1$ is an easy consequence of the Weierstrass preparation theorem, so we suppose the statement true for $m - 1$ and we prove it for m . For $T := T_1$ and $W := (T_2, \dots, T_m)$, write $F = \sum_{n=0}^{\infty} a_n T^n$ and $G = \sum_{n=0}^{\infty} b_n T^n$ where $a_n, b_n \in R[[W]]$ for $n = 0, \dots, \infty$.

If $a_0 \nmid b_0$, then, by the inductive hypothesis, there exists a homomorphism

$$\varphi: R[[W]] \longrightarrow \mathcal{O}$$

for some \mathcal{O} as above such that $\varphi(a_0) \nmid \varphi(b_0)$. Extend φ to a morphism, denoted by the same letter $\varphi: \Lambda \rightarrow \mathcal{O}$, by setting $\varphi(T) := 0$. Then $\varphi(F)$ does not divide $\varphi(G)$. Hence, in the following suppose that $a_0 \mid b_0$.

If $a_0 \mid b_0$, since F does not divide G , there are elements $c_n \in R[[W]]$, $n = 0, \dots, N-1$ and $N \geq 1$, such that $b_n = \sum_{i=0}^n a_i c_{n-i}$ for $n = 0, \dots, N-1$ and $a_0 \nmid (b_N - \sum_{i=1}^N a_i c_{N-i})$. Hence, by the inductive hypothesis, we see that there exists a morphism $\varphi: R[[W]] \rightarrow \mathcal{O}$ for some \mathcal{O} as above such that $\varphi(a_0) \nmid \varphi(b_N - \sum_{i=1}^N a_i c_{N-i})$. Extend φ to a morphism, denoted by the same letter $\varphi: \Lambda \rightarrow \mathcal{O}[[T]]$, by setting $\varphi(T) := T$. Hence, $\varphi(F)$ does not divide $\varphi(G)$ in $\mathcal{O}[[T]]$. By the inductive hypothesis, there exists $\varphi': \mathcal{O}[[T]] \rightarrow \mathcal{O}'$ such that $\varphi'(\varphi(F))$ does not divide $\varphi'(\varphi(G))$. Defining $\varphi'' := \varphi' \circ \varphi: \Lambda \rightarrow \mathcal{O}'$, yields $\varphi''(F) \nmid \varphi''(G)$. \square

Lemma 7.2. *Let $I = (x_1, \dots, x_n)$ with $n \geq 2$ be an ideal of Λ such that $I \not\subseteq P$ for all prime ideals P of Λ of height one. Then I contains at least two elements without common irreducible factors.*

Proof. The proof is by induction on n . The case $n = 2$ is immediate, so we suppose the result true for $n-1$ and prove it for n . Denote by f the common greatest divisor of the x_i for $i = 1, \dots, n-1$ and write $x'_i := x_i/f$ for $i = 1, \dots, n-1$. Then $J := (x'_1, \dots, x'_{n-1})$ is not contained in any prime ideal of Λ of height one, so, by the inductive hypothesis, there are two elements $g \in J$ and $h \in J$ without common irreducible factors. Then fg and fh are in I and g, h do not have common irreducible factors. Furthermore, any irreducible factor z of x_n may divide g or h (but not both of them) and does not divide f (if it does, then $I \subseteq (z)$, which contradicts our assumption). Write $x_n = ks$ where an irreducible factor z of x_n divides k if and only if z divides gh . Then any irreducible factor of s is prime to gh . If s is invertible, then x_n and $f(g+h) \in I$ do not have irreducible common factors: any irreducible factor of x_n does not divide f and divides exactly one between g and h . Suppose s is not invertible and write $s = \prod_{j=1}^t s_j^{m_j}$, where s_j are irreducible and m_j are non negative integers. If $s_j \mid g + nh$ for some integer $n \neq 0$, then $s_j \nmid g + (m+n)h$ for all integers $m \neq 0$, except possibly those m such that $p \mid m$ in the case when $(s_j) = (\varpi)$: indeed, if $s_j \mid g + (m+n)h$, then $s_j \mid mnh$ and, since $s_j \nmid h, s_j \mid m$, and this is possible only if s_j is a constant, hence $(s_j) = (\varpi)$, so that $p \mid m$. It follows that if $\varpi \nmid s$, then s and $g + mh$ do not have common irreducible factors for all integers m except possibly a finite number of them, while if $\varpi \mid s$, then s and $g + mh$ do not have common irreducible factors for infinitely many integers m . Choose an integer $m \neq 0$ such that s and $g + mh$ do not have common irreducible factors, with the additional condition that $p \nmid m$ if $\varpi \mid k$. Note that there are infinitely many integers m verifying these conditions, even if $R = \mathbb{Z}_2$: indeed, the condition $p \nmid m$ is required only if $\varpi \mid k$, but in this case $\varpi \nmid s$ and there are only a finite number of integers m such that s and $g + mh$ have common irreducible factors. We claim that x_n and $f(g + mh) \in I$ do not have common irreducible factors. Indeed, let $z \mid x_n$ be

an irreducible factor, so that $z \mid k$ or $z \mid s$. If $z \mid k$ then $z \nmid f$ and z divides exactly one of g and h . If $z \mid h$, then, since $z \nmid g$, $z \nmid g + mh$. If $z \mid g$, then $z \nmid mh$: indeed, $z \nmid h$ and, since $m \neq 0$, the only case when $z \mid m$ is that of $(z) = (\varpi)$ and $p \mid m$, but our additional condition on m stipulates that $p \nmid m$ when $\varpi \mid k$. Since $z \mid g$ and $z \nmid mh$, then $z \nmid g + mh$. Hence in any case if $z \mid k$ then $z \nmid f(g + mh)$. If $z \mid s$, then $z = s_j$ for some j , hence $z \nmid g + mh$ and since $s_j \nmid f$ then $s_j \nmid f(g + mh)$. The claim follows, thus completing the proof. \square

If X is a finitely generated Λ -module, denote by $\text{Fitt}_\Lambda(X)$ (respectively, $\text{Ann}_\Lambda(X)$) its Fitting ideal (respectively, its annihilator ideal) over Λ .

Lemma 7.3. *Let X be a finitely generated pseudo-null Λ -module. Then $\text{Fitt}_\Lambda(X)$ contains at least two elements with no common irreducible factors.*

Proof. Recall that a prime ideal P of Λ belongs to the support $\text{Supp}_\Lambda(X)$ of X in Λ if and only if the annihilator $\text{Ann}_\Lambda(X)$ of X in Λ is contained in P (see for example [31], page 26). Fix a prime ideal P of Λ of height 1. By the definition of a pseudo-null submodule, $P \notin \text{Supp}_\Lambda(X)$, so $\text{Ann}_\Lambda(X) \not\subseteq P$. Suppose that X is generated over Λ by h elements. Then by [33], Appendix, 8 on page 325, $\text{Ann}_\Lambda(X)^h \subseteq \text{Fitt}_\Lambda(X)$, hence, since P is a prime ideal, $\text{Fitt}_\Lambda(X) \not\subseteq P$ for all prime ideals P of height 1. The result follows from Lemma 7.2. \square

Proposition 7.4. *Let X be a finitely generated Λ -module and $\mathcal{L} \in \Lambda$. Suppose that $\varphi(\mathcal{L})$ belongs to $\text{Fitt}_\mathcal{O}(X \otimes_\varphi \mathcal{O})$ for all homomorphisms $\varphi: \Lambda \rightarrow \mathcal{O}$, where \mathcal{O} is the ring of integers of a finite extension of \mathbb{Q}_p . Then \mathcal{L} belongs to $(\text{Char}_\Lambda(X))$.*

Proof. If X is not Λ -torsion, then $\text{Fitt}_\Lambda(X) = 0$. Since $\text{Fitt}_\mathcal{O}(X \otimes_\varphi \mathcal{O})$ is equal to $\varphi(\text{Fitt}_\Lambda(X))$, it follows that $\varphi(\mathcal{L}) = 0$ for all φ as above and hence, by Lemma 7.1, $\mathcal{L} = 0$. Assume in the following that X is a Λ -torsion module. Since B in the exact sequence (7) is pseudo-null, by Lemma 7.3 there are at least two elements x_1 and x_2 in $\text{Fitt}_\Lambda(B)$ without common irreducible factors. Tensoring the exact sequence (7) with \mathcal{O} yields

$$\varphi(x_i)\text{Fitt}_\mathcal{O}(X \otimes_\varphi \mathcal{O}) \subseteq (\varphi(\text{Char}_\Lambda(X)))$$

for $i = 1, 2$. By assumption, $\varphi(\text{Char}_\Lambda(X))$ divides $\varphi(x_i\mathcal{L})$ for $i = 1, 2$ and hence, by Lemma 7.1, $\text{Char}_\Lambda(X)$ divides $x_i\mathcal{L}$ for $i = 1, 2$. Since x_1 and x_2 do not have common irreducible factors, $\text{Char}_\Lambda(X)$ divides \mathcal{L} and the result follows. \square

7.2. Admissible primes. A prime ideal $\ell \subseteq \mathcal{O}_F$ is said to be *n-admissible* if

- (1) ℓ does not divide πp ;
- (2) ℓ is inert in K/F ;
- (3) π does not divide $|\ell|^2 - 1$;

(4) π^n divides $|\ell| + 1 + a_\ell(f)$ or $|\ell| + 1 - a_\ell(f)$.

Let ℓ be an n -admissible prime. Then

$$H_{\text{sing}}^1(K_\ell, T_{f,\pi^n}) \simeq \mathcal{O}_{f,\pi}/\pi^n \quad \text{and} \quad H_{\text{fin}}^1(K_\ell, T_{f,\pi^n}) \simeq \mathcal{O}_{f,\pi}/\pi^n.$$

To show this, note that, since T_{f,π^n} is unramified at ℓ ,

$$H_{\text{sing}}^1(K_\ell, T_{f,\pi^n}) = \text{Hom}_{G_{K_\ell}}(I_{K_\ell}, T_{f,\pi^n}).$$

Since $\ell \nmid p$, all homomorphisms above factor through the tame inertia subgroup. The Frobenius $\text{Frob}_\ell(K)$ of K at ℓ (where, by an abuse of notation, ℓ denotes the unique prime of K above ℓ) acts on I_{K_ℓ} by $|\ell|^2$ and on T_{f,π^n} it acts with eigenvalues $|\ell|^2$ and 1 (which are distinct in $\mathcal{O}_{f,\pi}/\pi^n$). Hence,

$$H_{\text{sing}}^1(K_\ell, T_{f,\pi^n}) \simeq \mathcal{O}_{f,\pi}/\pi^n.$$

For the finite cohomology, since T_{f,π^n} is unramified at ℓ ,

$$H_{\text{fin}}^1(K_\ell, T_{f,\pi^n}) \simeq T_{f,\pi^n}/(\text{Frob}_\ell(K) - 1).$$

Hence, as above, $H_{\text{fin}}^1(K_\ell, T_{f,\pi^n}) \simeq \mathcal{O}_{f,\pi}/\pi^n$. Since ℓ is inert in K , it splits completely in K_{\wp^∞} . It follows that

$$\begin{aligned} \hat{H}_{\text{sing}}^1(K_{\wp^\infty,\ell}, T_{f,\pi^n}) &\simeq \Lambda_{\wp,\pi}/\pi^n \Lambda_{\wp,\pi}, \quad \text{and} \\ \hat{H}_{\text{fin}}^1(K_{\wp^\infty,\ell}, T_{f,\pi^n}) &\simeq \Lambda_{\wp,\pi}/\pi^n \Lambda_{\wp,\pi}. \end{aligned} \tag{8}$$

Proposition 7.5. *Let $s \in H^1(K, A_{f,\pi})$ be a non-zero element. Then there exist infinitely many admissible primes ℓ such that $\partial_\ell(s) = 0$ and $v_\ell(s) \neq 0$.*

Proof. This is a direct generalization of Theorem 3.2 in [5]. A similar argument will be given in Proposition 7.13. \square

7.3. Rigid pairs. Let $\rho = \rho_{f,\pi}$ denote the representation of $G_F = \text{Gal}(\bar{F}/F)$ on the $k := \mathcal{O}_{f,\pi}/\pi$ -vector space $A_{f,\pi}$. The k -vector space $\text{ad}\rho := \text{Hom}(A_{f,\pi}, A_{f,\pi})$ is endowed with an action of G_F by conjugation of endomorphisms. The G_F -module $\text{ad}\rho$ is called the *adjoint representation* of ρ . Denote by $\text{ad}^0\rho$ the k -subspace of trace-zero endomorphisms in $\text{ad}\rho$ with the induced action of G_F . Define the following local structures for the cohomology of $\text{ad}^0\rho$:

Primes $\mathfrak{q} \nmid \pi p$: Define $H_{\text{fin}}^1(F_{\mathfrak{q}}, \text{ad}^0\rho) := H^1(G_{F_{\mathfrak{q}}}/I_{F_{\mathfrak{q}}}, \text{ad}^0\rho)$ to be the unramified cohomology.

Primes $\mathfrak{q} \mid \pi, \mathfrak{q} \nmid p$: As in the previous case, define

$$H_{\text{ord}}^1(F_{\mathfrak{q}}, \text{ad}^0\rho) := H^1(G_{F_{\mathfrak{q}}}/I_{F_{\mathfrak{q}}}, (\text{ad}^0\rho)^{I_{F_{\mathfrak{q}}}})$$

to be the unramified cohomology.

Primes $\mathfrak{p} \mid p$: Let $\mathrm{ad}^{(1)}\rho$ denote the subspace $\mathrm{Hom}(A_{f,\pi}^{(1)}, A_{f,\pi}^{(\mathfrak{p})})$ of $\mathrm{ad}^0\rho$. Define

$$H_{\mathrm{ord}}^1(F_{\mathfrak{p}}, \mathrm{ad}^0\rho) := \ker \left(H^1(F_{\mathfrak{p}}, \mathrm{ad}^0\rho) \longrightarrow H^1(I_{F_{\mathfrak{p}}}, \mathrm{ad}^0\rho / \mathrm{ad}^{(1)}\rho) \right).$$

1-admissible primes ℓ : If ℓ is a 1-admissible prime, denote by $\mathrm{ad}^{(\ell)}\rho$ the unique one dimensional k -vector subspace of $\mathrm{ad}^0\rho$ on which the absolute Frobenius $\mathrm{Frob}_{\ell}(F)$ of F at ℓ acts with eigenvalue $|\ell|$ (the existence of this subspace follows because the Frobenius at ℓ acts on $A_{f,\pi}$ with eigenvalues $\pm|\ell|$ and ± 1 , so that the eigenvalues of its action on $\mathrm{ad}^0\rho$ are $|\ell|$, $|\ell|^{-1}$ and 1, while its uniqueness follows because $|\ell|^2 \neq 1$ in k). Define

$$H_{\mathrm{ord}}^1(F_{\ell}, \mathrm{ad}^0\rho) := H^1(F_{\ell}, \mathrm{ad}^{(\ell)}\rho)$$

and $H_{\mathrm{fin}}^1(F_{\ell}, \mathrm{ad}^0\rho)$ to be the kernel of the canonical map

$$H^1(F_{\ell}, \mathrm{ad}^0\rho) \rightarrow H_{\mathrm{ord}}^1(F_{\ell}, \mathrm{ad}^0\rho).$$

The group $H^1(F_{\ell}, \mathrm{ad}^0\rho)$ is two dimensional over k and there is a decomposition in one-dimensional k -vector spaces:

$$H^1(F_{\ell}, \mathrm{ad}^0\rho) = H_{\mathrm{fin}}^1(F_{\ell}, \mathrm{ad}^0\rho) \oplus H_{\mathrm{ord}}^1(F_{\ell}, \mathrm{ad}^0\rho).$$

See for example Lemma 1 in Section 3 of [41] for details.

Let \mathfrak{s} be a square-free product of 1-admissible primes. Define the \mathfrak{s} -Selmer group $\mathrm{Sel}_{\mathfrak{s}}(F, \mathrm{ad}^0\rho)$ attached to $\mathrm{ad}^0\rho$ to be the k -vector space consisting of those classes $\xi \in H^1(F, \mathrm{ad}^0\rho)$ such that

- (1) for primes $\mathfrak{q} \nmid \mathfrak{n}p$: $\mathrm{res}_{\mathfrak{q}}(\xi) \in H_{\mathrm{fin}}^1(F_{\mathfrak{q}}, \mathrm{ad}^0\rho)$;
- (2) for primes $\ell \mid \mathfrak{s}$: $\mathrm{res}_{\ell}(\xi) \in H_{\mathrm{ord}}^1(F_{\ell}, \mathrm{ad}^0\rho)$;
- (3) for primes $\mathfrak{q} \mid \mathfrak{n}$ and $\mathfrak{q} \nmid p$: $\mathrm{res}_{\mathfrak{q}}(\xi) \in H_{\mathrm{ord}}^1(F_{\mathfrak{q}}, \mathrm{ad}^0\rho)$;
- (4) for primes $\mathfrak{p} \mid p$: $\mathrm{res}_{\mathfrak{p}}(\xi) \in H_{\mathrm{ord}}^1(F_{\mathfrak{p}}, \mathrm{ad}^0\rho)$;

Denote by R the minimal nearly ordinary universal deformation ring attached to ρ with determinant the cyclotomic character. See [15], Section 3.8, for detailed definitions. Let $\mathfrak{m}_{f,\pi} := \ker(\mathbb{T}_{\mathfrak{n}} \rightarrow k)$ and denote by \mathbb{T}_f the completion of $\mathbb{T}_{\mathfrak{n}}$ at $\mathfrak{m}_{f,\pi}$. Then R is isomorphic to \mathbb{T}_f by Theorem 11.1 in [15].

Remark 7.6. The condition $[F(\zeta_5) : F] \neq 2$ when $p = 5$ in the Introduction is required to apply [15].

Lemma 7.7. *The modular form f is π -isolated if and only if $\mathrm{Sel}_{\mathcal{O}_F}(F, \mathrm{ad}^0\rho)$ is trivial.*

Proof. f is π -isolated if and only if $\mathbb{T}_f \simeq \mathcal{O}_{f,\pi}$, and this condition is equivalent to the isomorphism $R \simeq \mathcal{O}_{f,\pi}$. Now $R \simeq \mathcal{O}_{f,\pi}$ if and only if $m/(\pi, m^2) = 0$, and this condition is equivalent to $\text{Sel}_{\mathcal{O}_F}(F, \text{ad}^0 \rho) = 0$ by [15], Proposition 3.35. \square

Assume from now on that f is π -isolated in the sense of Assumption 1.3.

If \mathfrak{s} is a (possibly empty) square free product of 1-admissible primes, let $\text{Sel}_{(\mathfrak{s})}(F, \text{ad}^0 \rho)$ be the group defined in the same way as $\text{Sel}_{\mathfrak{s}}(F, \text{ad}^0 \rho)$ but with no conditions imposed on the prime dividing \mathfrak{s} . Let $\text{Sel}_{[\mathfrak{s}]}(F, \text{ad}^0 \rho)$ denote the subgroup of $\text{Sel}_{\mathfrak{s}}(F, \text{ad}^0 \rho)$ consisting of classes which are trivial at the primes dividing \mathfrak{s} . These notations can be combined: if $\mathfrak{s}_1, \mathfrak{s}_2, \mathfrak{s}_3$ are pairwise coprime square-free product of 1-admissible primes, define the group $\text{Sel}_{\mathfrak{s}_1(\mathfrak{s}_2)[\mathfrak{s}_3]}(F, \text{ad}^0 \rho) := \text{Sel}_{\mathfrak{s}_1}(F, \text{ad}^0 \rho) \cap \text{Sel}_{(\mathfrak{s}_2)}(F, \text{ad}^0 \rho) \cap \text{Sel}_{[\mathfrak{s}_3]}(F, \text{ad}^0 \rho)$.

Let $\text{ad}^0 \rho^* := \text{Hom}(\text{ad}^0 \rho, k)$ be the dual representation of $\text{ad}^0 \rho$. Then define the dual Selmer group of $\text{Sel}_{\mathfrak{s}}(F, \text{ad}^0 \rho)$ to be the subgroup $\text{Sel}_{\mathfrak{s}}(F, \text{ad}^0 \rho^*)$ of $H^1(F, \text{ad}^0 \rho^*)$ consisting of those elements $t \in H^1(F, \text{ad}^0 \rho^*)$ such that

$$\langle \text{res}_{\mathfrak{q}}(s), \text{res}_{\mathfrak{q}}(t) \rangle_{\mathfrak{q}} = 0$$

for all $s \in \text{Sel}_{\mathfrak{s}}(F, \text{ad}^0 \rho)$ and for all prime ideals \mathfrak{q} , where $\langle \cdot, \cdot \rangle_{\mathfrak{q}}$ is the local Tate pairing at \mathfrak{q} . Define as above the Selmer groups $\text{Sel}_{\mathfrak{s}}(F, \text{ad}^0 \rho^*)$, $\text{Sel}_{(\mathfrak{s})}(F, \text{ad}^0 \rho^*)$, $\text{Sel}_{[\mathfrak{s}]}(F, \text{ad}^0 \rho^*)$ and $\text{Sel}_{\mathfrak{s}_1(\mathfrak{s}_2)[\mathfrak{s}_3]}(F, \text{ad}^0 \rho^*)$.

The groups $\text{Sel}_{(\mathfrak{s})}(F, \text{ad}^0 \rho)$ and $\text{Sel}_{[\mathfrak{s}]}(F, \text{ad}^0 \rho^*)$ are dual to each other, and the same is true for $\text{Sel}_{\mathfrak{s}}(F, \text{ad}^0 \rho)$ and $\text{Sel}_{\mathfrak{s}}(F, \text{ad}^0 \rho^*)$.

Lemma 7.8. *Let ℓ be an admissible prime for f . Then the groups $\text{Sel}_{(\ell)}(F, \text{ad}^0 \rho)$ and $\text{Sel}_{(\ell)}(F, \text{ad}^0 \rho^*)$ are one dimensional over k .*

Proof. The groups $\text{Sel}_{\mathcal{O}_F}(F, \text{ad}^0 \rho)$ and $\text{Sel}_{\mathcal{O}_F}(F, \text{ad}^0 \rho^*)$ have the same cardinality by Theorem 2.19 in [10]. Furthermore, $\text{Sel}_{\mathcal{O}_F}(F, \text{ad}^0 \rho) = 0$ by Lemma 7.7 because f is π -isolated. Hence $\text{Sel}_{\mathcal{O}_F}(F, \text{ad}^0 \rho^*) = 0$. Since

$$\#\text{Sel}_{(\ell)}(F, \text{ad}^0 \rho) / \#\text{Sel}_{[\ell]}(F, \text{ad}^0 \rho^*) = \#k$$

by Theorem 2.19 in [10], it follows that $\text{Sel}_{(\ell)}(F, \text{ad}^0 \rho)$ is one dimensional over k . Replacing $\text{ad}^0 \rho$ by $\text{ad}^0 \rho^*$ and repeating the same argument shows that $\text{Sel}_{(\ell)}(F, \text{ad}^0 \rho^*)$ is one dimensional too. \square

Lemma 7.9. *Let ℓ be an admissible prime for f and suppose that $\text{Sel}_{\ell}(F, \text{ad}^0 \rho) \neq 0$. Then $\text{Sel}_{\ell}(F, \text{ad}^0 \rho) \simeq k$.*

Proof. Thanks to the inclusion $\text{Sel}_{\ell}(F, \text{ad}^0 \rho) \subseteq \text{Sel}_{(\ell)}(F, \text{ad}^0 \rho)$, this is immediate from Lemma 7.8. \square

Fix a pair of admissible primes $\ell_1 \neq \ell_2$. Write

$$\begin{aligned} v_{\ell_2} : \text{Sel}_{(\ell_1)}(F, \text{ad}^0 \rho) &\rightarrow H_{\text{fin}}^1(F_{\ell_2}, \text{ad}^0 \rho) \\ v_{\ell_2}^* : \text{Sel}_{(\ell_1)}(F, \text{ad}^0 \rho^*) &\rightarrow H_{\text{fin}}^1(F_{\ell_2}, \text{ad}^0 \rho^*) \end{aligned}$$

for the restriction maps at ℓ_2 .

Lemma 7.10. *Suppose that $\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho) \neq 0$ and $v_{\ell_2}, v_{\ell_2}^*$ are both non trivial. Then $\text{Sel}_{\ell_1 \ell_2}(F, \text{ad}^0 \rho) = 0$.*

Proof. By Lemma 7.8, choose generators ξ and ξ^* of the one dimensional k -vector spaces $\text{Sel}_{(\ell_1)}(F, \text{ad}^0 \rho)$ and $\text{Sel}_{(\ell_1)}(F, \text{ad}^0 \rho^*)$. Note that

$$\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho) \subseteq \text{Sel}_{(\ell_1)}(F, \text{ad}^0 \rho) \simeq k$$

and that $\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho) \neq 0$ by assumption. Therefore $\xi \in \text{Sel}_{\ell_1}(F, \text{ad}^0 \rho)$ and $\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho) \simeq k$. Since $\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho)$ and $\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho^*)$ have the same cardinality ([10], Theorem 2.19), $\xi^* \in \text{Sel}_{\ell_1}(F, \text{ad}^0 \rho^*)$. By [10], Theorem 2.19,

$$\#\text{Sel}_{\ell_1(\ell_2)}(F, \text{ad}^0 \rho) / \#\text{Sel}_{\ell_1[\ell_2]}(F, \text{ad}^0 \rho^*) = \#k. \quad (9)$$

Further note that $\text{Sel}_{\ell_1[\ell_2]}(F, \text{ad}^0 \rho^*) \subseteq \text{Sel}_{\ell_1}(F, \text{ad}^0 \rho^*) \simeq k$, and therefore, either $\text{Sel}_{\ell_1[\ell_2]}(F, \text{ad}^0 \rho^*) = 0$ or $\text{Sel}_{\ell_1[\ell_2]}(F, \text{ad}^0 \rho^*) \simeq k$, generated by ξ^* . In the second case, $\xi^* \in \text{Sel}_{\ell_1[\ell_2]}(F, \text{ad}^0 \rho^*)$ implies that $\text{res}_{\ell_2}(\xi^*) = 0$ in $H_{\text{fin}}^1(F_{\ell_2}, \text{ad}^0 \rho^*)$. The assumption $v_{\ell_2}^*(\xi^*) \neq 0$ excludes this possibility, so $\text{Sel}_{\ell_1[\ell_2]}(F, \text{ad}^0 \rho^*) = 0$. By (9), $\text{Sel}_{\ell_1(\ell_2)}(F, \text{ad}^0 \rho) \simeq k$. The inclusion

$$\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho) \subseteq \text{Sel}_{\ell_1(\ell_2)}(F, \text{ad}^0 \rho)$$

implies $\text{Sel}_{\ell_1(\ell_2)}(F, \text{ad}^0 \rho) = \text{Sel}_{\ell_1}(F, \text{ad}^0 \rho)$ and both of them are generated by ξ . Finally, note that

$$\text{Sel}_{\ell_1 \ell_2}(F, \text{ad}^0 \rho) \subseteq \text{Sel}_{\ell_1(\ell_2)}(F, \text{ad}^0 \rho),$$

so, as above, either $\text{Sel}_{\ell_1 \ell_2}(F, \text{ad}^0 \rho)$ is trivial or is one dimensional. In the second case, it is isomorphic to $\text{Sel}_{\ell_1(\ell_2)}(F, \text{ad}^0 \rho)$ and hence also to $\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho)$. So the reduction of ξ at ℓ_2 should be both ordinary (it belongs to $\text{Sel}_{\ell_1 \ell_2}(F, \text{ad}^0 \rho)$) and finite (it belongs to $\text{Sel}_{\ell_1 \ell_2}(F, \text{ad}^0 \rho)$), hence trivial. The assumption $v_{\ell_2}(\xi) \neq 0$ excludes this possibility, so $\text{Sel}_{\ell_1 \ell_2}(F, \text{ad}^0 \rho)$ is trivial. \square

Lemma 7.11. *If $\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho) = 0$, $\text{Sel}_{\ell_2}(F, \text{ad}^0 \rho) = 0$ and v_{ℓ_2} is the trivial map, then $\text{Sel}_{\ell_1 \ell_2}(F, \text{ad}^0 \rho) = 0$.*

Proof. Since $\text{Sel}_{\ell_2}(F, \text{ad}^0 \rho) = 0$, again by Theorem 2.19 in [10], $\text{Sel}_{(\ell_1) \ell_2}(F, \text{ad}^0 \rho)$ is one dimensional. By Lemma 7.8, choose a generator ξ of $\text{Sel}_{(\ell_1) \ell_2}(F, \text{ad}^0 \rho)$. Since

$v_{\ell_2}(\xi) = 0$, the restriction to F_{ℓ_2} of this class must be ordinary, and so ξ belongs to $\text{Sel}_{(\ell_1)\ell_2}(F, \text{ad}^0 \rho)$. Hence, $\text{Sel}_{(\ell_1)\ell_2}(F, \text{ad}^0 \rho)$ is generated by ξ and

$$\text{Sel}_{(\ell_1)\ell_2}(F, \text{ad}^0 \rho) \simeq \text{Sel}_{(\ell_1)}(F, \text{ad}^0 \rho).$$

Note that if $\xi \in \text{Sel}_{\ell_1(\ell_2)}(F, \text{ad}^0 \rho)$, then also $\xi \in \text{Sel}_{\ell_1}(F, \text{ad}^0 \rho)$. By assumption

$$\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho) = 0,$$

so $\xi \notin \text{Sel}_{\ell_1(\ell_2)}(F, \text{ad}^0 \rho)$. As $\xi \in \text{Sel}_{(\ell_1)\ell_2}(F, \text{ad}^0 \rho)$ and $\xi \notin \text{Sel}_{\ell_1(\ell_2)}(F, \text{ad}^0 \rho)$, one finds that $\text{Sel}_{\ell_1\ell_2}(F, \text{ad}^0 \rho)$ is trivial because it is the intersection of $\text{Sel}_{\ell_1(\ell_2)}(F, \text{ad}^0 \rho)$ and $\text{Sel}_{(\ell_1)\ell_2}(F, \text{ad}^0 \rho)$. \square

Definition 7.12. A pair (ℓ_1, ℓ_2) of admissible primes is said to be a *rigid pair* if $\text{Sel}_{\ell_1\ell_2}(F, \text{ad}^0 \rho)$ is trivial.

Choose $s \in H^1(K, A_{f,\pi})$, $s \neq 0$. Assume that s belongs to a specific eigenspace for the complex conjugation τ , so that $\tau(s) = \delta s$ with $\delta = \pm 1$. Fix an integer n and define $M := K(A_{f,\pi^n})$. Let M_s/M be the extension cut out by s , so that $\text{Gal}(M_s/M) \simeq A_{f,\pi}$ via s . Set $G_M := \text{Gal}(\bar{M}/M)$.

Since f is π -isolated, $\text{Sel}_{(\ell_1)}(F, \text{ad}^0 \rho)$ and $\text{Sel}_{(\ell_1)}(F, \text{ad}^0 \rho^*)$ are one dimensional over k . Let ξ and ξ^* be generators. The images $\bar{\xi}$ and $\bar{\xi}^*$ of ξ and ξ^* in

$$H^1(M, \text{ad}^0 \rho) = \text{Hom}(G_M, \text{ad}^0 \rho) \quad \text{and} \quad H^1(M, \text{ad}^0 \rho^*) = \text{Hom}(G_M, \text{ad}^0 \rho^*)$$

cut out extensions $M_{\bar{\xi}}$ and $M_{\bar{\xi}^*}$ of M whose Galois groups are identified via $\bar{\xi}$ and $\bar{\xi}^*$ with $\text{ad}^0 \rho$ and $\text{ad}^0 \rho^*$ respectively (that is, $\text{Gal}(M_{\bar{\xi}}/M) \simeq \text{ad}^0 \rho$ and $\text{Gal}(M_{\bar{\xi}^*}/M) \simeq \text{ad}^0 \rho^*$).

Denote by M_{s,ξ,ξ^*} the compositum of M_s , $M_{\bar{\xi}}$ and $M_{\bar{\xi}^*}$. Since the representations $A_{f,\pi}$, $\text{ad}^0 \rho$ and $\text{ad}^0 \rho^*$ are pairwise non isomorphic and absolutely irreducible, we have

$$\text{Gal}(M_{s,\xi,\xi^*}/F) \simeq (A_{f,\pi} \times \text{ad}^0 \rho \times \text{ad}^0 \rho^*) \rtimes \text{Gal}(M/F)$$

where the action of $\text{Gal}(M/F)$ on the normal subgroup $(A_{f,\pi}, \text{ad}^0 \rho, \text{ad}^0 \rho^*)$ is given by

$$(v, w, w^*)(\tau^j, T) = (\delta^j \bar{T}v, \bar{T}w\bar{T}^{-1}, \bar{T}w^*\bar{T}^{-1} \det(T)).$$

Proposition 7.13. Let ℓ_1 be admissible such that $\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho) \neq 0$. Fix a non trivial element $s \in H^1(K, A_{f,\pi})$. For any n there exists infinitely many n -admissible primes ℓ_2 such that $\partial_{\ell_2}(s) = 0$, $v_{\ell_2}(s) \neq 0$ and (ℓ_1, ℓ_2) is a rigid pair.

Proof. By Lemma 7.9, $\xi \in \text{Sel}_{\ell_1}(F, \text{ad}^0 \rho)$, so that $\xi^* \in \text{Sel}_{\ell_1}(F, \text{ad}^0 \rho^*)$ too. The Galois group $\text{Gal}(M_{s,\xi,\xi^*}/F)$ contains an element (v, w, w^*, τ, T) such that:

- (1) T acts on A_{f,π^n} with eigenvalues δ and λ where λ is an element of $(\mathcal{O}_{f,\pi}/\pi^n)^\times$ of order prime to p and $\neq \pm 1$;
- (2) v belongs to the unique line in $A_{f,\pi}$ where T acts by δ ;
- (3) w belongs to the unique line in $\text{ad}^0 \rho$ fixed by T ;
- (4) w^* belongs to the unique line in $\text{ad}^0 \rho^*$ fixed by T .

Choose now $\ell_2 \nmid p\pi$ and unramified in M_{s,ξ,ξ^*} such that the Frobenius element $\text{Frob}_{\ell_2}(M_{s,\xi,\xi^*}/F)$ of $\text{Gal}(M_{s,\xi,\xi^*}/F)$ at ℓ_2 verifies the relation

$$\text{Frob}_{\ell_2}(M_{s,\xi,\xi^*}/F) = (v, w, w^*, \tau, T).$$

We claim that ℓ_2 has the desired properties. By the Chebotarev density theorem, there are infinitely many such primes. Then ℓ_2 has the desired properties. To show that ℓ_2 is n -admissible, note that the Frobenius element $\text{Frob}_{\ell_2}(K/F)$ of $\text{Gal}(K/F)$ at ℓ_2 verifies the relation $\text{Frob}_{\ell_2}(K/F) = \tau$, which implies that ℓ_2 is inert in K . The congruences $a_{\ell_2}(f) \equiv \delta + \lambda \pmod{\pi^n}$ and $|\ell_2| \equiv \delta\lambda \pmod{\pi^n}$ enjoyed by the characteristic polynomial of Frobenius show $a_{\ell_2}(f) \equiv \delta(|\ell_2| + 1) \pmod{\pi^n}$. Finally, since $\lambda \neq \pm 1$, it follows that $|\ell_2| \not\equiv \pm 1 \pmod{\pi^n}$. Hence ℓ_2 is an n -admissible prime. Moreover, ℓ_2 has the properties stated in the theorem. First, note that $\partial_{\ell_2}(s) = 0$. Indeed, if l is a prime ideal of M_{s,ξ,ξ^*} dividing ℓ_2 , then

$$\text{res}_{\ell_2}(s) \in \ker(H^1(K_{\ell_2}, A_{f,\pi}) \longrightarrow H^1(M_{s,\xi,\xi^*,l}, A_{f,\pi})).$$

Since $H^1(M_{s,\xi,\xi^*,l}, A_{f,\pi}) \supseteq H^1(K_{\ell_2}^{\text{unr}}, A_{f,\pi}) \supseteq H_{\text{sing}}^1(K_{\ell_2}, A_{f,\pi})$, it follows that $\partial_{\ell_2}(s) = 0$ (here $M_{s,\xi,\xi^*,l}$ is the completion of M_{s,ξ,ξ^*} at l). For the proof that $v_{\ell_2}(s) \neq 0$: Let \mathfrak{l} be a prime ideal in M dividing ℓ and set $c := [M : F]$. Denote by $\text{Frob}_{\mathfrak{l}}(M_{s,\xi,\xi^*}/M)$ a Frobenius element of $\text{Gal}(M_{s,\xi,\xi^*}/M)$ at \mathfrak{l} . Note that

$$\text{Frob}_{\mathfrak{l}}(M_{s,\xi,\xi^*}/M) = (v, w, w^*, \tau, T)^c = (cv, cw, cw^*, 1, 1).$$

Let \bar{s} be the image of s in $\text{Gal}(M_s/M)$. Since c is even and prime to p by Property 1 of T ,

$$\bar{s}(\text{Frob}_{\mathfrak{l}}(M_{s,\xi,\xi^*}/M)) = \bar{s}(cv) = c\bar{s}(v) \neq 0$$

and $\text{res}_{\ell_2}(s) \neq 0$. So, $v_{\ell_2}(s) \neq 0$. Since

$$\bar{\xi}(\text{Frob}_{\mathfrak{l}}(M_{s,\xi,\xi^*}/M)) = \bar{\xi}(cw) = c\bar{\xi}(w) \neq 0,$$

$$\bar{\xi}^*(\text{Frob}_{\mathfrak{l}}(M_{s,\xi,\xi^*}/M)) = \bar{\xi}^*(cw^*) = c\bar{\xi}^*(w) \neq 0,$$

Lemma 7.10 implies $\text{Sel}_{\ell_1\ell_2}(F, \text{ad}^0 \rho^*) = 0$, so (ℓ_1, ℓ_2) is a rigid pair. \square

Proposition 7.14. *Let ℓ_1 be admissible such that $\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho) = 0$. Fix a non trivial element $s \in H^1(K, A_{f,\pi})$. For any n there exists infinitely many n -admissible primes ℓ_2 such that $\partial_{\ell_2}(s) = 0$, $v_{\ell_2}(s) \neq 0$ and either $\text{Sel}_{\ell_2}(F, \text{ad}^0 \rho) \simeq k$ or $\text{Sel}_{\ell_2}(F, \text{ad}^0 \rho) = 0$ and (ℓ_1, ℓ_2) is a rigid pair.*

Proof. Choose a prime ℓ_2 such that

$$\text{Frob}_{\ell_2}(M_{s,\xi,\xi^*}/F) = (v, 0, 0, \tau, T).$$

The same computations as in Proposition 7.13 show that ℓ_2 is admissible and that $v_{\ell_2}(s) \neq 0$. Note that $\xi(w) = 0$ and $\xi^*(w^*) = 0$. If $\text{Sel}_{\ell_2}(F, \text{ad}^0 \rho) = 0$, by Lemma 7.11 $\text{Sel}_{\ell_1 \ell_2}(F, \text{ad}^0 \rho)$ is trivial, so (ℓ_1, ℓ_2) is a rigid pair. If $\text{Sel}_{\ell_2}(F, \text{ad}^0 \rho) \neq 0$, then it is one-dimensional by Lemma 7.9. \square

7.4. Congruences between modular forms and the Euler system

7.4.1. Raising the level in one prime. Fix an n -admissible prime ℓ . Let $\mathbb{T}_{n^+, n^- \ell}$ be the Hecke algebra acting on the space of modular forms which are new at $n^- \ell$. It is known that there exists a morphism $f_\ell: \mathbb{T}_{n^+, n^- \ell} \rightarrow \mathcal{O}_{f, \pi}/\pi^n$ such that

- (1) for primes $\mathfrak{q} \nmid n\ell$: $f_\ell(T_{\mathfrak{q}}) \equiv a_{\mathfrak{q}}(f) \pmod{\pi^n}$;
- (2) for primes $\mathfrak{q} \mid n$: $f_\ell(U_{\mathfrak{q}}) \equiv a_{\mathfrak{q}}(f) \pmod{\pi^n}$;
- (3) $f_\ell(U_\ell) \equiv \epsilon \pmod{\pi^n}$, where π^n divides $|\ell| + 1 - \epsilon a_\ell(f)$.

This result follows from a generalization to the case $n > 1$ of [40]. For details, see [30], Theorem 3.3.

7.4.2. The Euler system. Denote by $X^{(\ell)}$ the Shimura curve (defined over F) whose complex points are given by

$$X^{(\ell)}(\mathbb{C}) = \mathcal{B}^\times \backslash \mathcal{H}^\pm \times \widehat{\mathcal{B}}^\times / \widehat{\mathcal{R}}^\times,$$

where $\mathcal{H}^\pm := \mathbb{C} - \mathbb{R}$, \mathcal{B}/F is a quaternion algebra of discriminant $n^- \ell$ which is ramified in exactly one of the archimedean places and $\mathcal{R} \subseteq \mathcal{B}$ is an Eichler order of level $\wp n^+$. Let $J^{(\ell)}$ be the Jacobian variety (defined over F) associated to $X^{(\ell)}$. Denote by $T_p(J^{(\ell)})$ the p -adic Tate module of $J^{(\ell)}$ and by Φ_ℓ the group of connected components of the fiber at ℓ of the Néron model of $J^{(\ell)}$ over \mathcal{O}_K . Denote by \mathcal{I}_{f_ℓ} the kernel of the map f_ℓ . By [30], which generalizes the result of [29] to the present situation, there exists a Hecke equivariant isomorphism of $\text{Gal}(\bar{F}/F)$ -modules:

$$v: T_p(J^{(\ell)})/\mathcal{I}_{f_\ell} \xrightarrow{\sim} T_{f, \pi^n}. \quad (10)$$

Remark 7.15. It is not known if (10) is an isomorphism when the degree d of F over \mathbb{Q} is even and $n^- = \mathcal{O}_F$. For simplicity, we do not consider this case in the present work.

Following Section 3, a Heegner point P_m of conductor \wp^m is a CM-point of conductor \wp^m in

$$X_{\mathcal{R}}^{(\ell)}(K) := \mathcal{B}^\times \backslash \text{Hom}(K, \mathcal{B}) \times \widehat{\mathcal{B}}^\times / \widehat{\mathcal{R}}^\times.$$

Let σ be the archimedean place where \mathcal{B} is split and fix an isomorphism ι_∞ of $\mathcal{B} \otimes_\sigma \mathbb{R}$ with $M_2(\mathbb{R})$. Then \mathcal{B} acts on \mathcal{H}^\pm by fractional linear transformations via ι_∞ and the set $\text{Hom}(K, \mathcal{B})$ can be embedded in \mathcal{H}^\pm by sending $\Psi \in \text{Hom}(K, \mathcal{B})$ to the fixed point of $\Psi(K^\times)$ acting on \mathcal{H}^\pm whose imaginary part is positive. Hence, a CM-point $P \in X_{\mathcal{R}}^{(\ell)}(K)$ of conductor \wp^m can be viewed as a point in $X^{(\ell)}(\mathbb{C})$ and the theory of complex multiplication shows that, in fact, $P \in X^{(\ell)}(\tilde{K}_{\wp^m})$. Furthermore, the Galois action on CM-points of conductor \wp^m described in Section 3 translates into the usual Galois action of \tilde{G}_{\wp^m} on $X^{(\ell)}(\tilde{K}_{\wp^m})$. For more details, see Chapter 9 of [45].

Recall the choice of orientations made in Section 4.2 and fix an orientation as explained in Section 3 at the prime ℓ . Define the set of Gross points $\text{Gr}^{(\ell)}(\wp^m)$ in $X_{\mathcal{R}}^{(\ell)}$ with respect to these orientations. Write $P_m = (x_m, \Psi_m)$. Let $e_{P_m} = (s(e_{P_m}), t(e_{P_m})) \in \mathcal{E}_{\wp}$ be the edge corresponding to $x_m \mathcal{R}_{\wp} x_m^{-1}$ as described in Section 3. Say that a sequence $(P_m)_{m \geq 1}$ of points in $\text{Gr}^{(\ell)}(\wp^\infty)$, with $P_m \in \text{Gr}^{(\ell)}(\wp^m)$, is *compatible* if $t(e_{P_m}) = s(e_{P_{m+1}})$ for all integers $m \geq 1$. Choose a sequence of compatible Heegner points $(P_m)_{m \geq 1}$ with $P_m \in \text{Gr}^{(\ell)}(\wp^m)$.

For the modular interpretation of Heegner points, which will not be recalled here, we refer to Section 2 of [48].

Since \mathcal{I}_{f_ℓ} is not Eisenstein, there is an isomorphism

$$J^{(\ell)}(\tilde{K}_{\wp^m})/\mathcal{I}_{f_\ell} \longrightarrow \text{Pic}(X^{(\ell)}(\tilde{K}_{\wp^m})/\mathcal{I}_{f_\ell}).$$

Denote by P_m^+ the image of P_m in $J^{(\ell)}(\tilde{K}_{\wp^m})/\mathcal{I}_{f_\ell}$. Define

$$P_m^* := \alpha_{\wp}^{-m} P_m^+.$$

Since $(P_m)_{m \geq 1}$ is compatible, it is easily seen that the points P_m^* are norm-compatible. Their images under the Kummer map followed by the map induced by ν

$$J^{(\ell)}(\tilde{K}_{\wp^m})/\mathcal{I}_{f_\ell} \longrightarrow H^1(\tilde{K}_{\wp^m}, T_p(J^{(\ell)})/\mathcal{I}_{f_\ell}) \longrightarrow H^1(\tilde{K}_{\wp^m}, T_{f, \pi^n})$$

yield a sequence of cohomology classes, $\tilde{\kappa}_m(\ell)$, which are compatible under corestriction. Taking limit defines a class $\tilde{\kappa}(\ell) \in \hat{H}^1(\tilde{K}_{\wp^\infty}, T_{f, \pi^n})$. Define finally the class

$$\kappa(\ell) \in \hat{H}^1(K_{\wp^\infty}, T_{f, \pi^n})$$

to be the corestriction of $\tilde{\kappa}(\ell)$ from \tilde{K}_{\wp^∞} to K_{\wp^∞} .

Lemma 7.16. $\kappa(\ell) \in \hat{H}_\ell^1(K_{\wp^\infty}, T_{f, \pi^n})$.

Proof. It is enough to observe, as in the beginning of Section 8 in [5], that $\kappa(\ell)$ is constructed from a sequence of global points of $X^{(\ell)}$, so it belongs to the usual Selmer group of $J^{(\ell)}$ relative to the Galois module $T_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$. For completeness, let us provide some details on this proof. From the definition of $\hat{H}_\ell^1(K_{\wp^\infty}, T_{f, \pi^n})$, we see that it is enough to show that

- (1) $\text{res}_{\mathfrak{q}'}(\tilde{\kappa}_m(\ell)) \in H_{\text{fin}}^1(\tilde{K}_{\wp^m, \mathfrak{q}'}, T_{f, \pi^n})$ for primes \mathfrak{q}' of \tilde{K}_{\wp^m} which do not divide $\pi p \ell$;
- (2) $\text{res}_{\mathfrak{q}'}(\tilde{\kappa}_m(\ell)) \in H_{\text{ord}}^1(\tilde{K}_{\wp^m, \mathfrak{q}'}, T_{f, \pi^n})$ for primes \mathfrak{q}' dividing π^- but not p ;
- (3) $\text{res}_{\mathfrak{p}'}(\tilde{\kappa}_m(\ell)) \in H_{\text{ord}}^1(\tilde{K}_{\wp^m, \mathfrak{p}'}, T_{f, \pi^n})$ for primes \mathfrak{p}' of \tilde{K}_{\wp^m} which divide p .

For (1), Remark 5.1 shows that the image of the Kummer map

$$J^{(\ell)}(\tilde{K}_{\wp^m, \mathfrak{q}'}) \longrightarrow H^1(\tilde{K}_{\wp^m, \mathfrak{q}'}, J^{(\ell)}[p^n])$$

is unramified; the result follows then taking quotient by \mathcal{I}_{f_ℓ} . For (3), note that the Kummer map $J^{(\ell)}(\tilde{K}_{\wp^m, \mathfrak{p}'}) \rightarrow H^1(\tilde{K}_{\wp^m, \mathfrak{p}'}, T_{f, n})$ factors through the maximal ordinary abelian subvariety $J^{(\ell), \text{ord}}$ of $J^{(\ell)}$; the result follows then by Remark 5.4, again taking quotients by \mathcal{I}_{f_ℓ} . For (2), the analogue of [5], Corollary 5.18 (see (22) with the prime \mathfrak{q}' replacing ℓ_m), shows that if the quotient $\Phi_{\mathfrak{q}}/\mathcal{I}_{f_\ell}$ of the group of connected components $\Phi_{\mathfrak{q}}$ at \mathfrak{q} of $J^{(\ell)}$ by \mathcal{I}_{f_ℓ} is trivial, then $\text{res}_{\mathfrak{q}}(\tilde{\kappa}_m(\ell))$ is unramified; on the other hand, the vanishing of $\Phi_{\mathfrak{q}}/\mathcal{I}_{f_\ell}$ follows because f is ramified at \mathfrak{q} . Indeed, if $\Phi_{\mathfrak{q}}/\mathcal{I}_{f_\ell} \neq 0$, then there is an $\mathcal{O}_{f, \pi}/\pi^n$ -valued modular form of level $\pi \ell/\mathfrak{q}$ which is congruent to f_ℓ , and hence to f , modulo π^n ; so the mod π representation associated to f should be unramified at \mathfrak{q} , which is not the case. \square

7.4.3. Raising the level in two primes. Choose distinct n -admissible primes ℓ_1 and ℓ_2 such that π^n divides both $|\ell_1| + 1 - \epsilon_1 a_{\ell_1}(f)$ and $|\ell_2| + 1 - \epsilon_2 a_{\ell_2}(f)$, with ϵ_1, ϵ_2 equal to ± 1 . Let \mathbb{T}_{ℓ_1} be the Hecke algebra acting on the Shimura curve $X^{(\ell_1)}$. Assume that f is π -isolated. The map arising from Kummer theory composed with (10) yields a map

$$J^{(\ell_1)}(K_{\ell_2})/\mathcal{I}_{f_{\ell_1}} \longrightarrow H^1(K_{\ell_2}, T_p(J^{(\ell_1)})/\mathcal{I}_{f_{\ell_1}}) \longrightarrow H^1(K_{\ell_2}, T_{f, \pi^n})$$

whose image is equal to $H_{\text{fin}}^1(K_{\ell_2}, T_{f, \pi^n})$ because both $T_p(J^{(\ell_1)})$ and T_{f, π^n} are unramified at ℓ_2 . For the same reason and the fact that $\ell_2 \nmid p$, the map induced by reduction modulo ℓ_2

$$J^{(\ell_1)}(K_{\ell_2})/\mathcal{I}_{f_{\ell_1}} \longrightarrow J^{(\ell_1)}(\mathbb{F}_{\ell_2^2})/\mathcal{I}_{f_{\ell_1}}$$

is an isomorphism, where $\mathbb{F}_{\ell_2^2}$ is the residue field of the ring of integers of K_{ℓ_2} . The identification $H_{\text{fin}}^1(K_{\ell_2}, T_{f, \pi^n}) \simeq \mathcal{O}_{f, \pi}/\pi^n$ and the inverse of the above map yield a surjective map

$$J^{(\ell_1)}(\mathbb{F}_{\ell_2^2})/\mathcal{I}_{f_{\ell_1}} \longrightarrow \mathcal{O}_{f, \pi}/\pi^n. \quad (11)$$

Let $\mathcal{S}_{\ell_2} \subseteq X^{(\ell_1)}(\mathbb{F}_{\ell_2^2})$ be the set of supersingular points of $X^{(\ell_1)}$ in characteristic ℓ_2 and let $\text{Div}(\mathcal{S}_{\ell_2})$ and $\text{Div}^0(\mathcal{S}_{\ell_2})$ be the set of formal divisors and the set of formal degree zero divisors with \mathbb{Z} -coefficients supported on \mathcal{S}_{ℓ_2} . Let the Hecke algebra \mathbb{T}_{ℓ_1} act on $\text{Div}(\mathcal{S}_{\ell_2})$ and $\text{Div}^0(\mathcal{S}_{\ell_2})$ via Albanese functoriality (it makes no difference

if the Picard functoriality were chosen: see the discussion in [5], Section 9). Since $\mathcal{I}_{f_{\ell_1}}$ is not Eisenstein, there is an identification $\text{Div}(\mathcal{S}_{\ell_2})/\mathcal{I}_{f_{\ell_1}} \simeq \text{Div}^0(\mathcal{S}_{\ell_2})/\mathcal{I}_{f_{\ell_1}}$, so there is a map

$$\gamma: \text{Div}(\mathcal{S}_{\ell_2}) \longrightarrow \mathcal{O}_{f,\pi}/\pi^n.$$

Write \bar{T} for the image of $T \in \mathbb{T}_{\ell_1}$ into $\mathbb{T}_{\ell_1}/\mathcal{I}_{f_{\ell_1}}$, so that for primes $\mathfrak{q} \nmid n\ell_1$ we have $\bar{T}_{\mathfrak{q}} \equiv a_{\mathfrak{q}}(f) \pmod{\pi^n}$, and for primes $\mathfrak{q} \mid n$ we have $\bar{U}_{\mathfrak{q}} \equiv a_{\mathfrak{q}}(f) \pmod{\pi^n}$ and $\bar{U}_{\ell_1} \equiv \epsilon_1 \pmod{\pi^n}$.

Lemma 7.17. *For $x \in \text{Div}(\mathcal{S}_{\ell_2})$ the following relations hold:*

- (1) *For $\mathfrak{q} \nmid n\ell_1$: $\gamma(T_{\mathfrak{q}}x) = \bar{T}_{\mathfrak{q}}\gamma(x)$.*
- (2) *For $\mathfrak{q} \mid n\ell_1$: $\gamma(U_{\mathfrak{q}}x) = \bar{U}_{\mathfrak{q}}\gamma(x)$.*
- (3) *$\gamma(T_{\ell_2}x) = \bar{T}_{\ell_2}\gamma(x)$.*
- (4) *$\gamma(\text{Frob}_{\ell_2}(F)(x)) = \epsilon_2\gamma(x)$, where, as above, $\text{Frob}_{\ell}(F)$ is the absolute Frobenius of F at ℓ .*

Proof. The first two relations can be obtained from the identification between the groups $H_{\text{fin}}^1(K_{\ell_2}, T_{f,\pi^n})$ and $T_{f,\pi^n}/(\text{Frob}_{\ell_2}^2(F) - 1)$. The last two relations follow from Eichler–Shimura. For more details, see Lemma 9.1 in [5]. \square

Before going on with the raising the level result, we state an analogue of Ihara's Lemma in the context of Shimura curves over totally real fields. First recall the setting of [22]: Define $G_{\infty} := \text{SL}_2(\mathbb{R})/\{\pm 1\}$ and, for any prime \mathfrak{q} of F , $G_{\mathfrak{q}} := \{g \in \text{GL}_2(F_{\mathfrak{q}}) : \text{val}_{\mathfrak{q}}(\det(g)) \equiv 0 \pmod{2}\}/F_{\mathfrak{q}}^{\times}$, where $\text{val}_{\mathfrak{q}}$ is the normalized valuation of $F_{\mathfrak{q}}$. Let $i_{\infty}: B^{\times} \rightarrow G_{\infty}$ and $i_{\mathfrak{q}}: B^{\times} \rightarrow G_{\mathfrak{q}}$ be the injections. Let $\mathcal{O}_F[1/\mathfrak{q}]$ be the ring of \mathfrak{q} -integers of F and $\mathcal{U} \subseteq \mathcal{B}$ any $\mathcal{O}_F[1/\mathfrak{q}]$ -order. Define

$$\Gamma_{\mathcal{U}} := \{\gamma \in \mathcal{U} : N_{B/F}(\gamma) = 1\}/\{\pm 1\},$$

where $N_{B/F}: B \rightarrow F$ is the norm map. Let $\tilde{\Gamma}_{\mathcal{U}}$ be the pull-back of the group $\text{GL}_2(\mathcal{O}_{\mathfrak{q}})/\mathcal{O}_{\mathfrak{q}}^{\times}$ under the map $i_{\mathfrak{q}}: \Gamma_{\mathcal{U}} \rightarrow G_{\mathfrak{q}}$. Denote by $X_{\mathcal{U}}$ the Shimura curve defined over a suitable abelian extension of F whose complex points are

$$X_{\mathcal{U}}(\mathbb{C}) = i_{\infty}(\tilde{\Gamma}_{\mathcal{U}}) \backslash \mathcal{H},$$

where \mathcal{H} is the upper complex plane. Suppose that $\Gamma_{\mathcal{U}}$ is torsion-free. Denote by $J_{\mathcal{U}}$ the Jacobian variety of $X_{\mathcal{U}}$. Let $\mathbb{F}_{q^{2n}}$ be the field with q^{2n} elements, where q is the residue characteristic of \mathfrak{q} and $|\mathfrak{q}| = q^n$ for a positive integer n . Let $J_{\mathcal{U}}^{\text{ss}}(\mathbb{F}_{q^{2n}})$ be the subgroup generated by the divisors supported on the supersingular points in $J_{\mathcal{U}}(\mathbb{F}_{q^{2n}})$. Then by [22], Section 3, (G), there is a canonical isomorphism

$$J_{\mathcal{U}}(\mathbb{F}_{q^{2n}})/J_{\mathcal{U}}^{\text{ss}}(\mathbb{F}_{q^{2n}}) \simeq \Gamma_{\mathcal{U}}^{\text{ab}}, \quad (12)$$

where, if G is a group, G^{ab} is the abelianization of G .

Let $U \subseteq \hat{B}^\times$ be a compact open subgroup and define $X_U \rightarrow \text{Spec}(F')$, where F' is a suitable abelian extension of F , to be the Shimura curve whose complex points are

$$X_U(\mathbb{C}) = B^\times \backslash \hat{B}^\times \times \mathcal{H}^\pm / U \simeq \coprod_{i=1}^t X_i(\mathbb{C}), \quad X_j(\mathbb{C}) = \Gamma_j \backslash \mathcal{H} \quad (13)$$

where $\Gamma_i \subseteq B^\times$ are suitable arithmetic subgroups. Write J_U for the Jacobian variety of X_U . Fix a prime \mathfrak{q} such that the \mathfrak{q} -component $U_{\mathfrak{q}}$ of U is isomorphic to $\text{GL}_2(\mathcal{O}_{F,\mathfrak{q}})$. For any $i = 1, \dots, t$, let $\tilde{\Gamma}_i$ denote the subgroup of norm-one elements in $\Gamma_j[1/\mathfrak{q}]/\mathcal{O}_F^\times[1/\mathfrak{q}]$. Assume that

$$\text{all the groups } \tilde{\Gamma}_i \text{ are torsion free.} \quad (14)$$

Let J_i denote the Jacobian variety of X_i and set $\tilde{\Gamma} := \prod_{i=1}^t \tilde{\Gamma}_i$. If $J^{\text{ss}}(\mathbb{F}_{q^{2n}})$ denotes the set of supersingular points in $J(\mathbb{F}_{q^{2n}})$, then from (12)

$$J_U(\mathbb{F}_{q^{2n}})/J_U^{\text{ss}}(\mathbb{F}_{q^{2n}}) \simeq \tilde{\Gamma}^{\text{ab}}. \quad (15)$$

By fixing an embedding of \mathcal{B} into $\text{M}_2(F_{\ell_2})$, one obtains an action of $\tilde{\Gamma}_i$ on the Bruhat–Tits tree $\mathcal{T}_{\mathfrak{q}}$ of $\text{PGL}_2(F_{\mathfrak{q}})$. Let v_0 be the vertex of $\mathcal{T}_{\mathfrak{q}}$ such that the stabilizer $\tilde{\Gamma}_{v_{i,0}}$ of $v_{i,0}$ in $\tilde{\Gamma}_i$ is the image of Γ_i in $\tilde{\Gamma}_i$. Let $e_{i,0}$ be the edge originating from $v_{i,0}$ and such that the stabilizer $\tilde{\Gamma}_{e_{i,0}}$ of $e_{i,0}$ in $\tilde{\Gamma}_i$ is the image of the subgroup Γ'_i of Γ_i obtained as in (13) but with $U \cap U_0(\mathfrak{q})$ replacing U . Here $U_0(\mathfrak{q})$ is defined by imposing that its local components $U_0(\mathfrak{q})_{\mathfrak{q}}$ satisfy the following conditions: $U_0(\mathfrak{q})_{\mathfrak{q}}$ is the standard upper triangular subgroup $\Gamma_0(\mathfrak{q})$ of $\text{GL}_2(F_{\mathfrak{q}})$ and $U_0(\mathfrak{q})_{\mathfrak{q}'} = \text{GL}_2(\mathcal{O}_{F,\mathfrak{q}'})$ for $\mathfrak{q}' \neq \mathfrak{q}$. More explicitly,

$$X_{U \cap U_0(\mathfrak{q})} = \coprod_{i=1}^t X'_i, \quad \text{with } X'_i = \Gamma'_i \backslash \mathcal{H}.$$

Write $v_{i,1}$ for the target of $e_{i,0}$. The group $\tilde{\Gamma}_i$ acts on the tree $\mathcal{T}_{\mathfrak{q}}$ with the closed edge attached to $e_{i,0}$ as a fundamental region. Set $\tilde{\Gamma}_{v_0} := \prod_{i=1}^t \tilde{\Gamma}_{v_{i,0}}$, $\tilde{\Gamma}_{v_1} := \prod_{i=1}^t \tilde{\Gamma}_{v_{i,1}}$ and $\tilde{\Gamma}_{e_0} := \prod_{i=1}^t \tilde{\Gamma}_{e_{i,0}}$. Hence, taking the product over all $i = 1, \dots, t$ of the exact sequence in Proposition 13, Section II, 2.8 in [43] for $i = 1$, $M = \mathbb{F}_p$, $G = \tilde{\Gamma}_i$ yields

$$0 \longrightarrow \text{Hom}(\tilde{\Gamma}, \mathbb{F}_p) \longrightarrow \text{Hom}(\tilde{\Gamma}_{v_0}, \mathbb{F}_p) \oplus \text{Hom}(\tilde{\Gamma}_{v_1}, \mathbb{F}_p) \xrightarrow{d} \text{Hom}(\tilde{\Gamma}_{e_0}, \mathbb{F}_p).$$

For $i = 1, \dots, t$ there are natural injective maps as in [28], Section 1, Equation (3):

$$\psi_i: J_i(\mathbb{C}) \longrightarrow \text{Hom}(\Gamma_i, \mathbb{S}) \quad \text{and} \quad \psi'_i: J'_i(\mathbb{C}) \longrightarrow \text{Hom}(\Gamma'_i, \mathbb{S}), \quad (16)$$

where $\mathbb{S} := \{z \in \mathbb{C} : |z| = 1\}$. Hence in the above exact sequence the modules appearing in the source and in the target of d correspond to the p -torsion of J_i and J'_i respectively, where J'_i is the Jacobian variety of X'_i .

Suppose now that U is contained in some Eichler order of \mathcal{B} of level \mathfrak{r} and let g be a modular form with coefficients in a finite field \mathbb{F} , of weight 2, level K and trivial central character, which is an eigenform for the quotient \mathbb{T} of the Hecke algebra of level $\mathfrak{m}^{-\ell}$ acting faithfully on J_U (recall that the discriminant of \mathcal{B} is $\mathfrak{n}^{-\ell}$). Let \mathfrak{m}_g be the kernel of the homomorphism $\mathbb{T} \rightarrow \mathbb{F}$ associated to g .

Assumption 7.18. Let U be an open compact subgroup of \widehat{B}^\times such that (14) is verified. If the residual Galois representation on $\mathrm{GL}_2(\mathbb{F})$ associated to g is irreducible then $\mathrm{Hom}(\tilde{\Gamma}, \mathbb{F}_p)[\mathfrak{m}_g] = 0$.

Remark 7.19. The technical condition in Assumption 7.18 is essential in the proof of Lemma 7.20 below. It consists in a version of Ihara's Lemma for Shimura curves over totally real fields. Indeed, if $F = \mathbb{Q}$, Assumption 7.18 holds thanks to Theorem 2 in [12] because under the above identifications the map d corresponds to the map α_p in that theorem. The result of Theorem 2 in [12] can be understood as an analogue of Ihara's Lemma in the context of Shimura curves over \mathbb{Q} . The results contained in [12] and successively refined in [13] are partially generalized to the totally real case in [25]. However, [25] does not cover the full generalization of Theorem 2 in [12]. It might be possible that the techniques in [25] and [26] can be used to prove some results in the direction of an analogue of Theorem 2 in [12]. In this paper we follow [15], which assumes a suitable generalization to totally real fields of Ihara's Lemma as an hypothesis, although Assumption 7.18 is stated in a different form with respect to [15], Hypothesis 5.9. Similar results for Hilbert modular varieties hold: see [14].

As a consequence of Assumption 7.18 we see that $\tilde{\Gamma}^{\mathrm{ab}}/\mathfrak{m}_g = 0$. Let now R be the ring of integers of a finite extension of \mathbb{Q} and fix a maximal ideal v of R such that $R_v/v \simeq \mathbb{F}$, where R_v is the completion of R at v . Suppose that g is a modular form with coefficients in R_v/v^m for some integer $m \geq 1$ of weight 2, level U and trivial central character, which is an eigenform for the Hecke algebra \mathbb{T} ; let \mathcal{I}_g denote the kernel of the associated homomorphism $\mathbb{T} \rightarrow R_v/v^m$ and note that \mathfrak{m}_g is the maximal ideal containing \mathcal{I}_g . If the above conditions on g are satisfied, $\tilde{\Gamma}^{\mathrm{ab}}/\mathfrak{m}_g = 0$ and hence, by Nakayama's Lemma, $\tilde{\Gamma}^{\mathrm{ab}}/\mathcal{I}_g = 0$. By (15),

$$\text{the canonical map } J_{\mathcal{U}}^{\mathrm{ss}}(\mathbb{F}_{q^{2n}}) \longrightarrow J_{\mathcal{U}}(\mathbb{F}_{q^{2n}})/\mathcal{I}_g \text{ is surjective.} \quad (17)$$

Suppose from now on that Assumption 7.18 is verified.

Lemma 7.20. *The map γ is surjective.*

Proof. Write $X = X^{(\ell_1)}$ and $J = J^{(\ell_1)}$. Let $J^{ss}(\mathbb{F}_{\ell_2^2})$ be the set of supersingular points in $J(\mathbb{F}_{\ell_2^2})$, where $\mathbb{F}_{\ell_2^2}$ is the quadratic extension of the residue field \mathbb{F}_ℓ of \mathcal{O}_F at ℓ_2 . Since the map (11) is surjective, it is enough to show that

$$\text{the canonical map } J^{ss}(\mathbb{F}_{\ell_2^2}) \longrightarrow J(\mathbb{F}_{\ell_2^2})/\mathcal{I}_{f_{\ell_1}} \text{ is surjective.} \quad (18)$$

Recall that X is the Shimura curve defined over F whose complex points are

$$X(\mathbb{C}) = \mathcal{B}^\times \backslash \widehat{\mathcal{B}}^\times \times \mathcal{H}^\pm / \widehat{\mathcal{R}}^\times.$$

Define X' to be the Shimura curve defined over F whose complex points are

$$X'(\mathbb{C}) = \mathcal{B}^\times \backslash \widehat{\mathcal{B}}^\times \times \mathcal{H}^\pm / \widehat{\mathcal{R}}'^\times,$$

where $\mathcal{R}' \subseteq \mathcal{R}$ is defined by requiring that, for a fixed isomorphism

$$\iota_{\wp}: \mathcal{R} \otimes_{\mathcal{O}_F} \mathcal{O}_{F,\wp} \simeq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_{F,\wp}) \mid c \equiv 0 \pmod{\wp} \right\},$$

$\mathcal{R}' \otimes_{\mathcal{O}_F} \mathcal{O}_{F,\wp}$ correspond to the elements which are congruent to $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \pmod{\wp}$, while $\mathcal{R}' \otimes_{\mathcal{O}_F} \mathcal{O}_{F,\mathfrak{q}} = \mathcal{R} \otimes_{\mathcal{O}_F} \mathcal{O}_{F,\mathfrak{q}}$ if $\mathfrak{q} \neq \wp$. Since $\mathcal{R}' \subseteq \mathcal{R}$, there is a canonical projection map $u: X' \rightarrow X$ and also, by Picard (respectively, Albanese) functoriality, maps $u^*: J \rightarrow J'$ (respectively, $u_*: J' \rightarrow J$), where J and J' are the Jacobian varieties of X and X' respectively. Write as above

$$X(\mathbb{C}) = \coprod_{i=1}^s X_i(\mathbb{C}) \quad \text{and} \quad X'(\mathbb{C}) = \coprod_{j=1}^t X'_j(\mathbb{C})$$

where $X_i = \Gamma_i \backslash \mathcal{H}$ and $X'_j(\mathbb{C}) = \Gamma'_j \backslash \mathcal{H}$ for suitable arithmetic subgroups Γ_i and Γ'_j ; here s and t are suitable integers such that $t \geq s$. The canonical projection $u: X' \rightarrow X$ can be decomposed as t projections $X'_j \rightarrow X_{i(j)}$ and if $i(j_1) = i(j_2)$ (that is, two projections have the same target), then $\Gamma'_{j_1} = \Gamma'_{j_2}$. For details, see Section 3 in [20]. Write finally J_i and J'_j for the Jacobian varieties of X_i and X'_j , respectively.

The subgroups $\tilde{\Gamma}'_j$ of norm one elements in $\Gamma'_j[1/\ell_2]/\mathcal{O}_F[1/\ell_2]$ are torsion free (see for example [19], Lemma 7.1, after noticing that p is not ramified in the extension K/\mathbb{Q}). Now view f_{ℓ_1} as a $\pmod{\pi^n}$ eigenform on X' and write $\mathcal{I}'_{f_{\ell_1}}$ for its associated ideal in the Hecke algebra \mathbb{T}_{ℓ_1} acting faithfully on J' . Write $\mathfrak{m}_{f_{\ell_1}}$ for the maximal ideal containing $\mathcal{I}'_{f_{\ell_1}}$. Since $\mathfrak{m}_{f_{\ell_1}}$ corresponds to an irreducible representation, it follows from (17) that

$$\text{the canonical map } J'^{ss}(\mathbb{F}_{\ell_2^2}) \longrightarrow J'(\mathbb{F}_{\ell_2^2})/\mathcal{I}'_{f_{\ell_1}} \text{ is surjective.} \quad (19)$$

We need the generalization to this context of [28], which can be obtained as follows. For any $j = 1, \dots, t$, let $i(j)$ such that $i(j(i)) = i$, that is, u^* maps

$J_{i(j)}$ into J'_j . An element x belongs to $\Sigma_j := \ker(J_{i(j)}(\mathbb{C}) \rightarrow J'_j(\mathbb{C}))$ if and only if the kernel of the map $\psi_{i(j)}(x)$ associated to x as in (16) contains Γ'_j . Set $\Sigma := \ker(J(\mathbb{C}) \rightarrow J'(\mathbb{C}))$. Using the fact that $\Gamma'_{j_1} = \Gamma'_{j_2}$ if $i(j_1) = i(j_2)$, we get an injection:

$$0 \longrightarrow \Sigma \longrightarrow \bigoplus_{i=1}^s \operatorname{Hom}(\Gamma_i / \Gamma'_{j(i)}, \mathbb{S}).$$

The order of the group $\widehat{\mathcal{R}}^\times / \widehat{\mathcal{R}}'^\times$ is prime to p , hence the same is true for the order of $(g^{-1} \widehat{\mathcal{R}}^\times g) / (g^{-1} \widehat{\mathcal{R}}'^\times g)$ for any $g \in \widehat{\mathcal{B}}^\times$. Since the groups $\Gamma_i / \Gamma'_{j(i)}$ are contained in $(g^{-1} \widehat{\mathcal{R}}^\times g) / (g^{-1} \widehat{\mathcal{R}}'^\times g)$ for suitable elements $g \in \widehat{\mathcal{B}}^\times$, it follows the order of any $\Gamma_i / \Gamma'_{j(i)}$ is prime to p , so the same is true for Σ . Dualizing shows that the cokernel of the map $u_*: J'(\mathbb{F}_{\ell_2^2}) \rightarrow J(\mathbb{F}_{\ell_2^2})$ has order prime to p . It follows that

$$\text{the canonical map } J'(\mathbb{F}_{\ell_2^2}) \longrightarrow J(\mathbb{F}_{\ell_2^2}) / \mathcal{I}_{f_{\ell_1}} \text{ is surjective.} \quad (20)$$

Finally, combining (19) and (20) shows (18). \square

Let B'/F be the totally definite quaternion algebra of discriminant $\mathfrak{n}^- \ell_1 \ell_2$ and R' an Eichler order of B' of level $\wp \mathfrak{n}^+$. For any ring C , denote by $S_2^{B'}(\wp \mathfrak{n}^+, C)$ the C -module of functions:

$$B'^\times \backslash \widehat{B}'^\times / \widehat{R}'^\times \longrightarrow C.$$

This module is endowed with an action on the Hecke algebra $\mathbb{T}_{\mathfrak{n} \ell_1 \ell_2}$.

Proposition 7.21. *There exists $g \in S_2^{B'}(\wp \mathfrak{n}^+, \mathcal{O}_{f,\pi} / \pi^n)$ such that:*

- (1) *for prime ideals $\mathfrak{q} \nmid \mathfrak{n} \ell_1 \ell_2$: $T_{\mathfrak{q}}(g) \equiv a_{\mathfrak{q}}(f)g \pmod{\pi^n}$;*
- (2) *for prime ideals $\mathfrak{q} \mid \mathfrak{n}$: $U_{\mathfrak{q}}(g) \equiv a_{\mathfrak{q}}(f)g \pmod{\pi^n}$;*
- (3) *$U_{\ell_1}g \equiv \epsilon_1 g \pmod{\pi^n}$ and $U_{\ell_2}g \equiv \epsilon_2 g \pmod{\pi^n}$.*

Furthermore, if (ℓ_1, ℓ_2) is a rigid pair, then g can be lifted to a π -isolated form in $S_2^{B'}(\wp \mathfrak{n}^+)$ taking values in $\mathcal{O}_{f,\pi}$.

Proof. Write \mathbb{T}_{ℓ_1} (respectively, $\mathbb{T}_{\ell_2, \ell_1}$) for the quotient of the Hecke algebra $\mathbb{T}_{\mathfrak{n} \ell_1}$ (respectively, $\mathbb{T}_{\mathfrak{n} \ell_1 \ell_2}$) acting on cusp forms of weight 2, trivial central character, $\Gamma_0(\mathfrak{n} \ell_1)$ (respectively, $\Gamma_0(\mathfrak{n} \ell_1 \ell_2)$) level structure and new at $\mathfrak{n}^- \ell_1$. Write

$$f_{\ell_1}: \mathbb{T}_{\ell_1} \longrightarrow \mathcal{O}_{f,\pi} / \pi^n$$

for the modular form satisfying $f_{\ell_1} \equiv f \pmod{\pi^n}$. This form has the properties that $T_{\mathfrak{q}}(f_{\ell_1}) \equiv a_{\mathfrak{q}}(f)f_{\ell_1} \pmod{\pi^n}$ for all $\mathfrak{q} \nmid \mathfrak{n} \ell_1$, $U_{\mathfrak{q}}(f_{\ell_1}) \equiv a_{\mathfrak{q}}(f)f_{\ell_1} \pmod{\pi^n}$ for all $\mathfrak{q} \mid \mathfrak{n}$ and $U_{\ell_2}(f_{\ell_1}) \equiv \epsilon_1 f_{\ell_1} \pmod{\pi^n}$.

Let $\mathcal{R}_1 \subseteq \mathcal{R}$ be an Eichler order of level $\wp \mathfrak{n}^+ \ell_2$ and denote by $X^{(\ell_2, \ell_1)}$ the Shimura curve (over F) whose complex points are given by:

$$X^{(\ell_2, \ell_1)}(\mathbb{C}) = \mathcal{B}^\times \backslash \widehat{\mathcal{B}}^\times \times \mathcal{H}^\pm / \widehat{\mathcal{R}}_1^\times.$$

Recall from above the set $\mathcal{S}_{\ell_2} \subseteq X^{(\ell_1)}(\mathbb{F}_{\ell_2^2})$ of supersingular points of $X^{(\ell_1)}$ in characteristic ℓ_2 . By [49], Section 5.4,

$$\mathcal{S}_{\ell_2} \simeq B'^{\times} \backslash \widehat{B}'^{\times} / \widehat{R}'^{\times}. \quad (21)$$

It follows that the character group \mathbb{X}_{ℓ_2} of $X^{(\ell_2, \ell_1)}$ at ℓ_2 is identified with the module $\text{Div}^0(\mathcal{S}_{\ell_2})$. Furthermore, the action of $\mathbb{T}_{\ell_2, \ell_1}$ on \mathbb{X}_{ℓ_2} induced from the action on $\text{Pic}(X^{(\ell_2, \ell_1)})$ by Picard functoriality is compatible with the standard Albanese action of $\mathbb{T}_{\ell_2, \ell_1}$ via correspondences in the set of supersingular points. Therefore, γ can also be viewed as a $\mathcal{O}_{f, \pi} / \pi^n$ -valued modular form on $B'^{\times} \backslash \widehat{B}'^{\times} / \widehat{R}'^{\times}$. Denote by g this modular form. Since γ is surjective by Lemma 7.20, the image of g is not contained in any proper subgroup of $\mathcal{O}_{f, \pi} / \pi^n$.

To show that g has the desired properties, write $T_{\mathfrak{q}}^*$ (with $\mathfrak{q} \nmid n\ell_1\ell_2$) and $U_{\mathfrak{q}}^*$ (with $\mathfrak{q} \mid n\ell_1\ell_2$) for the Hecke operators in $\mathbb{T}_{\ell_2, \ell_1}$ and $T_{\mathfrak{q}}$ and $U_{\mathfrak{q}}$ for the Hecke operators in \mathbb{T}_{ℓ_1} . By Lemma 7.17, $T_{\mathfrak{q}}^* g = a_{\mathfrak{q}}(f)g \pmod{\pi^n}$ and $U_{\mathfrak{q}}^* g = a_{\mathfrak{q}}(f)g \pmod{\pi^n}$. By Lemma 7.2 of [25], $U_{\ell_2}^* x = \text{Frob}_{\ell_2}(F)x$ for $x \in \mathcal{S}_{\ell_2}$. Hence Lemma 7.17 yields $(U_{\ell_2}^* g)(x) = \gamma(\text{Frob}_{\ell_2}(F)x) = \epsilon_2 g(x)$.

For the final part of the statement: The modular form g yields a surjective morphism $\phi_g: \mathbb{T}_{\ell_2, \ell_1} \rightarrow \mathcal{O}_{f, \pi} / \pi^n$; if (ℓ_1, ℓ_2) is a rigid pair, then $\mathbb{T}_{\ell_2, \ell_1} \simeq \mathcal{O}_{f, \pi}$ and therefore ϕ_g lifts to characteristic zero. \square

7.5. Explicit reciprocity laws. The two following theorems explore the relations between the classes $\kappa(\ell)$ constructed in Section 7.4 and the \wp -adic L -functions of Section 4. Their proofs are similar to the proofs of the corresponding results [5], Theorems 4.1 and 4.2. We will present a sketch of the arguments: for more details, the reader is referred to [5]. See also Section 5.3 in [29] and Section 3.5 in [30], where a result similar to that of Theorem 7.22 is proved.

Recall the maps ∂_{ℓ} and v_{ℓ} introduced in § 5.2. Thanks to the isomorphisms (8), we find a decomposition

$$\widehat{H}(K_{\wp^{\infty}, \ell}, T_{f, \pi^n}) = \widehat{H}_{\text{sing}}^1(K_{\wp^{\infty}, \ell}, T_{f, \pi^n}) \oplus \widehat{H}_{\text{fin}}^1(K_{\wp^{\infty}, \ell}, T_{f, \pi^n}).$$

In this decomposition the map ∂_{ℓ} corresponds to the projection to the first factor, while the map v_{ℓ} , a priori only defined on the kernel of ∂_{ℓ} , can be extended to a map

$$v_{\ell}: \widehat{H}(K_{\wp^{\infty}, \ell}, T_{f, \pi^n}) \longrightarrow \widehat{H}_{\text{fin}}^1(K_{\wp^{\infty}, \ell}, T_{f, \pi^n})$$

(the projection to the second factor).

Theorem 7.22 (First Explicit Reciprocity Law). *$v_{\ell}(\kappa(\ell)) = 0$ and the equality*

$$\partial_{\ell}(\kappa(\ell)) \equiv \theta_f \pmod{\pi^n}$$

holds in $\widehat{H}_{\text{sing}}^1(K_{\wp^{\infty}, \ell}, T_{f, \pi^n}) \simeq \Lambda_{\wp, \pi} / \pi^n \Lambda_{\wp, \pi}$ up to multiplication by elements in $\mathcal{O}_{f, \pi}^{\times}$ and $G_{\wp^{\infty}}$.

Proof. Denote by $\tilde{\partial}_\ell$ the residue map

$$\hat{H}^1(\tilde{K}_{\wp^\infty}, T_{f, \pi^n}) \longrightarrow \hat{H}_{\text{sing}}^1(\tilde{K}_{\wp^\infty, \ell}, T_{f, \pi^n})$$

(these cohomology groups are defined for $\hat{H}^1(K_{\wp^\infty}, T_{f, \pi^n})$ and $\hat{H}_{\text{sing}}^1(K_{\wp^\infty, \ell}, T_{f, \pi^n})$ by replacing K_{\wp^∞} by \tilde{K}_{\wp^∞}). It is enough to show that $\tilde{\partial}_\ell(\{P_m^*\}_m) \equiv \tilde{\theta}_f \pmod{\pi^n}$ (note the abuse of notation for the image of $\{P_m^*\}_m$ in $\hat{H}^1(\tilde{K}_{\wp^\infty}, T_{f, \pi^n})$).

Recall the notations of Section 6.2: Let B/F be the quaternion algebra which is ramified at all archimedean places and whose discriminant is $\text{Disc}(B) = \mathfrak{n}^-$. Denote by $R \subseteq B$ an Eichler order of level $\wp \mathfrak{n}^+$.

Recall that $\text{End}(P_m) \simeq \mathcal{O}_{\wp^m}$, where $\text{End}(P_m)$ is defined in [48], Section 2.1.1. The Heegner point P_m is described in Section 2.1.2 of [48] in terms of a certain abelian variety A_m with additional structures. Let k denote as in [48], Section 2.2, the residue field of the maximal unramified extension of $\mathcal{O}_{K, \ell}$. Denote by \bar{A}_m the reduced abelian variety over k and by $\text{End}(\bar{P}_m)$ the endomorphism ring of \bar{A}_m as defined in [48], Section 2.3.3. Then, by [48], Section 2.3.3, $\text{End}(\bar{P}_m) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq B$. Tensoring by \mathbb{Q} the map

$$\text{End}(P_m) \longrightarrow \text{End}(\bar{P}_m)$$

induced by reduction of endomorphisms yields an embedding $\psi: K \hookrightarrow B$.

Let $\mathcal{H}_\ell := \mathbb{C}_\ell - F_\ell$ be the ℓ -adic upper half plane, where \mathbb{C}_ℓ is the completion of an algebraic closure of F_ℓ . The \mathbb{C}_ℓ -points of the special fiber $X_\ell^{(\ell)}$ at ℓ of the Shimura curve $X^{(\ell)}$ can be described by using the Cerednik–Drinfeld theorem:

$$X_\ell^{(\ell)}(\mathbb{C}_\ell) \simeq B^\times \backslash (\hat{B}^\times \times \mathcal{H}_\ell) / \hat{R}[1/\ell]^\times,$$

where $R[1/\ell]$ is the Eichler $\mathcal{O}_F[1/\ell]$ -order of B of level $\wp \mathfrak{n}^+$ and $\mathcal{O}_F[1/\ell]$ is the ring of ℓ -integers of F . Then the point P_m reduces to the point $P'_m = (1, z) \in X_\ell^{(\ell)}(K_\ell)$, where z is one of the two fixed points of $\psi(K^\times)$ acting on \mathcal{H}_ℓ . The integrality property of P'_m follows because, since ℓ is inert in K/F , then it splits completely in \tilde{K}_{\wp^∞} .

Let \mathcal{V}_ℓ and \mathcal{E}_ℓ be, respectively, the set of geometrically irreducible components and the set of singular points, respectively, of $\bar{X}_\ell^{(\ell)}$. By [49], Lemma 5.4.4, the set \mathcal{V}_ℓ can be identified with $B_e^\times \backslash \hat{B}^\times / \hat{R}^\times$, where B_e^\times is the set of elements of B with even order at \wp . The reduction of P'_m in the special fiber $\bar{X}_\ell^{(\ell)}$ of $X_\ell^{(\ell)}$ belongs to a single geometrically irreducible component: this is because, since ℓ is inert in K and $\mathcal{O}_{\wp^m} \otimes \mathbb{Z}_\ell$ is maximal, $\psi(\mathcal{O}_{\wp^m} \otimes \mathbb{Z}_\ell)$ is contained in a unique maximal order, hence the action of $\psi(K^\times)$ on $\mathcal{V}_\ell \cup \mathcal{E}_\ell$ has a unique fixed point which is a vertex. Denote by $r(P_m)$ the corresponding element in $B_e^\times \backslash \hat{B}^\times / \hat{R}^\times$.

Fix a prime ℓ_∞ of \tilde{K}_{\wp^∞} dividing ℓ and set $\ell_m := \ell_\infty \cap K_{\wp^m}$. Note that the different choices of ℓ_∞ are permuted by the multiplication by an element of \tilde{G}_{\wp^∞} , and the same dependence holds for the definition of $\tilde{\theta}_f$. Let Φ_{ℓ_m} be the group of

connected components of the fiber at ℓ_m of the Néron model of $J^{(\ell)}$ over $\mathcal{O}_{\tilde{K}_{\wp^m}}$. There is a specialization map $\delta_{\ell_m}: J^{(\ell)}(\tilde{K}_{\wp^m}) \rightarrow \Phi_{\ell_m}$ which fits into the following commutative diagram:

$$\begin{array}{ccc} J^{(\ell)}(\tilde{K}_{\wp^m})/\mathcal{I}_{f_\ell} & \longrightarrow & H^1(\tilde{K}_{\wp^m}, T_{f,\pi^n}) \\ \downarrow \delta_{\ell_m} & & \downarrow \tilde{\delta}_\ell \\ \Phi_{\ell_m}/\mathcal{I}_{f_\ell} & \xrightarrow{\sim} & H_{\text{sing}}^1(\tilde{K}_{\wp^m, \ell_m}, T_{f,\pi^n}) \end{array} \quad (22)$$

where the bottom horizontal arrow is an isomorphism. The Heegner point P_m satisfies, by Section 2 of the Appendix in [4], the following relation:

$$\delta_{\ell_m}(P_m) = \omega_\ell(r(P_m)),$$

where $\omega_\ell: \mathbb{Z}^0[\mathcal{V}_\ell] \rightarrow \Phi_\ell$ is the map arising from the exact sequence

$$0 \longrightarrow \mathcal{X}_\ell \longrightarrow \mathcal{X}_\ell^\vee \longrightarrow \Phi_\ell \longrightarrow 0$$

connecting Φ_ℓ with the character group \mathcal{X}_ℓ of the maximal torus of the special fiber of $J_\ell^{(\ell)}$ and its \mathbb{Z} -dual \mathcal{X}_ℓ^\vee . Recall the identification of \mathcal{V}_ℓ with $B_e^\times \backslash \hat{B}^\times / \hat{R}^\times$ and note that the last double coset space can be identified with two copies of $B^\times \backslash \hat{B}^\times / \hat{R}^\times$ by sending a class $[b]$ in $B_e^\times \backslash \hat{B}^\times / \hat{R}^\times$ to the class $[b]$ in the first copy of $B^\times \backslash \hat{B}^\times / \hat{R}^\times$ if the \wp -adic valuation of b is even and to the class of $[b]$ of the second copy otherwise. It follows that evaluation on Heegner points gives rise to an Hecke equivariant map:

$$B^\times \backslash \hat{B}^\times / \hat{R}^\times \longrightarrow \Phi_{\ell_m} / \mathcal{I}_{f_\ell} \longrightarrow H_{\text{sing}}^1(K_{\wp^m, \ell_m}, T_{f,\pi^n}) \simeq \mathcal{O}_{f,\pi} / \pi^n$$

which, by multiplicity one, is equal to the modular form f^B up to multiplication by an element in $(\mathcal{O}_{f,\pi} / \pi^n)^\times$.

It follows from above that $\tilde{\delta}_\ell(P_m) = f^B(r_\ell(P_m)) \pmod{\pi^n}$. The result follows now from the definition of P_m^* and θ_f because the action of G_{\wp^∞} on $\text{Gr}^{(\ell)}(\wp^m)$ is compatible with the action of G_{\wp^∞} on $\text{Gr}(\wp^m)$ and, by our choice of the orientation at \wp , the compatibility of the sequence $\{P_m\}$ translates into the compatibility of Gross points. \square

Theorem 7.23 (Second Explicit Reciprocity Law). *Let ℓ_1 and ℓ_2 be two n -admissible primes. Let g be as in Proposition 7.21. The equality*

$$v_{\ell_2}(\kappa(\ell_1)) = \theta_g$$

holds in $\hat{H}_{\text{fin}}^1(K_{\wp^\infty, \ell_2}, T_{f,\pi^n}) \simeq \Lambda_{\wp,\pi} / \pi^n \Lambda_{\wp,\pi}$ up to multiplication by elements in $\mathcal{O}_{f,\pi}^\times$ and G_{\wp^∞} .

Proof. Consider the sequence $\{P_m\}_m$ of Heegner points. Fix (as in the proof of the above theorem) a prime $\ell_{2,\infty}$ of \tilde{K}_{\wp^∞} above ℓ_2 and let $\ell_{2,m} := \ell_{2,\infty} \cap \tilde{K}_{\wp^m}$. Since ℓ_2 is inert in K , the points P_m reduce modulo $\ell_{2,\infty}$ to supersingular points $\bar{P}_m \in X^{(\ell_1)}(\mathbb{F}_{\ell_{2,m}})$, where $\mathbb{F}_{\ell_{2,m}}$ is the residue field of \tilde{K}_{\wp^m} at $\ell_{2,m}$. Identify $\mathbb{F}_{\ell_{2,m}}$ with \mathbb{F}_{ℓ_2} for all m . Then \bar{P}_m can be viewed as a point in S_{ℓ_2} , and hence, by Equation (21), \bar{P}_m can be identified with an element in $B'^{\times} \backslash \hat{B}'^{\times} / \hat{R}'^{\times}$.

Reduction modulo $\ell_{2,m}$ of endomorphism as in the proof of Theorem 7.22 yields by extension of scalars an embedding $\varphi: K \rightarrow B'$, which is independent of m . The Galois action of \tilde{G}_{\wp^∞} on P_m is compatible with the action of \tilde{G}_{\wp^∞} on \bar{P}_m via φ . Write

$$\tilde{\theta}_{g,m} = \alpha_{\wp}^{-m} \sum_{\sigma \in \tilde{G}_{\wp^m}} g(\sigma \bar{P}_m) \cdot \sigma \in \mathcal{O}_{f,\pi} / \pi^n [\tilde{G}_{\wp^m}],$$

so that $\tilde{\theta}_g = \varprojlim_m \tilde{\theta}_{g,m} \in \mathcal{O}_{f,\pi} / \pi^n [\tilde{G}_{\infty}]$. The choice of $\ell_{2,\infty}$ together with the isomorphism $H_{\text{fin}}^1(K_{\ell_2}, T_{f,\pi^n}) \simeq \mathcal{O}_{f,\pi} / \pi^n$ yields identifications:

$$H_{\text{fin}}^1(\tilde{K}_{\wp^m, \ell_2}, T_{f,\pi^n}) = \mathcal{O}_{f,\pi} / \pi^n [\tilde{G}_{\wp^m}],$$

$$\hat{H}_{\text{fin}}^1(\tilde{K}_{\wp^\infty, \ell_2}, T_{f,\pi^n}) = \mathcal{O}_{f,\pi} / \pi^n [\tilde{G}_{\wp^\infty}],$$

where these cohomology groups are defined as in Section 5.2.1. By the definition of γ , the image of P_m^* in $H_{\text{fin}}^1(\tilde{K}_{\wp^m, \ell_2}, T_{f,\pi^n})$ corresponds to $\tilde{\theta}_{g,m} \pmod{\pi^n}$ and so the image of the compatible sequence $\{P_m^*\}$ corresponds to $\tilde{\theta}_g$. Define the class $\tilde{\kappa}(\ell_1)$ to be the image of $\{P_m^*\}$ in $\hat{H}^1(\tilde{K}_{\wp^\infty}, T_{f,\pi^n})$. It follows that $v_{\ell_2}(\tilde{\kappa}(\ell_1)) \in \hat{H}_{\text{fin}}^1(\tilde{K}_{\infty, \ell_2}, T_{f,\pi^n})$ is equal to $\tilde{\theta}_g \pmod{\pi^n}$. Since $\kappa(\ell_1)$ is the corestriction of $\tilde{\kappa}(\ell_1)$ from \tilde{K}_{\wp^∞} to K_{\wp^∞} , the result follows. \square

Corollary 7.24. *The equality*

$$v_{\ell_1}(\kappa(\ell_2)) \equiv v_{\ell_2}(\kappa(\ell_1)) \pmod{\pi^n}$$

holds in $\Lambda_{\wp,\pi} / \pi^n \Lambda_{\wp,\pi}$ up to multiplication by elements in $\mathcal{O}_{f,\pi}^\times$ and G_{\wp^∞} .

Proof. Since the definition of g is symmetric in ℓ_1 and ℓ_2 , this is obvious. \square

7.6. The argument. The remaining part of the section is devoted to the proof of Theorem 6.1. Keeping \wp fixed, denote $\text{Sel}_{\pi^\infty}(f/K_{\wp^\infty})$ (respectively, $\text{Sel}_{\pi^n}(f/K_{\wp^\infty})$) simply by $\text{Sel}_{f,\infty}$ (respectively, $\text{Sel}_{f,n}$). By Proposition 7.4, it is enough to show that $\varphi(\theta_f)^2$ belongs to $\text{Fitt}_{\mathcal{O}}(\text{Sel}_{f,\infty}^\vee \otimes_{\varphi} \mathcal{O})$ for all $\varphi \in \text{Hom}(\Lambda, \mathcal{O})$ where \mathcal{O} is the ring of integer of a finite extension of \mathbb{Q}_p . For this, by [33], Appendix, 10 on 325, is enough to show that

$$\varphi(\theta_f)^2 \text{ belongs to } \text{Fitt}_{\mathcal{O}}(\text{Sel}_{f,n}^\vee \otimes_{\varphi} \mathcal{O}) \text{ for all integers } n \geq 1. \quad (23)$$

Fix \mathcal{O} and φ as above. Write v for an uniformizer of \mathcal{O} . Set

$$t_f := \text{ord}_v(\varphi(\theta_f)).$$

If $\varphi(\theta_f) = 0$, then $\varphi(\theta_f)^2$ belongs trivially to $\text{Fitt}_{\mathcal{O}}(\text{Sel}_{f,n}^{\vee} \otimes_{\varphi} \mathcal{O})$ for all $n \geq 1$, so assume $\varphi(\theta_f) \neq 0$. If $\text{Sel}_{f,\infty}^{\vee} \otimes_{\varphi} \mathcal{O}$ is trivial, then its Fitting ideal is equal to \mathcal{O} and, again, $\varphi(\theta_f)^2$ belongs trivially to $\text{Fitt}_{\mathcal{O}}(\text{Sel}_{f,n}^{\vee} \otimes_{\varphi} \mathcal{O})$ for all $n \geq 1$, so assume that $\text{Fitt}_{\mathcal{O}}(\text{Sel}_{f,n}^{\vee} \otimes_{\varphi} \mathcal{O}) \neq 0$. The theorem is proved now by induction on t_f .

7.6.1. Construction of $\kappa_{\varphi}(\ell)$. Let ℓ be any $(n + t_f)$ -admissible prime and enlarge $\{\ell\}$ to a $(n + t_f)$ -admissible set S : such a set consists of s distinct $(n + t_f)$ -admissible primes such that the map

$$\text{Sel}_{f,n+t_f}(K) \longrightarrow \bigoplus_{\ell \in S} H_{\text{fin}}^1(K_{\ell}, A_{f,\pi^{n+t_f}})$$

is injective (Proposition 7.5 shows that such a set exists). Denote by \mathfrak{s} the square-free product of the primes in S and let

$$\kappa(\ell) \in \hat{H}_{\ell}^1(K_{\wp^{\infty}}, T_{f,\pi^{n+t_f}}) \subseteq \hat{H}_{\mathfrak{s}}^1(K_{\wp^{\infty}}, T_{f,\pi^{n+t_f}})$$

be the cohomology class attached to ℓ .

Proposition 7.25. *The group $\hat{H}_{\mathfrak{s}}^1(K_{\wp^{\infty}}, T_{f,\pi^n})$ is free of rank s over $\Lambda_{\varphi,\pi}/\pi^n$.*

Proof. This statement can be proved by a direct generalization of Theorem 3.2 in [2] as suggested in Proposition 3.3 in [5]. \square

Let $\kappa_{\varphi}(\ell)$ be the image of $\kappa(\ell)$ in

$$\mathcal{M} := \hat{H}_{\mathfrak{s}}^1(K_{\wp^{\infty}}, T_{f,\pi^{n+t_f}}) \otimes_{\varphi} \mathcal{O}.$$

Note that, by Proposition 7.25, \mathcal{M} is free of rank s over $\mathcal{O}_{f,\pi}/\pi^{n+t_f}$. By Theorem 7.22,

$$t := \text{ord}_v(\kappa_{\varphi}(\ell)) \leq \text{ord}_v(\partial_{\ell}(\kappa_{\varphi}(\ell))) = \text{ord}_v(\varphi(\theta_f)). \quad (24)$$

Choose an element $\tilde{\kappa}_{\varphi}(\ell) \in \mathcal{M}$ such that $v^t \tilde{\kappa}_{\varphi}(\ell) = \kappa_{\varphi}(\ell)$. This element is well defined modulo the v^t -torsion subgroup of \mathcal{M} ; to remove this ambiguity, denote by $\kappa'_{\varphi}(\ell)$ the image of $\tilde{\kappa}_{\varphi}(\ell)$ in $H_{\mathfrak{s}}^1(K_{\wp^{\infty}}, T_{f,\pi^n}) \otimes_{\varphi} \mathcal{O}$. The following properties of $\kappa'_{\varphi}(\ell)$ hold:

- (1) $\text{ord}_v(\kappa'_{\varphi}(\ell)) = 0$ (because $\text{ord}_v(\kappa_{\varphi}(\ell)) = t \leq t_f$);
- (2) $\partial_{\mathfrak{q}}(\kappa'_{\varphi}(\ell)) = 0$ for all $\mathfrak{q} \nmid \ell n^{-}$ (because $\kappa(\ell) \in \hat{H}_{\mathfrak{s}}^1(K_{\wp^{\infty}}, T_{f,n+t_f})$);
- (3) $v_{\ell}(\kappa'_{\varphi}(\ell)) = 0$ (by Theorem 7.22);

(4) $\partial_\ell(\kappa'_\varphi(\ell)) = t_f - t$ (by Theorem 7.22 and formula (24));

(5) The element $\partial_\ell(\kappa'_\varphi(\ell))$ belongs to the kernel of the homomorphism:

$$\eta_\ell: \hat{H}_{\text{sing}}^1(K_{\varphi^\infty, \ell}, T_{f, \pi^n}) \otimes_\varphi \mathcal{O} \longrightarrow \text{Sel}_{f, n}^\vee \otimes_\varphi \mathcal{O}. \quad (25)$$

To prove the last statement use the global reciprocity law of class field theory (5) as follows (see more details in [5]), Lemma 4.6. Denote by I_φ the kernel of φ . First note that it is enough to show that $\eta_\ell(\partial_\ell(\kappa'_\varphi(\ell)))(s) = 0$ for all $s \in \text{Sel}_{f, n}[I_\varphi]$. Note that, by the global reciprocity law of class field theory:

$$\sum_{\mathfrak{q} | S} \langle \partial_\ell(\tilde{\kappa}_\varphi(\ell)), s_\mathfrak{q} \rangle_\mathfrak{q} = 0$$

for all $s \in \text{Sel}_{f, n+t_f}[I_\varphi]$. On the other hand, $v^t \tilde{\kappa}_\varphi(\ell) = \kappa_\varphi(\ell)$ has trivial residue at all the primes $\mathfrak{q} \neq \ell$ (it is finite at those primes) so the element $\partial_\mathfrak{q}(\tilde{\kappa}_\varphi(\ell))$ annihilates $v^t H_{\text{fin}}^1(K_{\infty, \mathfrak{q}}, A_{f, \pi^{n+t_f}})[I_\varphi]$, which contains $H_{\text{fin}}^1(K_{\infty, \mathfrak{q}}, A_{f, \pi^n})[I_\varphi]$. Hence, if s belongs to $\text{Sel}_{f, n}[I_\varphi]$, then the terms in the above sum corresponding to primes $\mathfrak{q} \neq \ell$ are all zero. It follows that $\partial_\ell(\kappa'_\varphi(\ell))$ annihilates the image of $\text{Sel}_{f, n}[I_\varphi]$ in $H_{\text{fin}}^1(K_{\infty, \ell}, A_{f, \pi^n})$, so it belongs to the kernel of η_ℓ .

7.6.2. Case of $t_f = 0$. This is the basis for the induction argument. First, recall the following result.

Proposition 7.26. *The natural map $H^1(K, A_{f, \pi}) \rightarrow H^1(K_{\varphi^\infty}, A_{f, \pi^n})[\mathfrak{m}]$ induced by restriction is an isomorphism.*

Proof. This result can be obtained as in Theorem 3.4 of [5] by analyzing the inflation-restriction exact sequence

$$\begin{aligned} 0 \longrightarrow H^1(\text{Gal}(K_{\varphi^m}/K), A_{f, \pi^n}^{G_{K_{\varphi^m}}}) &\longrightarrow H^1(K, A_{f, \pi^n}) \longrightarrow \cdots \\ &\longrightarrow H^1(K_{\varphi^m}, A_{f, \pi^n})^{\text{Gal}(K_{\varphi^m}/K)} \longrightarrow H^2(\text{Gal}(K_{\varphi^m}/K), A_{f, \pi^n}^{G_{K_{\varphi^m}}}) \end{aligned}$$

where $G_{K_{\varphi^m}}$ is the absolute Galois group of K_{φ^m} , and the exact sequence

$$A_{f, \pi^{n-1}}^{G_K} \longrightarrow H^1(K, A_{f, \pi}) \longrightarrow H^1(K, A_{f, \pi^n}) \longrightarrow H^1(K, A_{f, \pi^n}) \longrightarrow H^2(K, A_{f, \pi}^{G_K})$$

induced by $0 \rightarrow A_{f, \pi} \rightarrow A_{f, \pi^n} \xrightarrow{\pi} A_{f, \pi^{n-1}} \rightarrow 0$ and noticing that, since $\rho_{f, \pi}$ is surjective, $A_{f, \pi^n}^{G_{K_{\varphi^m}}} = A_{f, \pi}^{G_K} = 0$. For details, see [5], Theorem 3.4. \square

Then we can state the basis of the inductive argument.

Proposition 7.27. *If $t_f = 0$ then $\text{Sel}_{f, n}^\vee = 0$.*

Proof. To prove this, note that, for all n -admissible primes ℓ , Theorem 7.22 implies that $\hat{H}_{\text{sing}}^1(K_{\varphi^\infty, \ell}, T_{f, \pi^n}) \otimes_{\varphi} \mathcal{O}$ is generated by $\partial_{\ell}(\kappa_{\varphi}(\ell))$ (as \mathcal{O} -module) and that the map η_{ℓ} in (25) is trivial. Assume now that $\text{Sel}_{f, n}^{\vee}$ is not trivial. Then Nakayama's lemma implies that the group $\text{Sel}_{f, n}^{\vee}/\mathfrak{m} = (\text{Sel}_{f, n}[\mathfrak{m}])^{\vee}$ is not trivial, where \mathfrak{m} is the maximal ideal of $\Lambda_{\varphi, \pi}$.

Let now $s \in \text{Sel}_{f, n}[\mathfrak{m}]$ be a non trivial element. Proposition 7.26 allows to consider s as an element of $H^1(K, A_{f, \pi})$. Invoke Proposition 7.5 to choose an n -admissible prime ℓ such that $\partial_{\ell}(s) = 0$ and $v_{\ell}(s) \neq 0$. Then the non degeneracy of the local Tate pairing implies that η_{ℓ} is trivial, which is a contradiction. \square

7.6.3. The minimality property. As a corollary of Proposition 7.25, note that

$$\text{the corestriction map } \hat{H}_{\#}^1(K_{\varphi^\infty}, T_{f, \pi^n})/\mathfrak{m} \longrightarrow H^1(K, T_{f, \pi}) \text{ is injective.} \quad (26)$$

Let now Π be the set of primes of \mathcal{O}_F such that:

- (1) ℓ is $n + t_f$ -admissible;
- (2) The number $t = \text{ord}_v(\kappa_{\varphi}(\ell))$ is minimal among the set of $(n + t_f)$ -admissible primes.

By Proposition 7.5, $\Pi \neq \emptyset$.

Proposition 7.28. $t < t_f$.

Proof. To prove this assertion, assume on the contrary that $t \geq t_f$. Since by definition $t \leq t_f$, then $t = t_f$ for all $(n + t_f)$ -admissible primes ℓ . Use Proposition 7.26 to choose a non trivial element in $H^1(K, A_{f, \pi}) \cap \text{Sel}_{f, n}$ (recall that by assumption, $\text{Sel}_{f, n}^{\vee} \otimes_{\varphi} \mathcal{O} \neq 0$, so $\text{Sel}_{f, n}[\mathfrak{m}] \neq 0$). By Proposition 7.5, choose an $(n + t_f)$ -admissible prime ℓ such that $v_{\ell}(s) \neq 0$. Now by the Property 5 enjoyed by the class $\kappa'_{\varphi}(\ell)$, it follows that $\text{ord}_v(\partial_{\ell}\kappa'_{\varphi}(\ell)) = 0$, so that $\partial_{\ell}\kappa'_{\varphi}(\ell)$ is a generator of $\hat{H}_{\text{sing}}^1(K_{\infty, \ell}, T_{f, \pi^n}) \otimes_{\varphi} \mathcal{O}$. By Nakayama's lemma again, the image of $\partial_{\ell}(\kappa'_{\varphi}(\ell))$ in $\hat{H}_{\text{sing}}^1(K_{\infty, \ell}, T_{f, \pi^n})/\mathfrak{m} \otimes_{\varphi} \mathcal{O}$ is not trivial. Use (26) to identify this last module with $H^1(K, T_{f, \pi}) \otimes \mathcal{O}$; then it follows that the natural image of $\partial_{\ell}(\kappa'_{\varphi}(\ell))$ in $H^1(K, T_{f, \pi}) \otimes \mathcal{O}$ is not trivial. By Property 5 enjoyed by the class $\kappa'_{\varphi}(\ell)$ again, it follows that $\partial_{\ell}(\kappa'_{\varphi}(\ell))$ is orthogonal to $v_{\ell}(s)$ with respect to the local Tate pairing, contradicting the fact that $\partial_{\ell}(\kappa'_{\varphi}(\ell))$ and $v_{\ell}(s)$ are both supposed to be non trivial and the fact that the Tate pairing is a perfect duality between one-dimensional \mathcal{O}/v -vector spaces. \square

7.6.4. Rigid pairs with the minimality property. This step is devoted to the proof that there exist primes $\ell_1, \ell_2 \in \Pi$ such that (ℓ_1, ℓ_2) is a rigid pair. To prove this, start by choosing any prime $\ell_1 \in \Pi$ and denote by s the image of $\kappa'_{\varphi}(\ell_1)$ in

$$(\hat{H}_{\#}^1(K_{\infty}, T_{f, \pi^n})/\mathfrak{m}) \otimes_{\varphi} \mathcal{O}/(v),$$

where \mathfrak{m} is the maximal ideal of $\Lambda_{\wp, \pi}$. By (26), view s as a non-zero element in $H^1(K, T_{f, \pi}) \otimes \mathcal{O}/(\nu)$. Note that $\partial_{\mathfrak{q}}(s) = 0$ for all $\mathfrak{q} \nmid \ell_1 \pi$. By Propositions 7.13 and 7.14, choose an $(n + t_f)$ -admissible prime ℓ_2 such that $\partial_{\ell_2}(s) = 0$, $v_{\ell_2}(s) \neq 0$ and either (ℓ_1, ℓ_2) is a rigid pair or $\text{Sel}_{\ell_2}(F, \text{ad}^0 \rho)$ is one-dimensional. The following relation holds:

$$t = \text{ord}_v(\kappa_{\varphi}(\ell_1)) \leq \text{ord}_v(\kappa_{\varphi}(\ell_2)) \leq \text{ord}_v(v_{\ell_1}(\kappa_{\varphi}(\ell_2))). \quad (27)$$

The first inequality follows from the minimality property of t using that $\ell_1 \in \Pi$ and that ℓ_2 is an $(n + t_f)$ -admissible prime. By the choice of ℓ_2 and Corollary 7.24, it follows that $\text{ord}_v(v_{\ell_1}(\kappa_{\varphi}(\ell_2))) = \text{ord}_v(v_{\ell_2}(\kappa_{\varphi}(\ell_1)))$. Now note that $\text{ord}_v(v_{\ell_2}(\kappa_{\varphi}(\ell_1))) \geq \text{ord}_v(\kappa_{\varphi}(\ell_1))$ and that the strict inequality holds if and only if $v_{\ell_2}(s) = 0$, so, since $v_{\ell_2}(s) \neq 0$, $\text{ord}_v(v_{\ell_1}(\kappa_{\varphi}(\ell_2))) = \text{ord}_v(\kappa_{\varphi}(\ell_1))$. Combining this with the inequalities in formula (27) shows that

$$t = \text{ord}_v(\kappa_{\varphi}(\ell_1)) = \text{ord}_v(\kappa_{\varphi}(\ell_2)). \quad (28)$$

It follows that $\ell_2 \in \Pi$. If (ℓ_1, ℓ_2) is not a rigid pair, then $\text{Sel}_{\ell_2}(F, \text{ad}^0 \rho)$ is one dimensional (this is the case only if $\text{Sel}_{\ell_1}(F, \text{ad}^0 \rho) = 0$). In this case, by Proposition 7.13, choose an $(n + t_f)$ -admissible prime ℓ_3 such that $\partial_{\ell_3}(s) = 0$, $v_{\ell_3}(s) \neq 0$ and (ℓ_2, ℓ_3) is a rigid pair. Repeat the argument above with ℓ_2 replacing ℓ_1 and ℓ_3 replacing ℓ_2 to show that $\ell_3 \in \Pi$. In any case then, either (ℓ_1, ℓ_2) or (ℓ_2, ℓ_3) is a rigid pair and the claim at the beginning of follows.

7.6.5. The congruence argument. Choose by the result explained in Subsection 7.6.4 a rigid pair (ℓ_1, ℓ_2) with $\ell_1, \ell_2 \in \Pi$. Note that, by Theorem 7.23,

$$t = t_g = \text{ord}_v(\theta_g) \quad (29)$$

(here g is the congruent modular form attached to (ℓ_1, ℓ_2) by Proposition 7.21). There is an exact sequence of Λ -modules:

$$0 \longrightarrow \text{Sel}_{\ell_1 \ell_2}^f \longrightarrow \text{Sel}_{f, n}^{\vee} \longrightarrow \text{Sel}_{[\ell_1, \ell_2]}^{\vee} \longrightarrow 0, \quad (30)$$

where $\text{Sel}_{[\ell_1, \ell_2]} \subseteq \text{Sel}_{f, n}$ is defined by the condition that the restriction at the primes ℓ_1 and ℓ_2 must be trivial and $\text{Sel}_{\ell_1 \ell_2}^f$ is the kernel of the surjection of duals. There is an inclusion:

$$(\text{Sel}_{\ell_1 \ell_2}^f)^{\vee} \subseteq H_{\text{fin}}^1(K_{\wp^{\infty}, \ell_1}, A_{f, \pi^n}) \oplus H_{\text{fin}}^1(K_{\wp^{\infty}, \ell_2}, A_{f, \pi^n}).$$

The dual of $H_{\text{fin}}^1(K_{\wp^{\infty}, \ell_1}, A_{f, \pi^n}) \oplus H_{\text{fin}}^1(K_{\wp^{\infty}, \ell_2}, A_{f, \pi^n})$, by the non-degeneracy of the local Tate pairing, is $\hat{H}_{\text{sing}}^1(K_{\wp^{\infty}, \ell_1}, A_{f, \pi^n}) \oplus \hat{H}_{\text{sing}}^1(K_{\wp^{\infty}, \ell_2}, A_{f, \pi^n})$, so the above inclusion leads to a surjection:

$$\eta_f: \hat{H}_{\text{sing}}^1(K_{\wp^{\infty}, \ell_1}, A_{f, \pi^n}) \oplus \hat{H}_{\text{sing}}^1(K_{\wp^{\infty}, \ell_2}, A_{f, \pi^n}) \longrightarrow \text{Sel}_{\ell_1 \ell_2}^f.$$

Recall that, since ℓ_1 is n -admissible, $\widehat{H}_{\text{sing}}^1(K_{\wp^\infty, \ell_1}, A_{f, \pi^n}) \simeq \Lambda_{\wp, \pi}/\pi^n$. Let η_f^φ be the map induced by η_f after tensoring by \mathcal{O} via φ . Then the domain of η_f^φ is isomorphic to $(\mathcal{O}/\varphi(\pi^n))^2$. By Property 5 above enjoyed by the classes $\kappa'_\varphi(\ell_1)$ and $\kappa'_\varphi(\ell_2)$, the kernel of η_f^φ contains $(\partial_{\ell_1}\kappa'_\varphi(\ell_1), 0)$ and $(0, \partial_{\ell_2}\kappa'_\varphi(\ell_2))$. The same property combined with equations (28) and (29) yields

$$t_f - t_g = \text{ord}_v(\partial_{\ell_1}(\kappa'_\varphi(\ell_1))) = \text{ord}_v(\partial_{\ell_2}(\kappa'_\varphi(\ell_2))).$$

It follows that

$$v^{2(t_f - t_g)} \text{ belongs to the Fitting ideal of } \text{Sel}_{\ell_1 \ell_2}^f \otimes_\varphi \mathcal{O}. \quad (31)$$

Repeat now the argument with the modular form g : there is an exact sequence

$$0 \longrightarrow \text{Sel}_{\ell_1 \ell_2}^g \longrightarrow \text{Sel}_{g, n}^\vee \longrightarrow \text{Sel}_{[\ell_1, \ell_2]}^\vee \longrightarrow 0,$$

and a surjection

$$\eta_g : \widehat{H}_{\text{fin}}^1(K_{\wp^\infty, \ell_1}, A_{f, \pi^n}) \oplus \widehat{H}_{\text{fin}}^1(K_{\wp^\infty, \ell_1}, A_{f, \pi^n}) \longrightarrow \text{Sel}_{\ell_1 \ell_2}^g.$$

Let η_g^φ be the map induced by η_g after tensoring by \mathcal{O} via φ . By the global reciprocity law of class field theory, the kernel of η_g^φ contains the elements

$$\begin{aligned} (v_{\ell_1}(\kappa'_\varphi(\ell_1)), v_{\ell_2}(\kappa'_\varphi(\ell_1))) &= (v_{\ell_1}(\kappa'_\varphi(\ell_1)), 0), \\ (v_{\ell_1}(\kappa'_\varphi(\ell_2)), v_{\ell_2}(\kappa'_\varphi(\ell_2))) &= (0, v_{\ell_2}(\kappa'_\varphi(\ell_2))), \end{aligned}$$

where the equalities follow from Property 3 above enjoyed by the classes $\kappa'_\varphi(\ell_1)$ and $\kappa'_\varphi(\ell_2)$. Note that $\text{ord}_v(v_{\ell_2}\kappa'_\varphi(\ell_1)) = \text{ord}_v(v_{\ell_1}\kappa'_\varphi(\ell_2)) = t_g - t = 0$. From this it follows that the module $\text{Sel}_{\ell_1 \ell_2}^g$ is trivial. As a consequence, there is an isomorphism

$$\text{Sel}_{g, n}^\vee \otimes_\varphi \mathcal{O} \xrightarrow{\sim} \text{Sel}_{[\ell_1, \ell_2]}^\vee \otimes_\varphi \mathcal{O}. \quad (32)$$

7.6.6. The inductive argument. Now assume that the theorem is true for all $t' < t_f$ and prove that it is true for t_f . Recall that $t = t_g < t_f$. Since (ℓ_1, ℓ_2) is a rigid pair, the modular form g satisfies the assumptions in the theorem, so, by the inductive hypothesis,

$$\varphi(\theta_g) \text{ belongs to the Fitting ideal of } \text{Sel}_{g, n}^\vee \otimes_\varphi \mathcal{O}. \quad (33)$$

Now use the theory of Fitting ideals:

$$\begin{aligned} v^{2t_f} &= v^{2(t_f - t_g)} v^{2t_g} \\ &\in \text{Fitt}_\mathcal{O}(\text{Sel}_{\ell_1 \ell_2}^f \otimes_\varphi \mathcal{O}) \cdot \text{Fitt}_\mathcal{O}(\text{Sel}_{g, n}^\vee \otimes_\varphi \mathcal{O}) \quad \text{by (31) and (33)} \\ &= \text{Fitt}_\mathcal{O}(\text{Sel}_{\ell_1 \ell_2}^f \otimes_\varphi \mathcal{O}) \cdot \text{Fitt}_\mathcal{O}(\text{Sel}_{[\ell_1, \ell_2]}^\vee \otimes_\varphi \mathcal{O}) \quad \text{by (32)} \\ &\subseteq \text{Fitt}_\mathcal{O}(\text{Sel}_{f, n}^\vee \otimes_\varphi \mathcal{O}) \quad \text{by (30)}. \end{aligned}$$

Since by definition $\text{ord}(\theta_f) = t_f$, it follows that $\varphi(\theta_f)^2 \in \text{Fitt}_\mathcal{O}(\text{Sel}_{f, n}^\vee \otimes_\varphi \mathcal{O})$, thus proving (23) and therefore Theorem 6.1.

References

- [1] M. Bertolini, Selmer group and Heegner points in anticyclotomic \mathbb{Z}_p -extensions. *Compositio Math.* **99** (1995), no. 2, 153–182. Zbl 0862.11043 MR 1351834
- [2] M. Bertolini and H. Darmon, Derived heights and generalized Mazur-Tate regulators. *Duke Math. J.* **76** (1994), no. 1, 75–111. Zbl 0853.14013 MR 1301187
- [3] M. Bertolini and H. Darmon, Heegner points on Mumford-Tate curves. *Invent. Math.* **126** (1996), no. 3, 413–456. Zbl 0882.11034 MR 1419003
- [4] M. Bertolini and H. Darmon, A rigid analytic Gross-Zagier formula and arithmetic applications. With an appendix by Bas Edixhoven. *Ann. of Math. (2)* **146** (1997), no. 1, 111–147. Zbl 1029.11027 MR 1469318
- [5] M. Bertolini and H. Darmon, Iwasawa's main conjecture for elliptic curves over anticyclotomic \mathbb{Z}_p -extensions. *Ann. of Math. (2)* **162** (2005), no. 1, 1–64. Zbl 1093.11037 MR 2178960
- [6] N. Bourbaki, *Éléments de mathématique*. Fasc. XXXI. Algèbre commutative, Chapitre 7. Diviseurs, Actualités Scientifiques et Industrielles, No. 1314 Hermann, Paris 1965. Zbl 0141.03501 MR 0260715
- [7] J. Coates and R. Greenberg, Kummer theory for abelian varieties over local fields. *Invent. Math.* **124** (1996), no. 1–3, 129–174. Zbl 0858.11032 MR 1369413
- [8] C. Cornut and V. Vatsal, Nontriviality of Rankin-Selberg L -functions and CM points. In *L-functions and Galois representations* (Durham, July 2004), London Math. Soc. Lecture Note Ser. 320, Cambridge University Press, Cambridge 2007. Zbl 1153.11025 MR 2392354
- [9] C. Cornut and V. Vatsal, CM points and quaternion algebras. *Doc. Math.* **10** (2005), 263–309. Zbl 1165.11321 MR 2148077
- [10] H. Darmon, F. Diamond, and R. Taylor, Fermat's last theorem. In *Current developments in mathematics*, 1995 (Cambridge, MA), International Press, Cambridge, MA, 1994, 1–154. Zbl 0877.11035 MR 1474977
- [11] P. Deligne and J. P. Serre, Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)* **7** (1974), 507–530 (1975). Zbl 0321.10026 MR 0379379
- [12] F. Diamond and R. Taylor, Nonoptimal levels of mod l modular representations. *Invent. Math.* **115** (1994), no. 3, 435–462. Zbl 0847.11025 MR 1262939
- [13] F. Diamond and R. Taylor, Lifting modular mod ℓ representations. *Duke Math. J.* **74** (1994), 253–269. Zbl 0809.11025 MR 1272977
- [14] M. Dimitrov, On Ihara's lemma for Hilbert modular varieties. *Compos. Math.* **145** (2009), no. 5, 1114–1146. Zbl 05625824 MR 2551991
- [15] K. Fujiwara, Deformation rings and Hecke algebras in the totally real case. Preprint, arXiv:math/0602606v2 [math.NT].
- [16] E. Goren, *Lectures on Hilbert modular varieties and modular forms*. CRM Monogr. Ser. 14, Amer. Math. Soc., Providence, RI, 2002. Zbl 0986.11037 MR 1863355
- [17] B. H. Gross, Heights and the special values of L -series. In *Number theory* (Montreal, Que., 1985), CMS Conf. Proc. 7, Amer. Math. Soc., Providence, RI, 1987, 115–187. Zbl 0623.10019 MR 0894322

- [18] B. H. Gross and J. A. Parson, On the local divisibility of Heegner points. In *Number theory, analysis and geometry in memory of Serge Lang*, Springer-Verlag, Berlin 2011, 215–242.
- [19] H. Hida, On p -adic Hecke algebras for GL_2 over totally real fields. *Ann. of Math. (2)* **128** (1988), no. 2, 295–384. Zbl 0658.10034 MR 0960949
- [20] H. Hida, On nearly ordinary Hecke algebras for $GL(2)$ over totally real fields. In *Algebraic number theory*, Adv. Stud. Pure Math. 17, Academic Press, Boston, MA, 1989, 139–169. Zbl 0742.11026 MR 1097614
- [21] B. Howard, Iwasawa theory of Heegner points on abelian varieties of GL_2 type. *Duke Math. J.* **124** (2004), no. 1, 1–45. Zbl 1068.11071 MR 2072210
- [22] Y. Ihara, Shimura curves over finite fields and their rational points. In *Applications of curves over finite fields* (Seattle, WA, 1997), Contemp. Math. 245, Amer. Math. Soc., Providence, RI, 1999, 15–23. Zbl 0984.11027 MR 1732224
- [23] K. Iwasawa, On the μ -invariants of Z_ℓ -extensions. In *Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki*, Kinokuniya, Tokyo 1973, 1–11. Zbl 0281.12005 MR 0357371
- [24] H. Jacquet and R. P. Langlands, Automorphic forms on $GL(2)$. Lecture Notes in Math. 114, Springer-Verlag, Berlin 1970. Zbl 0236.12010 MR 0401654
- [25] F. Jarvis, Level lowering for modular mod l representations over totally real fields. *Math. Ann.* **313** (1999), no. 1, 141–160. Zbl 0978.11020 MR 1666809
- [26] F. Jarvis, Mazur’s principle for totally real fields of odd degree, *Compositio Math.* **116** 1999, no. 1, 39–79. Zbl 1053.11043 MR 1669444
- [27] K. Kato, Iwasawa theory and generalizations. In *International Congress of Mathematicians*, Vol. I, Eur. Math. Soc., Zürich 2007, 335–357. Zbl 1183.11067 MR 2334196
- [28] S. Ling, Shimura subgroups of Jacobians of Shimura curves. *Proc. Amer. Math. Soc.* **118** (1993), no. 2, 385–390. Zbl 0795.14014 MR 1145947
- [29] M. Longo, On the Birch and Swinnerton-Dyer conjecture for modular elliptic curves over totally real fields. *Ann. Inst. Fourier (Grenoble)* **56** (2006), no. 3, 689–733. Zbl 1152.11028 MR 2244227
- [30] M. Longo, Euler systems obtained from congruences between Hilbert modular forms. *Rend. Semin. Mat. Univ. Padova* **118** (2007), 1–34. Zbl 05376044 MR 2378387
- [31] H. Matsumura, *Commutative ring theory*. Cambridge Stud. Adv. Math. 8, Cambridge University Press, Cambridge 1989. Zbl 0603.13001 MR 0879273
- [32] B. Mazur, Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* **18** (1972), 183–266. Zbl 0245.14015 MR 0444670
- [33] B. Mazur and A. Wiles, Class fields of abelian extensions of \mathbb{Q} . *Invent. Math.* **76** (1984), no. 2, 179–330. Zbl 0545.12005 MR 0742853
- [34] J. Milne, *Arithmetic duality theorems*. Perspect. Math. 1, Academic Press, Boston, MA, 1986. Zbl 0613.14019 MR 0881804
- [35] J. Nekovář, *Selmer complexes*. Astérisque No. 310, Soc. Math. France, Paris 2006. Zbl 1211.11120 MR 2333680
- [36] J. Nekovář, The Euler system method for CM points on Shimura curves, In *L-functions and Galois representations* (Durham, July 2004), London Math. Soc. Lecture Note Ser. 320, Cambridge University Press, Cambridge 2007. Zbl 1152.11023 MR 2392363

- [37] J. Nekovář, Growth of Selmer groups of Hilbert modular forms over ring class fields. *Ann. Sci. École Norm. Sup. (4)* **41** (2008), No. 6, 1003–1022. Zbl 05543878 MR 2504111
- [38] J. Nekovář, Level raising and Selmer groups for Hilbert modular forms of weight two. *Canad. J. Math.*, to appear; preprint <http://people.math.jussieu.fr/~nekovar/pu/level.pdf>.
- [39] R. Pollack and T. Weston, On μ -invariants of anticyclotomic p -adic L -functions of elliptic curves. *Compos. Math.* **147** (2011), no. 5, 1353–1381. Zbl 05961171 MR 2834724
- [40] A. Rajaei, On the levels of mod l Hilbert modular forms. *J. Reine Angew. Math.* **537** (2001), 33–65. Zbl 0982.11023 MR 1856257
- [41] R. Ramakrishna, Lifting Galois representations. *Invent. Math.* **138** (1999), no. 3, 537–562. Zbl 0968.11024 MR 1719819
- [42] P. Samuel, *Lectures on unique factorization domains*. Notes by M. Pavman Murthy, Tata Institute of Fundamental Research Lectures on Mathematics 30, Tata Institute of Fundamental Research, Bombay 1964. Zbl 0184.06601 MR 0214579
- [43] J.-P. Serre, *Trees*. Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation, Springer Monogr. Math., Springer-Verlag, Berlin 2003. Zbl 1013.20001 MR 1954121
- [44] G. Shimura, The special values of the zeta functions associated with Hilbert modular forms. *Duke Math. J.* **45** (1978), no. 3, 637–679. Zbl 0394.10015 MR 0507462
- [45] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*. Reprint of the 1971 original, Publ. Math. Soc. Japan 11, Kanô Memorial Lectures 1, Princeton University Press, Princeton, NJ, 1994. Zbl 0221.10029 MR 1291394
- [46] V. Vatsal, *Special value formulae for Rankin L -functions*. Math. Sci. Res. Inst. Publ. 49, Cambridge University Press, Cambridge 2004. Zbl 1077.11038 MR 2083212
- [47] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*. Lecture Notes in Math. 800, Springer-Verlag, Berlin 1980. Zbl 0422.12008 MR 0580949
- [48] S. Zhang, Heights of Heegner points on Shimura curves. *Ann. of Math. (2)* **153** (2001), no. 1, 27–147. Zbl 1036.11029 MR 1826411
- [49] S. Zhang, Gross-Zagier formula for GL_2 . *Asian J. Math.* **5** (2001), no. 2, 183–290. Zbl 1111.11030 MR 1868935
- [50] S. Zhang, Equidistribution of CM-points on quaternion Shimura varieties. *Internat. Math. Res. Notices* **2005** (2005), no. 59, 3657–3689. Zbl 1096.14016 MR 2200081

Received June 17, 2009

Matteo Longo, Dipartimento di Matematica Pura ed Applicata, Università di Padova, Via Trieste 63, 35121, Italy
E-mail: mlongo@math.unipd.it