# On the Brumer–Stark Conjecture

Samit Dasgupta
Mahesh Kakde

September 4, 2020

**Abstract**

Let $H/F$ be a finite abelian extension of number fields with $F$ totally real and $H$ a CM field. Let $S$ and $T$ be disjoint finite sets of places of $F$ satisfying the usual conditions. The Brumer–Stark conjecture states that the Stickelberger element $\Theta_{S,T}^{H/F}$ annihilates the $T$-smoothed class group $\mathrm{Cl}^T(H)$. We prove this conjecture away from $p = 2$, that is, after tensoring with $\mathbf{Z}[1/2]$. We prove a stronger version of this result conjectured by Kurihara that gives a formula for the minus part of the 0th Fitting ideal of the Pontryagin dual of $\mathrm{Cl}^T(H) \otimes \mathbf{Z}[1/2]$ in terms of Stickelberger elements. We also show that this stronger result implies Rubin's higher rank version of the Brumer–Stark conjecture, again away from 2.

Our technique is a generalization of Ribet's method, building upon on our earlier work on the Gross–Stark conjecture. Here we work with group ring valued Hilbert modular forms as introduced by Wiles. A key aspect of our approach is the construction of "higher congruences" between cusp forms and Eisenstein series, stronger than usually expected, arising as shadows of the trivial zeroes of $p$-adic $L$-functions. These higher congruences are essential to proving that the cohomology classes we construct are unramified at $p$.

# Contents

**1 Introduction** **3**
1.1 Main Result . . . . . 6
1.2 The Rubin–Stark Conjecture . . . . . 8
1.3 Summary of Proof . . . . . 9
1.4 Acknowledgements . . . . . 13

**2 Algebraic and Analytic Preliminaries** **14**
2.1 Analytic Class Number Formula . . . . . 14
2.2 Character group rings . . . . . 15
2.3 Fitting ideals . . . . . 16

**3 Main Results** **18**
3.1 The Selmer module of Burns–Kurihara–Sano . . . . . 18
3.2 Keystone Result . . . . . 20
3.3 Strong Brumer–Stark and Kurihara's Conjecture . . . . . 20
3.4 Rubin's Conjecture . . . . . 25

**4 On the smoothing and depletion sets** **27**
4.1 Removing primes above $p$ from the smoothing set . . . . . 27
4.2 Passing to the field cut out by $\chi$ . . . . . 28

**5 Divisibility Implies Equality** **30**
5.1 Base Case . . . . . 32
5.2 Strategy of Inductive Step . . . . . 33
5.3 Characters unramified at some place in $\Sigma_p$ . . . . . 34
5.4 Characters ramified at all places in $\Sigma_p$ . . . . . 34

**6 The module $\nabla$ and its key properties** **39**
6.1 Transpose . . . . . 40
6.2 Extension class via Galois cohomology . . . . . 41

**7 Group ring valued Hilbert Modular Forms** **43**
7.1 Replacing $R$ by its trivial zero free quotient . . . . . 43
7.2 Definitions and notations on Hilbert modular forms . . . . . 44
7.2.1 Hilbert modular forms . . . . . 44
7.2.2 Hecke Operators . . . . . 44
7.2.3 Cusps, $q$-expansions, and cusp forms . . . . . 45
7.2.4 $q$-expansions . . . . . 46
7.2.5 Cusps above infinity and zero . . . . . 46
7.2.6 Forms with Nebentypus . . . . . 46
7.2.7 Raising the level . . . . . 47
7.2.8 Group ring valued Hilbert modular forms . . . . . 47
7.2.9 Ordinary forms . . . . . 49
7.3 Eisenstein series . . . . . 49

**8 Construction of cusp forms** **50**
8.1 Construction of modified Eisenstein series . . . . . 50
8.2 Linear combinations cuspidal modulo high powers of $p$ . . . . . 53
8.2.1 Case 1: $\mathrm{cond}(H/F)$ not divisible by primes above $p$ . . . . . 54
8.2.2 Case 2: $\mathrm{cond}(H/F)$ is divisible by some primes above $p$ . . . . . 55
8.3 Group ring valued forms . . . . . 56
8.4 Applying the ordinary operator . . . . . 60

8.5 Homomorphism on the Hecke Algebra . . . . . 62

**9 Galois representation and cohomology class** **65**
9.1 Galois representation associated to each eigenform . . . . . 65
9.2 Galois representation associated to $\mathbf{T}_{\mathfrak{m}}$ . . . . . 67
9.3 Cohomology Class and Ramification away from $p$ . . . . . 69
9.4 Surjection from $\nabla$ . . . . . 70
9.5 Calculation of Fitting Ideal . . . . . 75

**A Appendix: Construction and Properties of $\nabla$** **77**
A.1 Construction of $\nabla$ . . . . . 78
A.2 Independence of $S'$ . . . . . 82
A.3 Projectivity of Presentation . . . . . 83
A.4 Transpose of $\nabla$ . . . . . 85
A.5 Extension class via Galois cohomology . . . . . 87

**B Appendix: Kurihara's Conjecture** **89**
B.1 Functorial properties . . . . . 89
B.2 Proof of Kurihara's Conjecture . . . . . 92

# 1 Introduction

Let $F$ be a totally real field of degree $n$ over $\mathbf{Q}$. Let $H$ be a finite abelian extension of $F$ that is a CM field. Write $G = \mathrm{Gal}(H/F)$. Associated to any character $\chi\colon G \longrightarrow \mathbf{C}^*$ one has the Artin $L$-function

$$L(\chi, s) = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})\mathrm{N}\mathfrak{p}^{-s}}, \qquad \mathrm{Re}(s) > 1,$$

where the product ranges over the maximal ideals $\mathfrak{p} \subset \mathcal{O}_F$. We adopt the convention that $\chi(\mathfrak{p}) = 0$ if $\chi$ is ramified at $\mathfrak{p}$. The Artin $L$-function $L(\chi, s)$ has a meromorphic continuation to $\mathbf{C}$ that is analytic if $\chi \neq 1$, and has only a single simple pole at $s = 1$ if $\chi = 1$.

Let $\Sigma, \Sigma'$ denote disjoint finite sets of places of $F$ with $\Sigma \supset S_\infty$, the set of infinite places of $F$. We do not impose any other conditions on $\Sigma, \Sigma'$.

The "$\Sigma$-depleted, $\Sigma'$-smoothed" $L$-function of $\chi$ is defined by

$$L_{\Sigma,\Sigma'}(\chi, s) = L(\chi, s) \prod_{\mathfrak{p} \in \Sigma \setminus S_\infty} (1 - \chi(\mathfrak{p})\mathrm{N}\mathfrak{p}^{-s}) \prod_{\mathfrak{p} \in \Sigma'} (1 - \chi(\mathfrak{p})\mathrm{N}\mathfrak{p}^{1-s}).$$

These $L$-functions can be packaged together into a Stickelberger element

$$\Theta^{H/F}_{\Sigma,\Sigma'}(s) \in \mathbf{C}[G]$$

defined by (we drop the superscript $H/F$ when unambiguous)

$$\chi(\Theta_{\Sigma,\Sigma'}(s)) = L_{\Sigma,\Sigma'}(\chi^{-1}, s) \qquad \text{for all } \chi \in \hat{G}.$$

A classical theorem of Siegel and Shintani implies that the specialization

$$\Theta_{\Sigma,\Sigma'} = \Theta_{\Sigma,\Sigma'}(0)$$

lies in $\mathbf{Q}[G]$. For an integral statement, we must impose conditions on the depletion and smoothing sets. Let $S, T$ denote disjoint finite sets of places of $F$ with $S \supset S_\infty \cup S_{\text{ram}}$, where $S_{\text{ram}}$ denotes the set of finite primes of $F$ ramified in $H$. We impose the following condition on $T$.

Let $T_H$ denote the set of primes of $H$ above those in $T$. The group of roots of unity $\zeta \in \mu(H)$ such that $\zeta \equiv 1 \pmod{\mathfrak{p}}$ for all $\mathfrak{p} \in T_H$ is trivial. (1)

If $T$ contains two primes of different residue characteristic, or one prime of residue characterstic larger than $[F : \mathbf{Q}] + 1$, then this condition automatically holds. A celebrated theorem of Deligne–Ribet [17] and Cassou-Noguès [9] states that

$$\Theta_{S,T} \in \mathbf{Z}[G]. \tag{2}$$

Let $\mathrm{Cl}^T(H)$ denote the ray class group of $H$ with conductor equal to the product of primes in $T_H$. This is defined as follows. Let $I_T(H)$ denote the group of fractional ideals of $H$ relatively prime to the primes in $T_H$. Let $P_T(H)$ denote the subgroup of $I_T(H)$ generated by principal ideals $(\alpha)$ where $\alpha \in \mathcal{O}_H$ satisfies $\alpha \equiv 1 \pmod{\mathfrak{p}}$ for all $\mathfrak{p} \in T_H$. Then

$$\mathrm{Cl}^T(H) = I_T(H)/P_T(H).$$

This $T$-smoothed class group is naturally a $\mathbf{Z}[G]$-module. The following conjecture stated by Tate ([49, Conjecture IV.6.2]) is often called the Brumer–Stark conjecture. Note that the actual conjecture stated by Tate is very slightly stronger—see the discussion following (5) below. This discrepancy disappears when 2 is inverted as it is in our results.

**Conjecture 1.1** ("The Brumer–Stark Conjecture")**.** *We have*

$$\Theta_{S,T} \in \mathrm{Ann}_{\mathbf{Z}[G]}(\mathrm{Cl}^T(H)). \tag{3}$$

A corollary of our main result is the prime-to-2 part of the Brumer–Stark conjecture.

**Theorem 1.2.** *We have*

$$\Theta_{S,T} \in \mathrm{Ann}_{\mathbf{Z}[G]}(\mathrm{Cl}^T(H)) \otimes \mathbf{Z}[\tfrac{1}{2}]. \tag{4}$$

Let us briefly describe the history of the Brumer–Stark conjecture as well as its significance. In 1890, Stickelberger proved (3) when $F = \mathbf{Q}$ by computing the ideal factorization of Gauss sums in cyclotomic fields [48]. In the late 1960s, Brumer defined and studied the Stickelberger element $\Theta_S = \Theta_{S,\emptyset}$ for arbitrary totally real fields $F$, generalizing Stickelberger's construction. Brumer conjectured that any element of $(\Theta_S \cdot \mathbf{Z}[G]) \cap \mathbf{Z}[G]$ annihilates $\mathrm{Cl}(H)/\overline{\mathrm{Cl}(F)}$, where $\overline{\mathrm{Cl}(F)}$ denotes the image of $\mathrm{Cl}(F)$ in $\mathrm{Cl}(H)$ under the natural map induced by extension of ideals. This conjecture was not published by Brumer, but was described in lectures and became well-known to researchers in the field [10]. Brumer's conjecture is explicitly stated for real quadratic $F$ in the 1970 Ph.D. thesis of Rideout [39, Theorem 1.15]. See also the paper of Coates–Sinnott, where Brumer's ideas are discussed [11, Pp. 254 and 256].

Throughout the 1970's Stark conducted a series of deep investigations into refinements of the analytic class number formula. His "rank one abelian conjecture," stated in [46], proposed the existence of units $u$ in abelian extensions $H/F$ whose absolute values at all conjugates of a given archimedean place $w$ are described explicitly in terms of the first derivatives at 0 of the $L$-functions of the extension $H/F$. In addition, Stark observed in the cases he studied the following interesting condition: if $e = \#\mu(H)$ denotes the number of roots of unity in $H$, then the extension $H(u^{1/e})/F$ is abelian. See Stark's pleasant exposition [47] for a description of the origin of his work on these conjectures, and in particular his discovery of this "abelian" condition (§4).

Tate realized that Brumer's conjecture and Stark's conjecture could be stated simultaneously in the same notational framework using an arbitrary place $v$ of $F$ that splits completely in $H$; when $v$ is finite one recovers Brumer's conjecture, and when $v$ is infinite one recovers Stark's rank one abelian conjecture. Tate introduced the smoothing set $T$ and noted that Stark's abelian condition can be interpreted as the statement that $\Theta_{S,T}$ annihilates $\mathrm{Cl}^T(H)$, and not just the class group $\mathrm{Cl}(H)$. Because of the incorporation of Stark's abelian condition into the conjecture, he called the conjecture the Brumer–Stark conjecture [49, §4.6].

The Brumer–Stark conjecture can be related to Hilbert's 12th problem as follows. Let $\mathfrak{p} \notin S \cup T$ denote a prime of $F$ that splits completely in $H$. Pick a prime $\mathfrak{P}$ of $H$ above $F$ and write $\Theta_{S,T} = \sum_{\sigma \in G} \zeta_{S,T}(\sigma)[\sigma^{-1}]$. Conjecture 1.1 implies that the ideal

$$\mathfrak{P}^{\Theta_{S,T}} = \prod_{\sigma \in G} \sigma^{-1}(\mathfrak{P})^{\zeta_{S,T}(\sigma)} \tag{5}$$

is a principal ideal $(u)$ generated by an element $u \equiv 1 \pmod{\mathfrak{p}\mathcal{O}_H}$ for all $\mathfrak{p} \in T$. A very mild refinement of Conjecture 1.1, which was the actual statement proposed by Tate, is that the generator $u$ can be chosen to satisfy $\overline{u} = u^{-1}$, where $\overline{u}$ denotes the image of $u$ under the complex conjugation of $H$. (In any case the quotient $v = u/\overline{u}$ for any generator $u$ would satisfy $\overline{v} = v^{-1}$ and generate the ideal $\mathfrak{P}^{2\Theta_{S,T}}$, so this refinement only concerns a factor of 2.) The element $u$ satisfying these properties is unique and is called a Brumer–Stark unit. This is a canonical $\mathfrak{p}$-unit in $H$ with valuations at primes above $\mathfrak{p}$ determined by the $L$-functions

of the extension $H/F$:

$$\sum_{\sigma\in G}\chi(\sigma)\,\mathrm{ord}_{\sigma^{-1}(\mathfrak{P})}(u)=L_{S,T}(\chi,0)$$

for all $\chi\in\hat{G}$. The conjectural existence of the elements $u\in H$ suggests the possibility of an explicit class field theory for the ground field $F$. This perspective is explored further in our forthcoming work [15], where we prove an explicit $p$-adic analytic formula for Brumer–Stark units and give applications to Hilbert's 12th problem for $F$.

## 1.1 Main Result

Kurihara stated a refinement of the prime-to-2 part of Conjecture 1.1 known as the Strong Brumer–Stark conjecture. Let

$$\mathrm{Cl}^T(H)^\vee=\mathrm{Hom}_{\mathbf{Z}}(\mathrm{Cl}^T(H),\mathbf{Q}/\mathbf{Z})$$

denote the Pontryagin dual of $\mathrm{Cl}^T(H)$ endowed with the contragradient $G$-action:

$$\sigma(f)(c)=f(\sigma^{-1}c).$$

Let $x\mapsto x^{\#}$ denote the involution on $\mathbf{Z}[G]$ induced by $g\mapsto g^{-1}$ for $g\in G$. Finally, for a $\mathbf{Z}[\frac{1}{2}][G]$-module $M$, let

$$M^-=M/(\sigma+1)\cong\{m\in M\colon \sigma m=-m\},$$

where $\sigma\in G$ denotes the unique complex conjugation of $H$. If $M$ is only a $\mathbf{Z}[G]$-module, we let $M^-=(M\otimes_{\mathbf{Z}}\mathbf{Z}[\frac{1}{2}])^-$. In particular $\mathbf{Z}[G]^-=\mathbf{Z}[\frac{1}{2}][G]/(\sigma+1)$. The following is a corollary of our main result.

**Theorem 1.3** ("Strong Brumer–Stark", Conjecture of Kurihara)**.** *We have*

$$\Theta_{S,T}^{\#}\in\mathrm{Fitt}_{\mathbf{Z}[G]^-}(\mathrm{Cl}^T(H)^{\vee,-}).\tag{6}$$

Here Fitt denotes the 0th Fitting ideal. The Fitting ideal of $\mathrm{Cl}(H)$ and its smoothed version $\mathrm{Cl}^T(H)$ have been the subject of significant study for many years. Experts have noted that the inclusion $\Theta_{S,T}\in\mathrm{Fitt}_{\mathbf{Z}[G]^-}(\mathrm{Cl}^T(H)^-)$ holds in important special instances, but is *false* in general. This is studied in detail in [21], where it is suggested that the Fitting ideal of the *Pontryagin dual* of the class group is better behaved than the class group itself. See also [35] for a discussion of these issues.

Theorem 1.3 is seen to imply the prime-to-2 part of the Brumer–Stark conjecture (Theorem 1.2) by combining the following observations: (a) the Fitting ideal of a module is contained in its annihilator; (b) for a module $M$ with finitely many elements one has $\mathrm{Ann}(M^\vee)=\mathrm{Ann}(M)^{\#}$; (c) $\sigma$ acts as $-1$ on $\Theta_{S,T}$, so the element $\Theta_{S,T}$ annihilates a $\mathbf{Z}[\frac{1}{2}][G]$-module $M$ if and only if it annhilates $M^-$.

Our main result is the proof of even stronger refinement of the prime-to-2 part of the Brumer–Stark conjecture, which was also originally conjectured by Kurihara. This result gives an exact formula for

$$\mathrm{Fitt}_{\mathbf{Z}[G]^-}(\mathrm{Cl}^T(H)^{\vee,-})$$

in terms of Stickelberger elements, as follows. Let $S = S_{\mathrm{ram}} \cup S_\infty$. For $v \in S_{\mathrm{ram}}$, let $I_v \subset G_v \subset G$ denote the inertia and decomposition groups, respectively, associated to $v$. Let

$$e_v = \frac{1}{\#I_v}\mathrm{N}I_v = \frac{1}{\#I_v}\sum_{\sigma \in I_v} \sigma \in \mathbf{Q}[G]$$

denote the idempotent that represents projection onto the characters unramified at $v$. Let $\sigma_v \in G_v$ denote any representative of the Frobenius coset of $v$. The element $1 - \sigma_v e_v \in \mathbf{Q}[G]$ is independent of choice of representative. Following [19], we define the Sinnott–Kurihara ideal, *a priori* a fractional ideal of $\mathbf{Z}[G]$, by

$$\mathrm{SKu}^T(H/F) = (\Theta^{\#}_{S_\infty,T}) \prod_{v \in S_{\mathrm{ram}}} (\mathrm{N}I_v, 1 - \sigma_v e_v).$$

Kurihara showed using the Deligne–Ribet/Cassou-Nogués theorem that $\mathrm{SKu}^T(H/F) \subset \mathbf{Z}[G]$ (see Lemma 3.4 below). The following is our main result.

**Theorem 1.4** (Conjecture of Kurihara)**.** *We have*

$$\mathrm{Fitt}_{\mathbf{Z}[G]^-}(\mathrm{Cl}^T(H)^{\vee,-}) = \mathrm{SKu}^T(H/F)^-.$$

Theorem 1.4 implies Strong Brumer–Stark (Theorem 1.3), and hence the prime-to-2 part of Brumer–Stark (Theorem 1.2), since

$$\Theta^{\#}_{S,T} = \Theta^{\#}_{S_\infty,T} \prod_{v \in S_{\mathrm{ram}}} (1 - \sigma_v e_v) \in \mathrm{SKu}^T(H/F). \tag{7}$$

Greither proved a version of Theorem 1.4 under the assumption of the Equivariant Tamagawa Number Conjecture [19].

The partial progress that had previously been obtained toward the Brumer–Stark conjecture applied the Iwasawa Main Conjecture for totally real fields proven by Wiles [53]. Greither proved some special cases of the Brumer–Stark conjecture [20] using the techniques of horizontal Iwasawa theory introduced by Wiles [54] under the assumption that the Iwasawa $\mu$-invariant $\mu_p(F)$ vanishes for each odd prime $p$. Greither and Popescu [22] proved the $p$-part of Theorem 1.3 for odd primes $p$ assuming that $\mu_p(F) = 0$ and that $S$ contains all the primes above $p$. Burns, Kurihara, and Sano refined the Greither–Popescu result [6]. Recently, Burns proved the $p$-part of Theorem 1.3 assuming that $\mu_p(F) = 0$ and that the Gross–Kuzmin Conjecture holds for $(H, p)$ (i.e. the non-vanishing of Gross's $p$-adic regulator) [4].

## 1.2 The Rubin–Stark Conjecture

Theorem 1.4 has as an important corollary the prime-to-2 part of Rubin's higher rank generalization of the Brumer–Stark conjecture. Let us recall Rubin's conjecture, stated originally in the beautiful paper [41]. We define $H_T^*$ to be the set of elements $h \in H^*$ such that $\mathrm{ord}_w(h-1) > 0$ for all $w \in T_H$.

Next we choose $r$ finite primes $S = \{v_1, \ldots, v_r\}$ of $F$ that split completely in $H$. Define

$$U_{S,T} = \{u \in H_T^* : |u|_w = 1 \text{ for all finite primes } w \notin S_H\} \tag{8}$$

and write $\mathbf{Q}U_{S,T} = U_{S,T} \otimes_{\mathbf{Z}} \mathbf{Q}$. Choose a prime $w_j$ of $H$ above each $v_j$. The map

$$\mathrm{ord}_G \colon \textstyle\bigwedge_{\mathbf{Q}[G]}^r \mathbf{Q}U_{S,T}^- \longrightarrow \mathbf{Q}[G]^- \tag{9}$$

induced by

$$\mathrm{ord}_G(u_1 \wedge \cdots \wedge u_r) = \det\left(\sum_{\sigma \in G} [\sigma^{-1}] \,\mathrm{ord}_{w_j}(\sigma(u_i))\right)_{i,j=1,\ldots,r} \tag{10}$$

is a $\mathbf{Q}[G]$-module isomorphism.

Define the Rubin–Brumer–Stark element

$$u_{\mathrm{RBS}} \in \textstyle\bigwedge_{\mathbf{Q}[G]}^r \mathbf{Q}U_{S,T}^- \subset \bigwedge_{\mathbf{Q}[G]}^r \mathbf{Q}U_{S,T}$$

by

$$\mathrm{ord}_G(u_{\mathrm{RBS}}) = \Theta_{S,T}.$$

Rubin conjectured that $u_{\mathrm{RBS}}$ lies in a certain $\mathbf{Z}[G]$-lattice that is nowadays called "Rubin's lattice," whose definition we now recall. For $i = 1, \ldots, r$, consider $\mathbf{Z}[G]$-module homomorphisms $\varphi_i : U_{S,T} \longrightarrow \mathbf{Z}[G]$. Let

$$\varphi \colon \textstyle\bigwedge_{\mathbf{Q}[G]}^r \mathbf{Q}U_{S,T} \longrightarrow \mathbf{Q}[G]$$

be the map induced by

$$\varphi(u_1 \wedge \cdots \wedge u_r) = \det(\varphi_i(u_j)).$$

The *rth exterior power bidual* of $U_{S,T}$, denoted $\bigcap_{\mathbf{Z}[G]}^r U_{S,T}$, is the set of $u \in \bigwedge_{\mathbf{Q}[G]}^r \mathbf{Q}U_{S,T}$ such that $\varphi(u) \in \mathbf{Z}[G]$ for all $r$-tuples $(\varphi_1, \ldots, \varphi_r)$. Rubin's lattice is defined by

$$\mathscr{L} = \left(\textstyle\bigwedge_{\mathbf{Q}[G]}^r \mathbf{Q}U_{S,T}^-\right) \cap \bigcap_{\mathbf{Z}[G]}^r U_{S,T}.$$

The exterior power bidual terminology was introduced by Burns and Sano [7], who studied and developed Rubin's construction in greater generality.

**Conjecture 1.5** (Rubin)**.** *We have* $u_{\mathrm{RBS}} \in \mathscr{L}$.

Note that $u_{\mathrm{RBS}}$ depends on the choice of the $w_j$ only up to multiplication by an element of $G$, and the validity of Conjecture 1.5 is independent of this choice. The Brumer–Stark conjecture is easily seen to be equivalent to the rank $r = 1$ case of Rubin's conjecture. In §3.4 we show that Theorem 1.3 implies the prime-to-2 part of Rubin's Conjecture:

**Theorem 1.6.** *We have* $u_{RBS} \in \mathscr{L} \otimes_{\mathbf{Z}} \mathbf{Z}[\frac{1}{2}]$.

## 1.3 Summary of Proof

We now sketch the proof of Theorem 1.4. For simplicity we consider the case that $H/F$ is unramified at all finite primes (i.e. has conductor 1). In this case the $\mathbf{Z}[G]^-$-module $\mathrm{Cl}^T(H)^-$ has a quadratic presentation, meaning that it has a finite $\mathbf{Z}[G]^-$-module presentation with the same number of generators and relations (see §2.3). This implies that $\mathrm{Fitt}_{\mathbf{Z}[G]^-}(\mathrm{Cl}^T(H)^-)$ is principal. Suppose we can show that

$$\mathrm{Fitt}_{\mathbf{Z}[G]^-}(\mathrm{Cl}^T(H)^-) \subset (\Theta_{S_\infty,T}). \tag{11}$$

The analytic class number formula implies that

$$\#\,\mathrm{Cl}^T(H)^- \doteq \prod_{\psi \text{ odd}} \psi(\Theta_{S_\infty,T}), \tag{12}$$

where $\doteq$ denotes equality up to a power of 2. In particular, the product in (12) lies in $\mathbf{Z}$. An elementary argument shows that (12) implies that the inclusion (11) must be an equality (see §2.3 for a description of this argument). Theorem 1.4 follows from this since one can show that

$$\mathrm{Fitt}_{\mathbf{Z}[G]^-}(\mathrm{Cl}^T(H)^{\vee,-}) = \mathrm{Fitt}_{\mathbf{Z}[G]^-}(\mathrm{Cl}^T(H)^-)^{\#}$$

in this setting ($H/F$ unramified at finite places).

The inclusion (11) is proved using Ribet's method, which was originally invented by Ribet to prove the converse of Herbrand's Theorem in the seminal work [38]. Our application of Ribet's Method owes a great debt to the techniques introduced by Wiles in [53]. We reintroduce the theory of *group ring valued Hilbert modular forms*. These were considered by Wiles in [53], and this theory is developed further by Silliman in [45] and in this paper.

Since $H/F$ has conductor 1, class field theory canonically identifies $G$ as a quotient of the narrow class group $\mathrm{Cl}^+(F)$. Let

$$\boldsymbol{\psi}\colon\ \mathrm{Cl}^+(F) \twoheadrightarrow G \longrightarrow (\mathbf{Z}[G]^-)^*$$

denote the canonical character. For a positive integer $k$, let $M_k$ denote the usual group of Hilbert modular forms for $F$ of level 1 with Fourier coefficients lying in $\mathbf{Z}$. For $k$ odd, define $M_k(\boldsymbol{\psi})$ to be the $\mathbf{Z}[G]^-$-submodule of $M_k \otimes \mathbf{Q}[G]^-$ consisting of those $f$ whose Fourier coefficients lie in $\mathbf{Z}[G]^-$ and such that for each odd character $\psi \in \hat{G}$, the specialization $\psi(f)$

is a classical form of nebentypus $\psi$. The form $f$ can be viewed as encoding the "family" of forms $\{\psi(f)\}$. The fact that $f$ has integral Fourier coefficients implies that the forms $\psi(f)$ in this family satisfy certain congruences.

One of the few examples of group ring valued forms that one can write down explicitly are the Eisenstein series $E_k$. Using these Eisenstein series along with an important auxiliary construction drawn from [45], we prove that for positive integers $k$ sufficiently large and close to 1 in $\hat{\mathbf{Z}}$, there is a *cuspidal* group ring valued form $f$ such that:

$$f \equiv E_k \pmod{\Theta_{S_\infty,T}}. \tag{13}$$

Let $\mathbf{T}$ denote the Hecke algebra over $\mathbf{Z}[G]^-$ of the module of weight $k$ cuspidal group ring valued forms. The congruence (13) implies that there is a surjective $\mathbf{Z}[G]^-$-algebra homomorphism

$$\varphi\colon \mathbf{T} \longrightarrow \mathbf{Z}[G]^-/(\Theta_{S_\infty,T}) \tag{14}$$

such that for all primes $\mathfrak{l} \subset \mathcal{O}_F$, we have

$$\varphi(T_\mathfrak{l}) = 1 + \boldsymbol{\psi}(\mathfrak{l}). \tag{15}$$

Let $I$ denote the kernel of $\varphi$ (the *Eisenstein ideal*).

Let $p$ denote an odd prime, and replace $\mathbf{T}$ and $I$ by their $p$-adic completions. The Galois representations associated to cusp forms together with the congruence (13) allow for the construction of a faithful $\mathbf{T}$-module $B$ along with a cohomology class

$$\kappa \in H^1(G_F, B/IB)$$

that is unramified at all primes not dividing $p$ or lying in $T$. Furthermore the image of $\kappa$ generates $B/IB$, and complex conjugation acts as $-1$ on this space. If $\kappa$ were unramified at all primes dividing $p$ as well, then $\kappa$ would cut out an extension of $H$ unramified outside the primes of $T$ and tamely ramified at those primes. By class field theory this yields a surjective homomorphism

$$\mathrm{Cl}^T(H)^- \twoheadrightarrow B/IB.$$

Since $\mathbf{T}/I \cong \mathbf{Z}_p[G]^-/(\Theta_{S_\infty,T})$ and $B$ is a faithful $\mathbf{T}$-module, general principles regarding Fitting ideals imply

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]^-}(\mathrm{Cl}^T(H)^-) \subset \mathrm{Fitt}_{\mathbf{Z}_p[G]^-}(B/IB) \subset (\Theta_{S_\infty,T}).$$

This yields the desired inclusion (11). Unfortunately, it is simply not true that $\kappa$ is necessarily unramified at the primes above $p$. Overcoming this obstacle is perhaps the central contribution to the theory of Ribet's method advanced by this paper. Previous works have employed the ingenious method of Wiles [54] to introduce auxiliary primes into the set $S$ and twist by characters with conductor divisible by these primes. However this

technique introduces certain error terms that destroy the delicate results that we need to obtain here and hence give only partial results (see [20]). Therefore, our new method deals with ramification at $p$ head-on. We first show that the congruence (13) and corresponding homomorphism (14) can be strengthened. There is a certain non-zerodivisor $x \in \mathbf{Z}_p[G]^-$ and a surjective $\mathbf{Z}_p[G]^-$-algebra homomorphism

$$\varphi_x \colon \mathbf{T} \longrightarrow \mathbf{Z}_p[G]^-/(x\Theta_{S_\infty,T}) \tag{16}$$

that is Eisenstein in the sense that (15) holds. The element $x$ can be viewed as encoding the mod $p$ trivial zeroes of the characters $\psi \in \hat{G}$ at the primes $\mathfrak{p} \mid p$, i.e. such that $\psi(\mathfrak{p}) \equiv 1$ modulo a prime above $p$ (in which case $L_{S_\infty \cup \{\mathfrak{p}\},T}(\psi, 0) \equiv 0$). It is striking that these trivial zeroes play a crucial role even while considering the primitive Stickelberger element $\Theta_{S_\infty,T}$.

Working as before, we let $I$ denote the kernel of $\varphi_x$ and construct a faithful $\mathbf{T}$-module $B$ together with a cohomology class

$$\kappa \in H^1(G_F, B/IB) \tag{17}$$

generating $B/IB$. The class $\kappa$ is unramified at all primes not dividing $p$ or lying in $T$. To produce a class unramified at primes above $p$, we rather bluntly consider the image of the inertia groups at all primes above $p$ under $\kappa$ and denote the $\mathbf{T}$-module that they generate in $B$ by $B(I_p)$. We define $\overline{B} = B/(IB, B(I_p))$ and note that the image of $\kappa$ in $H^1(G_F, \overline{B})$ is now tautologically unramifed at the primes above $p$. Hence we deduce a surjective homomorphism $\mathrm{Cl}^T(H)^- \twoheadrightarrow \overline{B}$ which yields

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]^-}(\mathrm{Cl}^T(H)^-) \subset \mathrm{Fitt}_{\mathbf{Z}_p[G]^-}(\overline{B}). \tag{18}$$

The Galois representations used in the construction of $\kappa$ are *ordinary* at all primes dividing $p$. Theorems of Hida and Wiles precisely describe the shape of ordinary representations when restricted to the decomposition groups at these primes. Using this we are able to relate the module $B(I_p)$ to the element $x \in \mathbf{Z}_p[G]^-$ and prove:

$$(x)\,\mathrm{Fitt}_{\mathbf{Z}_p[G]^-}(\overline{B}) \subset \mathrm{Fitt}_{\mathbf{Z}_p[G]^-}(B/IB) \subset (x\Theta_{S_\infty,T}). \tag{19}$$

Since $x$ is a non-zerodivisor, it can be canceled from the left and right sides of this inclusion; combining with (18), we obtain the desired result

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]^-}(\mathrm{Cl}^T(H)^-) \subset (\Theta_{S_\infty,T}).$$

Our calculation of Fitting ideals leading to the first inclusion in (19) is new (see Theorem 9.10), as is the idea to produce "extra congruences" yielding the second inclusion; we expect this technique to have further applications toward Bloch–Kato type results proved using Ribet's method.

This concludes our summary of the proof of Theorem 1.4 in the case that $H/F$ is unramified at all finite primes. It is worth reflecting that the inclusion (11) deduced from Ribet's method is the *reverse* of that required by the Strong Brumer–Stark conjecture. Combining this inclusion with the analytic argument of (12) enables us to deduce that the inclusion is an equality, and hence to conclude that the desired inclusion holds. In the general case of conductor greater than 1, this equality does not hold and hence both sides must be replaced by generalizations.

The paper is organized as follows. In §2, we present some analytic and algebraic preliminaries, including some results on Fitting ideals. In §3 we recall the $\mathbf{Z}[G]$-module $\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)$ of Burns, Kurihara, and Sano that plays the role of $\mathrm{Cl}^T(H)^\vee$ in the discussion above in the more general context when there exist ramified primes for $H/F$. Here $\Sigma$ and $\Sigma'$ denote arbitrary finite disjoint sets of places of $F$ such that $\Sigma \supset S_\infty$. In order to prove the $p$-part of Theorem 1.4 for an odd prime $p$ (that is, after tensoring with $\mathbf{Z}_p$), we choose the sets

$$\Sigma = S_\infty \cup \{v \in S_{\mathrm{ram}}, v \mid p\}, \qquad \Sigma' = T \cup \{v \in S_{\mathrm{ram}}, v \nmid p\}. \tag{20}$$

The keystone result proven over the course of the paper using group ring valued Hilbert modular forms over $\mathbf{Z}_p[G]$, from which all our previously stated theorems are deduced, is the following.

**Theorem 1.7.** *The $\mathbf{Z}_p[G]^-$-module $\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)_p^- = (\mathrm{Sel}_{\Sigma}^{\Sigma'}(H) \otimes_{\mathbf{Z}} \mathbf{Z}_p)^-$ is quadratically presented and we have*

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]^-}(\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)_p^-) = (\Theta_{\Sigma,\Sigma'}^{\#}). \tag{21}$$

The module $\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)_p$ plays an important role in our argument since $\mathrm{Cl}^T(H)_p^\vee$ is in general not quadratically presented. Also in §3, we deduce a partial result towards Kurihara's conjecture for the Fitting ideal of $\mathrm{Cl}^T(H)^{\vee,-}$, namely, we compute $\mathrm{Fitt}_{\mathbf{Z}_p[G]^-} \mathrm{Sel}_{\Sigma}^{T}(H)_p^-$ assuming Theorem 1.7. We show that this partial result is strong enough to imply Strong Brumer–Stark (Theorem 1.3). The key point here is that $\mathrm{Cl}^T(H)^{\vee,-}$ is a quotient of $\mathrm{Sel}_{\Sigma}^{T}(H)_p^-$. We conclude §3 by deducing the prime-to-2 part of Rubin's conjecture, i.e. Theorem 1.6.

In §4 we make some technical modifications of the smoothing and depletion sets $\Sigma, \Sigma'$ that assist in later arguments. In §5 we prove an analogue of the discussion surrounding (11)–(12) above to show that an inclusion in (21) for all $H/F$ implies an equality—see Theorem 5.1 for a precise statement. This result is significantly more complicated than the situation in (12) and requires a delicate induction.

In §6 we describe a $\mathbf{Z}[G]$-module $\nabla_{\Sigma}^{\Sigma'}(H)$ that was essentially defined previously by Ritter and Weiss [40]. Our contribution is the introduction of the smoothing set $\Sigma'$. In §6 we state the salient properties of $\nabla_{\Sigma}^{\Sigma'}(H)$. The actual construction of $\nabla_{\Sigma}^{\Sigma'}(H)$ and the proof of these properties is postponed to Appendix A. Under the appropriate assumptions, the $\mathbf{Z}[G]$-module $\nabla_{\Sigma}^{\Sigma'}(H)$ is locally quadratically presented and is a transpose of the module $\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)$ in the sense of Jannsen [24]. We remark that smoothing at $\Sigma'$ is essential toward deducing the

quadratic presentation property. It is likely that $\nabla_{\Sigma}^{\Sigma'}(H)$ is isomorphic to the canonical transpose $\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)^{\mathrm{tr}}$ defined by Burns–Kurihara–Sano in [5], though we have not tried to prove this.

Burns–Kurihara–Sano study their Selmer group and its transpose in detail under the assumption $\Sigma \supset S_{\mathrm{ram}}$. For us, it is essential to relax this assumption as in (20). We also give an interpretation of the minus part $\nabla_{\Sigma}^{\Sigma'}(H)^{-}$ in terms of Galois cohomology (Lemma 6.4) that does not appear explicitly in prior works. However the essential content of this lemma (indeed, our proof of it) can be gleaned from the calculations of Ritter–Weiss.

The remainder of the paper, which uses Ribet's method applied to group ring valued Hilbert modular forms, proves the inclusion that is the supposition of Theorem 5.1. In §7 we set our notations for classical Hilbert modular forms. In §7–8 we define group ring valued Hilbert modular forms and construct a cusp form congruent to an Eisenstein series in this context. We use this construction to define a homomorphism on the Hecke algebra generalizing (16). Our construction of a cusp form is a strong refinement of Wiles' construction of cusp forms in [53] in two ways: (i) we work over a group ring rather than character by character, and more importantly (ii) we construct "extra congruences" beyond those predicted by the Stickelberger element using trivial zeroes as discussed in (16) above. One key difference that allows us to produce these congruences is that we calculate the constant terms of relevant Eisenstein series at all cusps, rather than focusing exclusively on the cusps above $\infty$. These calculations are contained in [14]. Furthermore, we apply important results of Silliman that show the existence of group ring valued modular forms with certain prescribed constant terms [45].

We conclude in §9 by exploiting the Galois representations associated to Hilbert modular cusp forms in order to construct the cohomology class $\kappa$ of (17), and using this construction to deduce the desired inclusion of Fitting ideals. Our new calculation of the Fitting ideal in Theorem 9.10 should have future applications; it is inspired by the calculation of Gross's regulator in our previous work [16, §5].

As mentioned above, Appendix A contains the construction the Ritter–Weiss modules $\nabla_{\Sigma}^{\Sigma'}(H)$ and proofs of their key properties. Appendix B contains the proof of Kurihara's Conjecture (Theorem 1.7), bootstrapping from the partial result proved in §3 and mentioned above (i.e. the computation of $\mathrm{Fitt}_{\mathbf{Z}_p[G]^-}\mathrm{Sel}_{\Sigma}^{T}(H)_p^-$). This proof is included in an appendix because it requires the full details of the construction of $\nabla_{\Sigma}^{\Sigma'}(H)$, and not just the properties listed in §6.

## 1.4 Acknowledgements

It is a pleasure to recognize the significant influence of the works of David Burns, Cornelius Greither, Cristian Popescu, Masato Kurihara, Jürgen Ritter, Kenneth Ribet, Takamichi Sano, Alfred Weiss, and Andrew Wiles on this project. We would also like to thank David Burns, Henri Darmon, Masato Kurihara, Cristian Popescu, Takamichi Sano, Andreas Nickel,

Jesse Silliman, and Jiuya Wang for very helpful discussions. In particular we are indebted to Sano for introducing us to the paper [40] of Ritter–Weiss.

The first named author was supported by NSF grants DMS-1600943 and DMS-1901939 during the execution of this project.

# 2 Algebraic and Analytic Preliminaries

Throughout this paper we work with a totally real field $F$ and a finite abelian CM extension $H$. We let $G = \mathrm{Gal}(H/F)$. In this section we record some basic algebraic and analytic facts that will be used in the sequel.

## 2.1 Analytic Class Number Formula

Let $H^+$ denote the maximal totally real subfield of the CM field $H$, and let $\epsilon$ denote the nontrivial character of $\mathrm{Gal}(H/H^+)$.

**Lemma 2.1.** *We have $L_{S_\infty,T}(H/H^+,\epsilon,0) \in \mathbf{Z}$ and*

$$\#\,\mathrm{Cl}^T(H)^- \doteq L_{S_\infty,T}(H/H^+,\epsilon,0) \tag{22}$$

$$= \prod_{\psi\in\hat{G}\ odd} L_{S_\infty,T}(H/F,\psi,0). \tag{23}$$

*where $\doteq$ denotes equality up to a power of 2.*

*Proof.* This result is well-known, but we have not found a precise reference for it; the results (22)–(23) are proven in [33, Proposition 2] without the $T$-smoothing.

Since $\epsilon$ is $\pm1$-valued, $L_{S_\infty,T}(H/H^+,\epsilon,0)$ is rational by Klingen [26] or Siegel [44]. It is actually an integer by Cassou-Noguès [9] or Deligne–Ribet [17], because of our assumption on the set $T$ made in the introduction.

To prove (22), we note

$$L_{S_\infty,T}(H/H^+,\epsilon,0) = \frac{\zeta^*_{H,S_\infty,T}(0)}{\zeta^*_{H^+,S_\infty,T}(0)} \tag{24}$$

$$= \frac{\#\,\mathrm{Cl}^T(H)R_T(H)}{\#\,\mathrm{Cl}^T(H^+)R_T(H^+)} \tag{25}$$

$$\doteq \#\,\mathrm{Cl}^T(H)^-. \tag{26}$$

In (24), $\zeta^*_{H,S_\infty,T}(0)$ denotes the leading term of the zeta function at $s=0$ (both this zeta function and $\zeta_{H^+,S_\infty,T}$ have order

$$\mathrm{rank}(\mathcal{O}_H^*) = \mathrm{rank}(\mathcal{O}_{H^+}^*) = [H^+:\mathbf{Q}] - 1$$

at $s = 0$). Equation (25) is simply the $T$-smoothed Dedekind class number formula expressed at $s = 0$; see for instance [36, (16)]. The "up to 2-power" equality (26) follows from the following:

- $\mathrm{Cl}^T(H) \otimes \mathbf{Z}[\frac{1}{2}] \cong (\mathrm{Cl}^T(H^+) \otimes \mathbf{Z}[\frac{1}{2}]) \oplus \mathrm{Cl}^T(H)^-$.
- $R_T(H) = 2^{[H^+:\mathbf{Q}]-1} R_T(H^+)$ since $\mathcal{O}^*_{H,S_\infty,T} = \mathcal{O}^*_{H^+,S_\infty,T}$ by property (1).

Finally (23) follows from (22) by the Artin formalism for $L$-functions, as

$$\mathrm{Ind}_{G_{H^+}}^{G_F} \epsilon = \bigoplus_{\psi \in \hat{G}\,\mathrm{odd}} \psi.$$

□

## 2.2 Character group rings

We fix an odd prime $p$ and a finite extension $\mathcal{O}$ of $\mathbf{Z}_p$ that contains all the values of all characters $G \longrightarrow \overline{\mathbf{Q}}_p^*$. There is an $\mathcal{O}$-algebra embedding

$$\mathcal{O}[G] \hookrightarrow \prod_{\psi \in \hat{G}} \mathcal{O}_\psi, \qquad x \mapsto (\psi(x))_{\psi \in \hat{G}}.$$

Here $\mathcal{O}_\psi$ denotes the ring $\mathcal{O}$ endowed with the $G$-action in which $g \in G$ acts by multiplication by $\psi(g)$. More generally, given any subset of characters $\Psi \subset \hat{G}$, we define $R_\Psi$ to be the image of

$$\mathcal{O}[G] \longrightarrow \prod_{\psi \in \Psi} \mathcal{O}_\psi, \qquad x \mapsto (\psi(x))_{\psi \in \Psi}.$$

The quotients $R_\Psi$ of $\mathcal{O}[G]$ defined in this way will be referred to as *character-group rings*. Each $R_\Psi$ is a finite index subring of a finite product of DVRs.

Write $G = G_p \times G'$, where $G_p$ is the $p$-Sylow subgroup of $G$, and $G'$ is the subgroup of elements with prime-to-$p$ order. The ring $\mathcal{O}[G]$ decomposes as a product of local rings $R_\chi = \mathcal{O}[G_p]_\chi$ indexed by the characters $\chi \in \hat{G'}$. Here $\mathcal{O}[G_p]_\chi$ denotes the $\mathcal{O}$-algebra $\mathcal{O}[G_p]$ endowed with the $G$-action in which $g \in G$ acts by $\chi(g)\overline{g}$, where $\overline{g}$ denotes the image of $g$ under the canonical projection $G \longrightarrow G_p$. Each connected component $R_\chi$ of $\mathcal{O}[G]$ is an example of a character-group ring, with associated set $\Psi = \{\psi \colon \psi|_{G'} = \chi\}$. The characters $\psi \in \Psi$ are said to *belong to* $\chi$.

**Lemma 2.2.** *Let $I \subset G$ be a subgroup. The quotient $\mathcal{O}[G]/\mathrm{N}I$ is a character-group ring. More precisely, $\mathcal{O}[G]/\mathrm{N}I \cong R_\Psi$ where $\Psi = \{\psi \in \hat{G} \colon \psi(I) \neq 1\}$.*

*Proof.* Consider the canonical surjective $\mathcal{O}$-algebra homomorphism

$$\alpha \colon \mathcal{O}[G] \twoheadrightarrow R_\Psi.$$

It is clear that $\mathrm{N}I$ lies in the kernel of $\alpha$, since $\psi(\mathrm{N}I) = 0$ if $\psi(I) \neq 1$. Conversely if $x \in \ker \alpha$, then for all $g \in I$ we see that $\psi(gx) = \psi(x)$ for all $\psi \in \hat{G}$. This is clear if $\psi(g) = 1$, and follows from $x \in \ker \alpha$ if $\psi(g) \neq 1$. Hence $gx = x$ for all $g \in I$, which implies that $x \in (\mathrm{N}I)$. □

**Corollary 2.3.** *Let $\chi \in \hat{G}'$ and let $I \subset G_p$. Then $R_\chi/\mathrm{N}I \cong R_\Psi$, where*

$$\Psi = \{\psi \in \hat{G} \colon \psi|_{G'} = \chi, \psi(I) \neq 1\}.$$

*In particular, $R_\chi/\mathrm{N}I$ can be expressed as a finite index subring of a product of DVRs.*

## 2.3 Fitting ideals

In this section we collect some results—presumably well-known—about Fitting ideals. Let $R$ be a commutative ring. An $R$-module $M$ is called *quadratically presented* over $R$ if there exists a positive integer $m$ and an exact sequence

$$R^m \xrightarrow{\varphi} R^m \longrightarrow N \longrightarrow 0.$$

In this case, $\mathrm{Fitt}_R(N)$ is principal and generated by the determinant of the map $\varphi$.

**Lemma 2.4.** *Let $B$ be a finite index subring of a finite product of PIDs (such as any character-group ring $R_\Psi$ associated to a subset $\Psi \subset \hat{G}$). Let $N$ be a quadratically presented $B$-module such that $\mathrm{Fitt}_B(N) = (x)$ for some non-zerodivisor $x \in B$. Suppose that $B/(x)$ is finite. Then $N$ is finite and*

$$\#N = \#B/(x).$$

*Proof.* Let $A$ be an $m \times m$ matrix representing the relations among the generators of $N$, so $N \cong B^m/A \cdot B^m$ and $\mathrm{Fitt}_B(N) = (\det(A))$. We must show $\#(B^m/A \cdot B^m) = \#B/\det(A)$. This result is well-known for PIDs (e.g. via Smith Normal Form). We can deduce the result for $B$ using the fact that $B$ is a finite index subring of a product of PIDs.

Indeed, it is clear that if the result holds for two rings $B, B'$, then it holds for $B \times B'$, since both sides of the desired equality factor as a product over the corresponding terms for $B$ and $B'$.

Furthermore, if the result holds for a ring $B'$, then it holds for a finite index subring $B \subset B'$ as we now show. We see that

$$\frac{\#B'/\det(A)B'}{\#B/\det(A)B} = \frac{\#B'/B}{\#\det(A)B'/\#\det(A)B} = 1 \tag{27}$$

since multiplication by the non-zerodivisor $\det(A)$ is an isomorphism between the space in the numerator and in the denominator. Similarly, one sees that

$$\frac{\#(B')^m/A \cdot (B')^m}{\#B^m/A \cdot B^m} = \frac{\#(B')^m/B^m}{\#A \cdot (B')^m/A \cdot B^m} = 1 \tag{28}$$

since multiplication by $A$ induces an isomorphism between the space in the numerator and in the denominator. Only injectivity of this map is not obvious; for this, note that if $Av \in AB^m$ for some $v \in (B')^m$, then multiplying by the adjugate of $A$ we obtain $\det(A)v \in \det(A)B^m$, whence $v \in B^m$ since $\det(A)$ is a non-zerodivisor.

Equations (27) and (28) imply that the lemma holds for any finite index subring $B$ of a ring $B'$ for which it holds; this gives the result. □

**Lemma 2.5.** *Let $\Psi \subset \hat{G}$ and let $R_\Psi$ denote the associated character-group ring over $\mathcal{O}$. Let $x \in R_\Psi$ be a non-zerodivisor. Then $\#R_\Psi/(x) = \#\mathcal{O}/(\prod_{\psi\in\Psi} \psi(x))$.*

*Proof.* We proceed as in the proof of the previous lemma. There is an injection

$$R_\Psi \hookrightarrow \mathcal{O}_\Psi = \prod_{\psi\in\Psi} \mathcal{O}, \qquad y \mapsto (\psi(y))_{\psi\in\Psi}$$

with image of finite index. Then

$$\#(\mathcal{O}_\Psi/R_\Psi) = \#(x\mathcal{O}_\Psi/xR_\Psi)$$

since multiplication by $x$ is an isomorphism between the two quotients. It follows that

$$\#(R_\Psi/xR_\Psi) = \#(\mathcal{O}_\Psi/x\mathcal{O}_\Psi) = \prod_{\psi\in\Psi} \#(\mathcal{O}/\psi(x)),$$

where the last equality holds since $\mathcal{O}_\Psi$ is a product ring. The result follows. □

We can now describe the "elementary argument" mentioned in the introduction to show that (12) implies that the inclusion (11) is an equality. We work over $\mathcal{O}[G]^-$. In the case that $H/F$ is unramified at all finite primes, one can show that

$$\mathrm{Cl}^T(H)^-_{\mathcal{O}} := \mathrm{Cl}^T(H)^- \otimes \mathcal{O}$$

is quadratically presented as a module over $\mathcal{O}[G]^-$, so the inclusion (11) implies that

$$\mathrm{Fitt}_{\mathcal{O}[G]^-}(\mathrm{Cl}^T(H)^-_{\mathcal{O}}) = (x \cdot \Theta_{S_\infty,T})$$

for some $x \in \mathcal{O}[G]^-$. Hence by Lemmas 2.4 and 2.5, we have

$$\#\,\mathrm{Cl}^T(H)^-_{\mathcal{O}} = \#\mathcal{O}[G]^-/(x\Theta_{S_\infty,T}) = \#\mathcal{O}/\prod_{\psi \text{ odd}} \psi(x\Theta_{S_\infty,T}).$$

Therefore (12) implies that $\psi(x) \in \mathcal{O}^*$ for all $\psi$. This implies that $x \in (\mathcal{O}[G]^-)^*$, yielding the desired result.

We conclude with two more standard lemmas on Fitting ideals.

**Lemma 2.6.** *Let $R$ be a commutative ring, $C$ a quadratically presented $R$-module, and*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

*a short exact sequence of $R$-modules. Then*

$$\mathrm{Fitt}_R(B) = \mathrm{Fitt}_R(A)\,\mathrm{Fitt}_R(C).$$

See [25, Lemma 2.13] for a proof.

**Lemma 2.7.** *Let $R$ be a commutative ring, and $B, B'$ two quadratically presented $R$-modules fitting into exact sequences*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

$$0 \longrightarrow A' \longrightarrow B' \longrightarrow C \longrightarrow 0.$$

*of $R$-modules. Then*

$$\mathrm{Fitt}_R(A)\,\mathrm{Fitt}_R(B') = \mathrm{Fitt}_R(A')\,\mathrm{Fitt}_R(B).$$

*Proof.* Let $M$ denote the fiber product of $B$ and $B'$ with respect to $C$, i.e. the $R$-module of ordered pairs $(b, b')$ such that $b$ and $b'$ have the same image in $C$. Projection onto the first and second components yields two short exact sequences

$$0 \longrightarrow A' \longrightarrow M \longrightarrow B \longrightarrow 0,$$

$$0 \longrightarrow A \longrightarrow M \longrightarrow B' \longrightarrow 0.$$

Computing $\mathrm{Fitt}_R(M)$ in two ways using these exact sequences and Lemma 2.6 yields the desired result. □

# 3 Main Results

## 3.1 The Selmer module of Burns–Kurihara–Sano

We recall the definition of the Selmer module defined by Burns–Kurihara–Sano in [5] and studied further by Burns in [4]. This $G$-module will play a central role in this paper. For this, we fix finite disjoint sets of places $\Sigma, \Sigma'$ of $F$ such that $\Sigma \supset S_\infty$. Let $H^*_{\Sigma'}$ denote the subgroup of $x \in H^*$ such that $\mathrm{ord}_w(x-1) > 0$ for each prime $w \in \Sigma'_H$, where this latter set denotes the set of primes of $H$ lying above those in $\Sigma'$. Define

$$\mathrm{Sel}_\Sigma^{\Sigma'}(H) = \mathrm{Hom}_{\mathbf{Z}}(H^*_{\Sigma'}, \mathbf{Z}) / \prod_{w \notin \Sigma_H \cup \Sigma'_H} \mathbf{Z} \tag{29}$$

where the product ranges over the primes $w \notin \Sigma_H \cup \Sigma'_H$, and the implicit map sends a tuple $(x_w)$ to the function $\sum_w x_w \,\mathrm{ord}_w$. As usual we give $\mathrm{Sel}_\Sigma^{\Sigma'}(H)$ the contragradient $G$-action $(g\varphi)(x) = \varphi(g^{-1}x)$.

Let $Y_{H,\Sigma}$ denote the free abelian group on the places of $H$ above $\Sigma$, endowed with its canonical $G$-action.

**Lemma 3.1.** *There is a canonical short exact sequence of* $\mathbf{Z}[G]^-$*-modules*

$$0 \longrightarrow Y_{H,\Sigma}^- \longrightarrow \mathrm{Sel}_\Sigma^{\Sigma'}(H)^- \longrightarrow \mathrm{Cl}^{\Sigma'}(H)^{\vee,-} \longrightarrow 0.$$

*Proof.* We have a canonical short exact sequence

$$0 \longrightarrow Y_{H,\Sigma\setminus S_\infty} \longrightarrow \mathrm{Sel}_\Sigma^{\Sigma'}(H) \longrightarrow \mathrm{Sel}_{S_\infty}^{\Sigma'}(H) \longrightarrow 0,$$

where the first nontrivial arrow is induced by $w \mapsto \mathrm{ord}_w$. Note that $Y_{H,S_\infty}^- = 0$. To prove the result we must show that

$$\mathrm{Sel}_{S_\infty}^{\Sigma'}(H)^- \cong \mathrm{Cl}^{\Sigma'}(H)^{\vee,-}. \tag{30}$$

Yet the sequence (5) in [4] for $\Sigma = S_\infty$ reads

$$0 \longrightarrow \mathrm{Cl}^{\Sigma'}(H)^\vee \longrightarrow \mathrm{Sel}_{S_\infty}^{\Sigma'}(H) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(\mathcal{O}^*_{H,S_\infty,\Sigma'}, \mathbf{Z}) \longrightarrow 0.$$

Since $H$ is a CM field, $(\mathcal{O}^*_{H,S_\infty,\Sigma'})^-$ is trivial, yielding (30). The result follows. □

It is convenient to provide an alternate presentation of $\mathrm{Sel}_\Sigma^{\Sigma'}(H)$ as follows. Let $S'$ be any finite set of places of $F$ containing $\Sigma$ and disjoint from $\Sigma'$. Assume that $S'$ is chosen such that the class group $\mathrm{Cl}_{S'}^{\Sigma'}(H)$ is trivial. As shown in [5, equation (12)], there is a canonical isomorphism

$$\mathrm{Sel}_\Sigma^{\Sigma'}(H) \cong \mathrm{Hom}_{\mathbf{Z}}(\mathcal{O}^*_{H,S',\Sigma'}, \mathbf{Z}) / \prod_{w \in S'_H - \Sigma_H} \mathbf{Z}, \tag{31}$$

with the implicit map as in (29).

As a final note in this section, we show that the Fitting ideal of $\mathrm{Sel}_\Sigma^{\Sigma'}(H)$ vanishes on any non-identity component $\psi$ with a trivial zero. More precisely, let $\psi \in \hat{G}$, $\psi \neq 1$, such that $\psi(G_v) = 1$ for some $v \in \Sigma$. Here $G_v \subset G$ denotes the decomposition group at $v$. Writing

$$\mathrm{Sel}_\Sigma^{\Sigma'}(H)_\psi = \mathrm{Sel}_\Sigma^{\Sigma'}(H) \otimes_{\mathbf{Z}[G]} \mathcal{O}_\psi$$

with $\mathcal{O}_\psi$ as in §2.2, we claim that $\mathrm{Fitt}_{\mathcal{O}_\psi}(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_\psi) = 0$. For this, it suffices to show that the finitely generated $\mathcal{O}_\psi$-module $\mathrm{Sel}_\Sigma^{\Sigma'}(H)_\psi$ is infinite. Let $X_{H,\Sigma} \subset Y_{H,\Sigma}$ denote the submodule of degree 0 elements. Let $K$ denote the fraction field of $\mathcal{O}_\psi$. Then

$$\begin{aligned}
\mathrm{Sel}_\Sigma^{\Sigma'}(H)_\psi \otimes_{\mathcal{O}_\psi} K &\cong \mathrm{Hom}(\mathcal{O}^*_{H,\Sigma,\Sigma'}, K)_\psi \\
&\cong \mathrm{Hom}(X_{H,\Sigma}, K)_\psi \\
&\cong \mathrm{Hom}_K((X_{H,\Sigma} \otimes K)^\psi, K).
\end{aligned}$$

The first isomorphism follows from [4, Equation (5)] and the second from the Dirichlet Unit Theorem. Hence it suffices to show that $(X_{H,\Sigma} \otimes K)^\psi \neq 0$. Since $\psi \neq 1$, we have

$$(X_{H,\Sigma} \otimes K)^\psi \cong (Y_{H,\Sigma} \otimes K)^\psi \supset (Y_{H,\{v\}} \otimes K)^\psi = (\mathrm{Ind}_{G_v}^G K)^\psi \cong K$$

by Frobenius reciprocity, as $\psi(G_v) = 1$. The desired result $\mathrm{Fitt}_{\mathcal{O}_\psi}(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_\psi) = 0$ follows.

**Lemma 3.2.** *Let $\Psi \subset \hat{G}$ with $1 \notin \Psi$ and let $R_\Psi$ denote the associated character group ring. Suppose that for each $\psi \in \Psi$, there exists $v \in \Sigma$ such that $\psi(G_v) = 1$. Then*

$$\mathrm{Fitt}_{R_\Psi}(\mathrm{Sel}_\Sigma^{\Sigma'}(H) \otimes_{\mathbf{Z}[G]} R_\Psi) = 0 = \Theta_{\Sigma,\Sigma'} R_\Psi.$$

*Proof.* The first equality follows immediately from the fact that $\mathrm{Fitt}_{\mathcal{O}_\psi}(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_\psi) = 0$ since Fitting ideals are functorial with respect to quotients. Similarly the second equality follows since for all $\psi \in \Psi$ we have

$$\psi(\Theta_{\Sigma,\Sigma'}) = L_{\Sigma,\Sigma'}(\psi, 0) = (1 - \psi(v)) L_{\Sigma - \{v\},\Sigma'}(\psi, 0) = 0.$$

□

## 3.2 Keystone Result

Recall that $S_{\mathrm{ram}}$ denotes the set of primes of $F$ above $p$ that are ramified in $H/F$. As in the introduction, let $T$ denote a finite set of primes of $F$ that are unramified in $H$ and such that $T$ satisfies the condition (1). Let

$$\begin{aligned} \Sigma &= \{v \in S_{\mathrm{ram}} \colon v \mid p\} \cup S_\infty, \\ \Sigma' &= \{v \in S_{\mathrm{ram}} \colon v \nmid p\} \cup T. \end{aligned} \tag{32}$$

In other words, we transfer the ramified primes not above $p$ from the depletion set to the smoothing set. The theorem whose proof occupies most of the paper, and from which all other results are deduced, is the following.

**Theorem 3.3.** *The $\mathbf{Z}_p[G]^-$-module $\mathrm{Sel}_\Sigma^{\Sigma'}(H)_p^- = (\mathrm{Sel}_\Sigma^{\Sigma'}(H) \otimes_{\mathbf{Z}} \mathbf{Z}_p)^-$ is quadratically presented and we have*

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]^-}(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_p^-) = (\Theta_{\Sigma,\Sigma'}^{\#}).$$

Implicit in the statement of Theorem 3.3 is that $\Theta_{\Sigma,\Sigma'}^{\#} \in \mathbf{Z}_p[G]$, which follows from a lemma of Kurihara (see Lemma 3.4 and Remark 3.6 below).

## 3.3 Strong Brumer–Stark and Kurihara's Conjecture

In Theorem 1.4 we stated Kurihara's formula for the Fitting ideal of the $\mathbf{Z}[G]^-$module $\mathrm{Cl}^T(H)^{\vee,-}$, which he conjectured in [27] (see also [19]). The following lemma shows that the statement is well-formed.

**Lemma 3.4** (Kurihara)**.** $\mathrm{SKu}^T(H/F)$ *is contained in $\mathbf{Z}[G]$ and hence is an ideal of this ring.*

*Proof.* The key input for this result is the integrality statement (2) of Deligne–Ribet and Cassou-Noguès. For $S_\infty \subset J \subset S_\infty \cup S_{\mathrm{ram}}$, we write $\overline{J} = S_{\mathrm{ram}} \setminus J$. Note that

$$\mathrm{SKu}^T(H/F) = \left( \prod_{v \in \overline{J}} \mathrm{N} I_v \cdot (\Theta_{J,T}^{H/F})^{\#} \colon S_\infty \subset J \subset S_\infty \cup S_{\mathrm{ram}} \right).$$

Write $H^{\overline{J}}$ for the maximal subextension of $H$ unramified at all primes in $\overline{J}$. Then $H^{\overline{J}}$ is the subfield of $H$ fixed by the subgroup of $G$ generated by $I_v$ for all $v \in \overline{J}$. Multiplication by $\prod_{v\in\overline{J}} \mathrm{N}I_v$ defines a homomorphism

$$\mathbf{Z}[\mathrm{Gal}(H^{\overline{J}}/F)] \longrightarrow \mathbf{Z}[G],$$

and we have

$$\prod_{v\in\overline{J}} \mathrm{N}I_v \cdot (\Theta_{J,T}^{H^{\overline{J}}/F})^{\#} = \prod_{v\in\overline{J}} \mathrm{N}I_v \cdot (\Theta_{J,T}^{H/F})^{\#}. \tag{33}$$

Therefore

$$\mathrm{SKu}^T(H/F) = \left( \prod_{v\in\overline{J}} \mathrm{N}I_v \cdot (\Theta_{J,T}^{H^{\overline{J}}/F})^{\#} \colon S_\infty \subset J \subset S_\infty \cup S_{\mathrm{ram}} \right). \tag{34}$$

By (2), the element $(\Theta_{J,T}^{H^{\overline{J}}/F})^{\#}$ belongs to $\mathbf{Z}[\mathrm{Gal}(H^{\overline{J}}/F)]^-$ and hence (33) lies in $\mathbf{Z}[G]$. The result follows. □

The following is our main result.

**Theorem 3.5** (Conjecture of Kurihara)**.** *We have*

$$\mathrm{Fitt}_{\mathbf{Z}[G]^-}(\mathrm{Cl}^T(H)^{\vee,-}) = \mathrm{SKu}^T(H/F)^-.$$

As noted in (7), Theorem 3.5 implies Strong Brumer–Stark (Theorem 1.3). In this section, we assume Theorem 3.3 and prove a partial result toward Theorem 3.5 that still yields Strong Brumer–Stark. In Appendix B we bootstrap from this partial result to complete the proof of Theorem 3.5.

For an odd prime $p$ we define the $p$-modified Sinnott–Kurihara ideal by

$$\mathrm{SKu}_p^T(H/F) = (\Theta_{\Sigma,T}^{\#}) \prod_{v\in S_{\mathrm{ram}},\, v\nmid p} (\mathrm{N}I_v, 1-\sigma_v e_v) \subset \mathbf{Z}_p[G]$$

where $\Sigma$ is as in (32).

**Remark 3.6.** The fact that $\mathrm{SKu}_p^T(H/F) \subset \mathbf{Z}_p[G]$ follows directly from Lemma 3.4, since

$$\Theta_{\Sigma,T}^{\#} = \Theta_{S_\infty,T}^{\#} \prod_{v\in S_{\mathrm{ram}},\, v|p} (1-\sigma_v e_v).$$

Moreover, for $v \nmid p$ the $p$-Sylow subgroup of $I_v$ is a quotient of $(\mathcal{O}/v)^*$ and hence $\#I_v$ divides $\mathrm{N}v - 1$ in $\mathbf{Z}_p$. Therefore for $\Sigma, \Sigma'$ as in Theorem 3.3,

$$\begin{aligned}
\Theta_{\Sigma,\Sigma'}^{\#} &= \Theta_{\Sigma,T}^{\#} \prod_{v\in S_{\mathrm{ram}}, v\nmid p} (1-\sigma_v e_v \mathrm{N}v) \\
&= \Theta_{\Sigma,T}^{\#} \prod_{v\in S_{\mathrm{ram}}, v\nmid p} \left[ (1-\sigma_v e_v) + \left( \sigma_v \cdot \mathrm{N}I_v \frac{1-\mathrm{N}v}{\#I_v} \right) \right] \\
&\in \mathrm{SKu}_p^T(H/F) \subset \mathbf{Z}_p[G].
\end{aligned}$$

The partial result toward Theorem 3.5 that we prove in this section is the following.

**Theorem 3.7.** *For every odd prime $p$ we have*

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]^-}(\mathrm{Sel}_\Sigma^T(H)_p^-) = \mathrm{SKu}_p^T(H/F)^-.$$

Before discussing the proof of Theorem 3.7, let us note that it is strong enough to imply Strong Brumer–Stark.

**Corollary 3.8.** *The Strong Brumer–Stark Conjecture is true:*

$$\Theta_{S,T}^\#(H/F) \in \mathrm{Fitt}_{\mathbf{Z}[G]^-}(\mathrm{Cl}^T(H)^{\vee,-}).$$

*Proof of Corollary 3.8.* It suffices to work prime by prime, i.e. to show that

$$\Theta_{S,T}^\#(H/F) \in \mathrm{Fitt}_{\mathbf{Z}_p[G]^-}(\mathrm{Cl}^T(H)_p^{\vee,-})$$

for each odd prime $p$. By Lemma 3.1 there is a surjection $\mathrm{Sel}_\Sigma^T(H)^- \twoheadrightarrow \mathrm{Cl}^T(H)^{\vee,-}$ that together with Theorem 3.7 implies

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]^-}(\mathrm{Cl}^T(H)_p^{\vee,-}) \supset \mathrm{SKu}_p^T(H/F). \tag{35}$$

Since

$$\Theta_{S,T}^\# = \Theta_{\Sigma,T}^\# \prod_{v\in S_{\mathrm{ram}},\, v\nmid p} (1-\sigma_v e_v) \in \mathrm{SKu}_p^T(H/F),$$

the result follows. □

We now prove Theorem 3.7 assuming our keystone result, Theorem 3.3.

*Proof of Theorem 3.7.* First note that it suffices to prove the result after extending scalars to $\mathcal{O}$ and then projecting to the connected component $R = \mathcal{O}[G_p]_\chi$ of $\mathcal{O}[G]^-$ associated to each odd character $\chi$ of $G'$. Theorem 3.3 yields

$$\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R) = (\Theta_{\Sigma,\Sigma'}^\#), \tag{36}$$

where the right side denotes the principal ideal of $R$ generated by the projection of the element $\Theta_{\Sigma,\Sigma'}^\# \in \mathcal{O}[G]$ to $R$.

To prove the theorem, we must demonstrate the effect of removing the primes in

$$S' = \{v \in S_{\mathrm{ram}}, v \nmid p\}$$

from the superscript of the Selmer group in (36). For this we first consider the short exact sequence of $\mathbf{Z}[G]^-$-modules

$$0 \longrightarrow \mathrm{Cl}^T(H)^{\vee,-} \longrightarrow \mathrm{Cl}^{\Sigma'}(H)^{\vee,-} \longrightarrow \textstyle\prod_{w\in S'_H}((\mathcal{O}_H/w)^*)^{\vee,-} \longrightarrow 0. \tag{37}$$

For each $v \in S'$, note that the inertia group $I_v \subset G$ acts trivially on $(\mathcal{O}_H/w)^*$. Decompose $I_v$ as a product $I_v = I_{v,p} \times I'_v$ of its subgroups of $p$-power order elements and prime-to-$p$ order elements, respectively. For $\tau \in I'_v$, the element $\tau - 1 \in \mathcal{O}[G]$ has image $\chi(\tau) - 1$ in $R$. This is a unit if $\chi(\tau) \neq 1$, and is 0 if $\chi(\tau) = 1$. Since $\tau - 1$ kills $(\mathcal{O}_H/w)^*$, it follows that the base extension of $(\mathcal{O}_H/w)^*$ to $R$ is trivial unless $\chi(I'_v) = 1$. And in this latter case $\tau - 1$ has vanishing image in $R$ for $\tau \in I'_v$.

Next note that by class field theory, $I_{v,p}$ is a quotient of $(\mathcal{O}_F/v)^*$ since $v \nmid p$. Hence $I_{v,p}$ is cyclic, and $\mathrm{N}v \equiv 1 \pmod{\#I_{v,p}}$. Let $\tau_v$ be a generator of $I_{v,p}$. Fixing a prime $w$ of $H$ above $v$ and a generator $u$ for $(\mathcal{O}_H/w)^*$ yields an isomorphism

$$\mathbf{Z}[G_v]/(\tau_v - 1, \sigma_v - \mathrm{N}v, \tau - 1 : \tau \in I'_v) \cong (\mathcal{O}_H/w)^*, \qquad x \mapsto u^x,$$

where $\sigma_v$ is any element representing the Frobenius $I_v$-coset in $G_v$. Inducing from $G_v$ to $G$, taking duals, and projecting to the $R$-component yields:

$$\prod_{w \in S'_H} ((\mathcal{O}_H/w)^*)^\vee_R \cong \prod_{v \in S', \chi(I'_v)=1} R/(\tau_v - 1, \sigma_v^{-1} - \mathrm{N}v). \tag{38}$$

Next consider the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Y^-_{H,\Sigma} & \longrightarrow & \mathrm{Sel}^T_\Sigma(H)^- & \longrightarrow & \mathrm{Cl}^T(H)^{\vee,-} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & Y^-_{H,\Sigma} & \longrightarrow & \mathrm{Sel}^{\Sigma'}_\Sigma(H)^- & \longrightarrow & \mathrm{Cl}^{\Sigma'}(H)^{\vee,-} & \longrightarrow & 0. \end{array}$$

The snake lemma in conjunction with (37) yields a short exact sequence

$$0 \longrightarrow \mathrm{Sel}^T_\Sigma(H)^- \longrightarrow \mathrm{Sel}^{\Sigma'}_\Sigma(H)^- \longrightarrow \textstyle\prod_{w \in S'_H} ((\mathcal{O}_H/w)^*)^{\vee,-} \longrightarrow 0. \tag{39}$$

Applying (38), this may be written

$$0 \longrightarrow \mathrm{Sel}^T_\Sigma(H)^- \longrightarrow \mathrm{Sel}^{\Sigma'}_\Sigma(H)^- \longrightarrow \prod_{\substack{v \in S' \\ \chi(I'_v)=1}} R/(\tau_v - 1, \sigma_v^{-1} - \mathrm{N}v) \longrightarrow 0. \tag{40}$$

Consider for each $v \in S'$ such that $\chi(I'_v) = 1$ the short exact sequence:

$$0 \longrightarrow R/(\mathrm{N}I_{v,p}, \sigma_v^{-1} - \mathrm{N}v) \longrightarrow R/(\sigma_v^{-1} - \mathrm{N}v) \longrightarrow R/(\tau_v - 1, \sigma_v^{-1} - \mathrm{N}v) \longrightarrow 0, \tag{41}$$

where the first non-trivial arrow is multiplication by $\tau_v - 1$ and the next arrow is projection. Only the injectivity of this multiplication is unclear. Suppose $x(\tau_v - 1) = y(\sigma_v^{-1} - \mathrm{N}v)$ for $x, y \in R$. Then $y(\sigma_v^{-1} - \mathrm{N}v)$ vanishes in $R/(\tau_v - 1) \cong \mathcal{O}[G_p/I_{v,p}]$. But $\sigma_v^{-1} - \mathrm{N}v$ is a non-zerodivisor in this group ring, and hence the image of $y$ in this ring vanishes, i.e.

$y = (\tau_v - 1)y'$ for some $y' \in R$. Then $x - y'(\sigma_v - \mathrm{N}v)$ is annihilated by $\tau_v - 1$ and hence is a multiple of $\mathrm{N}I_{v,p}$. Thus $x \in (\mathrm{N}I_{v,p}, \sigma_v^{-1} - \mathrm{N}v)$, proving the desired injectivity.

Applying Lemma 2.7 to (40) and the product of (41) over the appropriate $v$ yields

$$\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^T(H)_R) \prod_{v\in S', \chi(I_v')=1} (\sigma^{-1} - \mathrm{N}v) = \mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R) \prod_{v\in S', \chi(I_v')=1} (\mathrm{N}I_v, \sigma_v^{-1} - \mathrm{N}v). \quad (42)$$

A key point is that the terms $\sigma^{-1} - \mathrm{N}v$ are non-zerodivisors and hence can be inverted in $\mathrm{Frac}(R)$. Note also that if $\chi(I_v') \neq 1$ then the projection of $I_v$ to $R$ vanishes and hence $e_v = 0$ in $\mathrm{Frac}(R)$. In particular

$$\begin{aligned}\Theta_{\Sigma,\Sigma'}^{\#} &= \Theta_{\Sigma,T}^{\#} \prod_{v\in S'} (1 - \sigma_v e_v \mathrm{N}v) \\ &= \Theta_{\Sigma,T}^{\#} \prod_{v\in S', \chi(I_v')=1} (1 - \sigma_v e_v \mathrm{N}v).\end{aligned}$$

Furthermore, if $\chi(I_v') = 1$ then $\mathrm{N}I_v = (\#I_v')\mathrm{N}I_{v,p}$, and the integer $\#I_v'$ is a $p$-adic unit. Also in this case $e_v = e_{v,p}e_v' = e_{v,p}$ in $\mathrm{Frac}(R)$, where $e_{v,p} = \mathrm{N}I_{v,p}/\#I_{v,p}$ and $e_v' = \mathrm{N}I_v'/\#I_v' = 1$.

Therefore, applying (36) to (42) yields:

$$\begin{aligned}\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^T(H)_R) &= (\Theta_{\Sigma,\Sigma'}^{\#}) \prod_{v\in S', \chi(I_v')=1} (\mathrm{N}I_{v,p}, \sigma_v^{-1} - \mathrm{N}v)(\sigma^{-1} - \mathrm{N}v)^{-1} \\ &= (\Theta_{\Sigma,T}^{\#}) \prod_{v\in S', \chi(I_v')=1} (\mathrm{N}I_{v,p}, \sigma_v^{-1} - \mathrm{N}v)(1 - \sigma_v e_{v,p}\mathrm{N}v)(\sigma^{-1} - \mathrm{N}v)^{-1} \\ &= (\Theta_{\Sigma,T}^{\#}) \prod_{v\in S', \chi(I_v')=1} (\mathrm{N}I_{v,p}, 1 - \sigma_v e_{v,p}\mathrm{N}v).\end{aligned}$$

Finally we note that for $v \in S', \chi(I_v') = 1$, since $\mathrm{N}v \equiv 1 \pmod{\#I_{v,p}}$ we have

$$\begin{aligned}(\mathrm{N}I_{v,p}, 1 - \sigma_v e_{v,p}\mathrm{N}v) &= (\mathrm{N}I_{v,p}, 1 - \sigma_v e_{v,p}) \\ &= (\mathrm{N}I_v, 1 - \sigma_v e_v).\end{aligned}$$

To conclude the proof, we note that for $v \in S'$ such that $\chi(I_v') \neq 1$, we have

$$(\mathrm{N}I_v, 1 - \sigma_v e_v) = (1) \text{ in } R.$$

We have therefore proven that

$$\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^T(H)_R) = (\Theta_{\Sigma,T}^{\#}) \prod_{v\in S'} (\mathrm{N}I_v, 1 - \sigma_v e_v \mathrm{N}v),$$

which is the projection to $R$ of the desired result. □

## 3.4 Rubin's Conjecture

In this section we prove that Strong Brumer–Stark implies Rubin's conjecture away from 2. This result is known by the experts, but since only a dual version of this appears in the literature (see [34, Corollary 2.4]), we give a proof here.

**Lemma 3.9.** *Let $R$ be a commutative ring and let $N \subset M$ be $R$-modules with $N$ finitely generated and $M$ finitely presented. For each positive integer $r$, the ideal* $\mathrm{Fitt}(M/N)$ *annihilates the cokernel of the canonical map*

$$\bigwedge_R^r N \longrightarrow \bigwedge_R^r M.$$

*Proof.* We first reduce to the case that $M$ and $N$ are both finitely generated free $R$-modules. By the assumptions on $M$ and $N$, we may fix a surjection $R^m \longrightarrow M$ and a finite presentation

$$R^n \longrightarrow R^m \longrightarrow M/N \longrightarrow 0$$

This yields a commutative diagram

$$\begin{array}{ccccc} R^n & \longrightarrow & R^m & \longrightarrow & M/N \\ \vdots & & \downarrow & & \| \\ N & \longrightarrow & M & \longrightarrow & M/N. \end{array}$$

The dotted arrow exists because $R^n$ is free. Using the right exactness of the exterior power functor we get a commutative diagram

$$\begin{array}{ccccc} \bigwedge_R^r R^n & \longrightarrow & \bigwedge_R^r R^m & \twoheadrightarrow & C_2 \\ \downarrow & & \downarrow & & \downarrow \\ \bigwedge_R^r N & \longrightarrow & \bigwedge_R^r M & \twoheadrightarrow & C_1. \end{array}$$

Here $C_1$ and $C_2$ are cokernels of the obvious maps. It is also clear that the map $C_2 \longrightarrow C_1$ is surjective. Therefore it is enough to show that $\mathrm{Fitt}(M/N)$ annihilates $C_2$. Hence we may assume that $M \cong R^m$ and $N \cong R^n$ are both free $R$-modules. Without loss of generality we further assume that $n \geq m$. Let the map $R^n \longrightarrow R^m$ be given by an $m \times n$ matrix $A$. We fix an $m \times m$ submatrix, say $A'$ of $A$. We must show that $\det(A')$ annihilates $C_2$.

The map $\bigwedge_R^r R^n \longrightarrow \bigwedge_R^r R^m$ is given by the $r$th compound matrix $C_r(A)$—this is the $\binom{m}{r} \times \binom{n}{r}$ matrix whose entries are the $r \times r$ minors of $A$. Let $x \in \bigwedge_R^r R^m$. Denote by $\mathrm{adj}_r(A')$ the $r$th higher adjugate matrix of $A'$, so

$$\mathrm{adj}_r(A') \cdot C_r(A')x = \det(A')x.$$

Observe that $C_r(A')$ is an $\binom{m}{r} \times \binom{m}{r}$ submatrix of $C_r(A)$ obtained by deleting $\binom{n}{r} - \binom{m}{r}$ columns. Let $\tilde{x}$ be the element of $\bigwedge_R^r R^n$ obtained from $x$ by inserting 0's in the entries corresponding to these deleted columns. Then $C_r(A)\tilde{x} = C_r(A')x$, hence

$$\mathrm{adj}_r(A') \cdot C_r(A)\tilde{x} = \mathrm{adj}_r(A') \cdot C_r(A')x = \det(A')x.$$

This shows that $\det(A')x$ belongs to the image of $\bigwedge_R^r R^n \longrightarrow \bigwedge_R^r R^m$. Hence $\det(A')$ annihilates $C_2$, as desired. □

For Rubin's conjecture, recall that we are given a set of $r$ prime ideals

$$S' = \{v_1, \ldots, v_r\}$$

of $F$ that split completely in $H$. Let $A \subset \mathrm{Cl}^T(H)^-$ denote the subgroup generated by the classes associated to the primes in $S'$. By duality we obtain a surjection $\mathrm{Cl}^T(H)^{\vee,-} \longrightarrow A^\vee$. The strong Brumer–Stark conjecture implies that

$$\Theta_{S,T}^{\#} \in \mathrm{Fitt}_{\mathbf{Z}[G]^-}(\mathrm{Cl}^T(H)^{\vee,-}) \subset \mathrm{Fitt}_{\mathbf{Z}[G]^-}(A^\vee). \tag{43}$$

The $\mathbf{Z}[G]^-$-module $A$ sits in a short exact sequence

$$0 \longrightarrow U_{S',T}^- \longrightarrow Y_{H,S'}^- \longrightarrow A \longrightarrow 0. \tag{44}$$

Here $U_{S',T}$ is defined in (8). The first nontrivial map in (44) sends

$$u \mapsto \sum_{w \in S'_H} \mathrm{ord}_w(u)w = \sum_{i=1}^{r} \left( \sum_{\sigma \in G} \mathrm{ord}_{w_i}(\sigma(u))[\sigma^{-1}] \right) w_i,$$

where the $w_i$ are the chosen primes above the $v_i \in S'$ as in (9)–(10). The second nontrivial map in (44) sends $w \in S'_H$ to its class in $A \subset \mathrm{Cl}^T(H)^-$. Since $A$ is finite, the long exact sequence associated to the functor $\mathrm{Hom}_{\mathbf{Z}[\frac{1}{2}]}(-, \mathbf{Z}[\frac{1}{2}])$ applied to (44) yields

$$0 \longrightarrow \mathrm{Hom}_{\mathbf{Z}[\frac{1}{2}]}(Y_{H,S'}^-, \mathbf{Z}[\tfrac{1}{2}]) \longrightarrow \mathrm{Hom}_{\mathbf{Z}[\frac{1}{2}]}(U_{S',T}^-, \mathbf{Z}[\tfrac{1}{2}]) \longrightarrow A^\vee \longrightarrow 0. \tag{45}$$

To maintain $G$-equivariance of this sequence, all terms are given the contragradient $G$-action. Note that by Shapiro's Lemma there is a canonical isomorphism of functors

$$\mathrm{Hom}_{\mathbf{Z}[\frac{1}{2}]}(-, \mathbf{Z}[\tfrac{1}{2}]) \cong \mathrm{Hom}_{\mathbf{Z}[G]}(-, \mathbf{Z}[G]^-)$$

on the category of $\mathbf{Z}[G]^-$-modules. We can therefore write (45) as

$$0 \longrightarrow \mathrm{Hom}_{\mathbf{Z}[G]}(Y_{H,S'}^-, \mathbf{Z}[G]^-) \longrightarrow \mathrm{Hom}_{\mathbf{Z}[G]}(U_{S',T}^-, \mathbf{Z}[G]^-) \longrightarrow A^\vee \longrightarrow 0. \tag{46}$$

Using (43), Lemma 3.9 implies that $\Theta_{S,T}^{\#} \in \mathrm{Fitt}_{\mathbf{Z}[G]^-}(A^\vee)$ annihilates the cokernel of the induced map

$$\bigwedge_{\mathbf{Z}[G]}^r \mathrm{Hom}_{\mathbf{Z}[G]}(Y_{H,S'}^-, \mathbf{Z}[G]^-) \longrightarrow \bigwedge_{\mathbf{Z}[G]}^r \mathrm{Hom}_{\mathbf{Z}[G]}(U_{S',T}^-, \mathbf{Z}[G]^-). \tag{47}$$

Suppose now that we are given an element

$$\varphi \in \bigwedge_{\mathbf{Z}[G]}^r \mathrm{Hom}_{\mathbf{Z}[G]}(U_{S',T}^-, \mathbf{Z}[G]^-).$$

We must prove that $\varphi(u_{\mathrm{RBS}}) \in \mathbf{Z}[G]^-$. Note that after tensoring with $\mathbf{Q}$ over $\mathbf{Z}[\frac{1}{2}]$, the map in (47) becomes an isomorphism, so $\varphi$ extends to an element of

$$\bigwedge_{\mathbf{Z}[G]}^r \mathrm{Hom}_{\mathbf{Z}[G]}(Y_{H,S'}^-, \mathbf{Q}[G]^-).$$

We then note that

$$\begin{aligned} \varphi(u_{\mathrm{RBS}}) &= \varphi(\mathrm{ord}_G(u_{\mathrm{RBS}})(w_1 \wedge \cdots \wedge w_r)) \\ &= (\mathrm{ord}_G(u_{\mathrm{RBS}})^{\#}\varphi)(w_1 \wedge \cdots \wedge w_r) \\ &= (\Theta_{S,T}^{\#} \cdot \varphi)(w_1 \wedge \cdots \wedge w_r). \end{aligned} \tag{48}$$

Here # appears because of the contragradient $G$-action. Since $\Theta_{S,T}^{\#}$ annihilates the cokernel of (47), it follows that (48) lies in $\mathbf{Z}[G]^-$ as desired. This concludes the proof that Theorem 1.3 implies Theorem 1.6.

# 4 On the smoothing and depletion sets

The goal of the rest of the paper is to prove Theorem 3.3. After extending to $\mathcal{O}$ and projecting onto the component $R = R_\chi = \mathcal{O}[G_p]_\chi$ corresponding to a prime-to-$p$ order character $\chi$, this statement reads

$$\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R) = (\Theta_{\Sigma,\Sigma'}^{\#}). \tag{49}$$

In this section, we alter some of the parameters in this equation.

## 4.1 Removing primes above $p$ from the smoothing set

The set $T$, and hence $\Sigma'$, may contain primes above $p$. We show that it is safe to remove these primes from $T$ without altering the situation. Note that by definition these primes are necessarily unramified in $H$.

**Lemma 4.1.** *Let $\Sigma'' = \Sigma' - \{v \in T : v \mid p\}$. We have*

$$\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R \cong \mathrm{Sel}_\Sigma^{\Sigma''}(H)_R$$

*and*

$$(\Theta_{\Sigma,\Sigma'}^{\#}) = (\Theta_{\Sigma,\Sigma''}^{\#}).$$

*Proof.* As in (40), we have a short exact sequence

$$0 \longrightarrow \mathrm{Sel}_{\Sigma}^{\Sigma''}(H)_R \longrightarrow \mathrm{Sel}_{\Sigma}^{\Sigma'}(H)_R \longrightarrow \Big[\prod_{\substack{v\in T\\ v|p}} \prod_{w|v} (\mathcal{O}_H/w)^*\Big]_R^{\vee} \longrightarrow 0.$$

The group on the right in brackets has prime-to-$p$ order, hence its tensor product with $R$ vanishes. This proves the first result. On the analytic side, we note that the factor $(1-\sigma_v \mathrm{N}v)$ has image in $R$ that is a unit when $v \mid p$ and hence the elements

$$\Theta^{\#}_{\Sigma,\Sigma'} = \Theta^{\#}_{\Sigma,\Sigma''} \prod_{v\in T,\ v|p} (1-\sigma_v \mathrm{N}v)$$

and $\Theta^{\#}_{\Sigma,\Sigma''}$ generate the same ideal under projection to $R$. □

Hereafter we replace $\Sigma'$ by $\Sigma''$ and therefore assume that $T$ and $\Sigma'$ contain no primes above $p$.

## 4.2 Passing to the field cut out by $\chi$

Next, we show that we can replace $H$ by the fixed field of the kernel of $\chi$ inside $G'$, which we denote $H_\chi$.

**Lemma 4.2.** *Let $H_\chi \subset H$ denote the subfield of $H$ fixed by the kernel of $\chi$ inside $G'$. Let $\Sigma \supset S_\infty$ and $\Sigma'$ be finite disjoint sets of places of $F$ whose union contains the set $S_{ram}$ of finite primes ramified in $H/F$. There is a canonical isomorphism $\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)_R \cong \mathrm{Sel}_{\Sigma}^{\Sigma'}(H_\chi)_R$.*

*Proof.* The inclusion $H_\chi \subset H$ induces a map $\mathrm{Sel}_{\Sigma}^{\Sigma'}(H) \longrightarrow \mathrm{Sel}_{\Sigma}^{\Sigma'}(H_\chi)$, which upon passing to the $R$-component induces a map

$$\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)_R \longrightarrow \mathrm{Sel}_{\Sigma}^{\Sigma'}(H_\chi)_R.$$

To show that this map is an isomorphism, we use the presentation (31) for the Selmer groups. Note that

$$\begin{aligned}(\mathrm{Hom}_{\mathbf{Z}}(\mathcal{O}^*_{H,S',\Sigma'}, \mathbf{Z}) \otimes_{\mathbf{Z}} \mathcal{O})_R &= \mathrm{Hom}_{\mathcal{O}}(\mathcal{O}^*_{H,S',\Sigma'} \otimes \mathcal{O}, \mathcal{O})_R \\ &= \mathrm{Hom}_{\mathcal{O}}((\mathcal{O}^*_{H,S',\Sigma'} \otimes \mathcal{O})^{G'=\chi}, \mathcal{O}),\end{aligned}$$

where the last equality follows since $\mathcal{O}^*_{H,S',\Sigma'} \otimes \mathcal{O}$ is a free $\mathcal{O}$-module of finite rank. Here the superscript denotes the sub-$\mathcal{O}$-module on which $g \in G'$ acts by multiplication by $\chi(g)$. We therefore obtain a commutative diagram

$$\begin{array}{ccccccc}
(Y_{H,S'-\Sigma})_R & \longrightarrow & \mathrm{Hom}_{\mathcal{O}}((\mathcal{O}^*_{H,S',\Sigma'} \otimes \mathcal{O})^{G'=\chi}, \mathcal{O}) & \longrightarrow & \mathrm{Sel}_{\Sigma}^{\Sigma'}(H)_R & \longrightarrow & 0 \\
\downarrow & & \downarrow \wr & & \downarrow & & \\
(Y_{H_\chi,S'-\Sigma})_R & \longrightarrow & \mathrm{Hom}_{\mathcal{O}}((\mathcal{O}^*_{H_\chi,S',\Sigma'} \otimes \mathcal{O})^{G'=\chi}, \mathcal{O}) & \longrightarrow & \mathrm{Sel}_{\Sigma}^{\Sigma'}(H_\chi)_R & \longrightarrow & 0.
\end{array} \tag{50}$$

As indicated, the middle vertical arrow is clearly an isomorphism (Galois theory). Therefore the right vertical arrow is surjective. To prove that it is also injective, it suffices to prove that the left vertical arrow is surjective. This follows since the primes in $S' - \Sigma$ are unramified in $H_\chi$. □

It is clear from the definitions that the images of $\Theta_{\Sigma,\Sigma'}^{H/F}$ and $\Theta_{\Sigma,\Sigma'}^{H_\chi/F}$ in $R$ are equal. Lemma 4.2 therefore shows that it suffices to prove equation (49) with $H$ replaced by $H_\chi$. Next we show that the primes ramified in $H$ but not ramified in $H_\chi$ can be excluded from the depletion and smoothing sets. In other words, we let

$$\Sigma(\chi) = \{v \mid p\colon v \text{ is ramified in } H_\chi\} \cup S_\infty,$$
$$\Sigma'(\chi) = \{v \nmid p\colon v \text{ is ramified in } H_\chi\} \cup T.$$

Note that

$$\Theta_{\Sigma,\Sigma'}(H_\chi/F)^\# = \Theta_{\Sigma(\chi),\Sigma'(\chi)}(H_\chi/F)^\# \prod_{v\in\Sigma-\Sigma(\chi)} (1-\sigma_v) \prod_{v\in\Sigma'-\Sigma'(\chi)} (1-\sigma_v \mathrm{N}v). \tag{51}$$

The fact that the Selmer group also behaves nicely with respect to the addition of unramified primes to the depletion and smoothing sets is well known:

**Lemma 4.3.** *Suppose that the $R$-module $\mathrm{Sel}_{\Sigma(\chi)}^{\Sigma'(\chi)}(H_\chi)_R$ is quadratically presented. Then $\mathrm{Sel}_{\Sigma}^{\Sigma'}(H_\chi)_R$ is quadratically presented as well, and we have*

$$\mathrm{Fitt}(\mathrm{Sel}_{\Sigma}^{\Sigma'}(H_\chi)_R) = \mathrm{Fitt}(\mathrm{Sel}_{\Sigma(\chi)}^{\Sigma'(\chi)}(H_\chi)_R) \prod_{v\in\Sigma-\Sigma(\chi)} (1-\sigma_v) \prod_{v\in\Sigma'-\Sigma'(\chi)} (1-\sigma_v \mathrm{N}v).$$

*Proof.* We have the commutative diagram

$$\begin{array}{ccccc}
(Y_{H_\chi,S'-\Sigma})_R & \hookrightarrow & \mathrm{Hom}_{\mathcal{O}}((\mathcal{O}^*_{H_\chi,S',\Sigma'}\otimes\mathcal{O})^{G'=\chi},\mathcal{O}) & \twoheadrightarrow & \mathrm{Sel}_{\Sigma}^{\Sigma'}(H_\chi)_R \\
\downarrow & & \downarrow & & \downarrow \\
(Y_{H_\chi,S'-\Sigma(\chi)})_R & \hookrightarrow & \mathrm{Hom}_{\mathcal{O}}((\mathcal{O}^*_{H_\chi,S',\Sigma'(\chi)}\otimes\mathcal{O})^{G'=\chi},\mathcal{O}) & \twoheadrightarrow & \mathrm{Sel}_{\Sigma(\chi)}^{\Sigma'(\chi)}(H_\chi)_R.
\end{array}$$

similar to the one in (50). The middle vertical arrow is surjective with kernel given by $\prod_{v\in\Sigma'-\Sigma'(\chi)}\prod_{w|v}((\mathcal{O}_H/w)^*)^\vee_R$, which has Fitting ideal $\prod_{v\in\Sigma'-\Sigma'(\chi)}(1-\sigma_v\mathrm{N}v)$. In particular the right hand vertical arrow is surjective.

The left vertical arrow is injective with cokernel $(Y_{H_\chi,\Sigma-\Sigma(\chi)})_R$, which has Fitting ideal $\prod_{v\in\Sigma-\Sigma(\chi)}(1-\sigma_v)$. Since $\mathrm{Sel}_{\Sigma(\chi)}^{\Sigma'(\chi)}(H_\chi)_R$ and $(Y_{H_\chi,\Sigma-\Sigma(\chi)})_R$ are quadratically presented, the snake lemma along with Lemma 2.6 yields the required result. □

In view of (51) and Lemma 4.3, in order to prove (49) it suffices to prove that $\mathrm{Sel}_{\Sigma(\chi)}^{\Sigma'(\chi)}(H_\chi)_R$ is quadratically presented over $R$ and that

$$\mathrm{Fitt}_R(\mathrm{Sel}_{\Sigma(\chi)}^{\Sigma'(\chi)}(H_\chi)_R) = (\Theta^\#_{\Sigma(\chi),\Sigma'(\chi)}). \tag{52}$$

To recapitulate, by the results of §4, it remains to prove that the module $\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)_R$ is quadratically presented over $R$ and that

$$\mathrm{Fitt}_R(\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)_R) = (\Theta_{\Sigma,\Sigma'}^{\#}) \tag{53}$$

when:

- $H/F$ is such that $\chi$ is a *faithful* odd character of the maximal prime-to-$p$ subgroup $G' \subset G$;
- the sets $\Sigma, \Sigma'$ are defined as in the beginning of §3.2 for this extension $H/F$;
- the set $T$ contains no primes above $p$.

The results of this section show that (53) in this setting implies Theorem 3.3.

# 5 Divisibility Implies Equality

In this section we prove an analogue in the general setting of the "elementary argument" mentioned in the introduction and described in §2.3 for the case where $H/F$ is unramified at all finite primes. First, this argument will replace $\mathrm{Cl}^T(H)^-$ with an appropriate Selmer module since the former is not in general quadratically presented. Second, the analytic argument will be quite a bit more complicated for two reasons. (i) The Selmer module and Stickelberger element will have "trivial zeroes" at any character $\psi$ for which there exists $v \in \Sigma$ such that $\psi(G_v) = 1$, hence any generalization of (12) must account for trivial zeroes. (ii) The class number formula relates the size of class groups to $L$-values, and the exact sequences relating these class groups to Selmer modules are in general not split; appropriate quotients must be taken on which the size of class groups and Selmer modules can be related.

Recall the notation $G = \mathrm{Gal}(H/F) = G_p \times G'$, with $G_p$ of $p$-power order and $G'$ of prime-to-$p$ order. Let $R = \mathcal{O}[G_p]_\chi$ be a connected component of $\mathcal{O}[G]$ corresponding to an odd character $\chi$ of $G'$. Let $H_p$ denote the fixed field of $G'$ in $H$, so $\mathrm{Gal}(H_p/F) \cong G_p$. By our earlier reductions we can assume that $\chi$ is a faithful character of $G'$.

We recall the sets $\Sigma, \Sigma'$ defined in §4 and introduce the notation $\Sigma_p$. As usual $S_{\mathrm{ram}}$ denotes the set of finite primes of $F$ ramified in $H$.

$$\Sigma = \{v \in S_{\mathrm{ram}} \colon v \mid p\} \cup S_\infty, \tag{54}$$

$$\Sigma_p = \{v \in S_{\mathrm{ram}} \colon v \mid p \text{ and } \chi(G'_v) = 1\} \subset \Sigma, \tag{55}$$

$$\Sigma' = \{v \in S_{\mathrm{ram}} \colon v \nmid p\} \cup T. \tag{56}$$

In (55), $G'_v = G' \cap G_v$. Since $\chi$ is faithful, the condition $\chi(G'_v) = 1$ is equivalent to $G'_v = 1$, i.e. that $G_v$ is a $p$-group. The goal of this section is to prove the following:

**Theorem 5.1.** *Suppose that in every situation with notation as above, we have that the $R$-module $\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R$ is quadratically presented and that*

$$\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R) \subset (\Theta^{\#}_{\Sigma,\Sigma'}). \tag{57}$$

*Then each such inclusion is an equality.*

Note that our proof is inductive in nature, so we do not show directly that a single such inclusion is necessarily an equality; we show that if *every* such inclusion holds, then they are *all* equalities. For the remainder of this section, we assume that (57) always holds.

Recall the following exact sequence of $\mathcal{O}[G]$-modules (Lemma 3.1):

$$0 \longrightarrow Y_{H,\Sigma}^{-} \longrightarrow \mathrm{Sel}_\Sigma^{\Sigma'}(H)^{-} \longrightarrow \mathrm{Cl}^{\Sigma'}(H)^{\vee,-} \longrightarrow 0. \tag{58}$$

Note that $(Y_{H,\Sigma})_R \cong (Y_{H,\Sigma_p})_R$ since $(Y_{H,\{v\}})_R = 0$ when $\chi(G'_v) \neq 1$. In particular:

$$\text{if } \Sigma_p = \emptyset, \text{ then } \mathrm{Sel}_\Sigma^{\Sigma'}(H)_R \cong (\mathrm{Cl}^{\Sigma'}(H)^\vee)_R. \tag{59}$$

**Lemma 5.2.** *Let $\alpha$ be any character of $G'$. Denote by $\mathcal{O}_\alpha$ the ring $\mathcal{O}$ endowed with the $G'$-action in which $G'$ acts via $\alpha$. Write*

$$\mathrm{Cl}^{\Sigma'}(H)^\vee_{\mathcal{O}_\alpha} = \mathrm{Cl}^{\Sigma'}(H)^\vee \otimes_{\mathbf{Z}[G']} \mathcal{O}_\alpha.$$

*Let $H_\alpha$ denote the fixed field of the kernel of $\alpha$ in $G'$. Then*

$$\mathrm{Cl}^{\Sigma'}(H_\alpha)^\vee_{\mathcal{O}_\alpha} \cong \mathrm{Cl}^{\Sigma'}(H)^\vee_{\mathcal{O}_\alpha}$$

*Proof.* This follows because $[H : H_\alpha]$ is relatively prime to $p$. The maps

$$\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_H \qquad \text{and} \qquad \mathfrak{a} \mapsto \frac{1}{[H : H_\alpha]} \mathrm{N}_{H/H_\alpha}\mathfrak{a}$$

are explicit mutually inverse isomorphisms between $\mathrm{Cl}^{\Sigma'}(H_\alpha)_{\mathcal{O}_\alpha}$ and $\mathrm{Cl}^{\Sigma'}(H)_{\mathcal{O}_\alpha}$. The isomorphism in the lemma is the Pontryagin dual of this, with $\alpha$ replaced by $\alpha^{-1}$. □

The proof of Theorem 5.1 relies on the analytic class number formula, which manifests itself in the following lemma.

**Lemma 5.3.** *We have*

$$\#(\mathrm{Cl}^{\Sigma'}(H)^\vee)_R = \#\mathcal{O}/L,$$

*where*

$$L = L_{S_\infty,\Sigma'}(H/H_p, \chi, 0) = \prod_{\psi|_{G'}=\chi} L_{S_\infty,\Sigma'}(H/F, \psi, 0).$$

*Here the product runs over the characters $\psi$ of $G = \mathrm{Gal}(H/F)$ that belong to $\chi$.*

*Proof.* For the purposes of the first equality, we can work entirely over $H_p$, i.e. we can replace $F$ by $H_p$. Note that $H_p$ is totally real since its degree over $F$ is odd. For the extension $H/H_p$, the associated set $\Sigma_p$ is empty, since $G_v = G'_v$ and $\chi$ is faithful, so $\chi(G'_v) = 1$ implies that $G'_v = 1$ and hence $v$ is unramified (in fact totally split). In this setting the ring $R$ is just $\mathcal{O}_\chi$, i.e. the ring $\mathcal{O}$ in which the group $\mathrm{Gal}(H/H_p)$ acts via $\chi$. Therefore the running assumption (57) together with the isomorphism (59) yield

$$\mathrm{Fitt}_{\mathcal{O}_\chi}(\mathrm{Cl}^{\Sigma'}(H)^\vee_{\mathcal{O}_\chi}) \subset (L_{S_\infty,\Sigma'}(H/H_p,\chi,0)),$$

which says simply

$$\#\mathcal{O}/L_{S_\infty,\Sigma'}(H/H_p,\chi,0) \mid \#\,\mathrm{Cl}^{\Sigma'}(H)^\vee_{\mathcal{O}_\chi}.$$

We apply the same result to all odd characters $\alpha$ of $H/H_p$, to obtain

$$\#\mathcal{O}/L_{S_\infty,\Sigma'}(H/H_p,\alpha,0) \mid \#\,\mathrm{Cl}^{\Sigma'}(H_\alpha)^\vee_{\mathcal{O}_\alpha} = \#\,\mathrm{Cl}^{\Sigma'}(H)^\vee_{\mathcal{O}_\alpha}, \tag{60}$$

where the last equality uses Lemma 5.2. Taking the product over all $\alpha$ gives

$$\#\mathcal{O}/L_{S_\infty,\Sigma'}(H/H^+,\epsilon,0) \mid \#\,\mathrm{Cl}^{\Sigma'}(H)^{\vee,-}_{\mathcal{O}}, \tag{61}$$

where $H^+$ is the maximal totally real subfield of $H$, and $\epsilon$ is the nontrivial character of $\mathrm{Gal}(H/H^+)$. The left side of (61) uses the Artin formalism for $L$-functions, and the right side uses the fact that $\mathcal{O}[\mathrm{Gal}(H/H_p)]^-$ is the direct product of the $\mathcal{O}_\alpha$. Now, (61) is actually an equality by the analytic class number formula (Lemma 2.1). It follows that each divisibility (60) is an equality as well. This yields the first equality of the lemma, with $\alpha = \chi$. The second equality follows from the Artin formalism for $L$-functions. □

## 5.1 Base Case

The proof of Theorem 5.1 will proceed by an induction on $\#\Sigma_p$. We first handle the case that $\Sigma_p$ is empty. Note that in this case, the image of $\Theta_{\Sigma,\Sigma'}$ is a non-zerodivisor in $R$. The fact that $\mathrm{Sel}^{\Sigma'}_\Sigma(H)_R$ is quadratically presented together with the inclusion (57) imply that we may write

$$\mathrm{Fitt}_R(\mathrm{Sel}^{\Sigma'}_\Sigma(H)_R) = (x \cdot \Theta^\#_{\Sigma,\Sigma'})$$

for some $x \in R$. By (59), which applies since $\Sigma_p = \emptyset$, this reads

$$\mathrm{Fitt}_R(\mathrm{Cl}^{\Sigma'}(H)^\vee_R) = (x \cdot \Theta^\#_{\Sigma,\Sigma'}).$$

Lemmas 2.4 and 2.5 imply that

$$\#\,\mathrm{Cl}^{\Sigma'}(H)^\vee_R = \#\mathcal{O}/\prod_{\psi|_{G'}=\chi} \psi(x) L_{\Sigma,\Sigma'}(H/F,\psi,0). \tag{62}$$

Yet

$$L_{\Sigma,\Sigma'}(H/F,\psi,0) = L_{S_\infty,\Sigma'}(H/F,\psi,0) \prod_{v\in\Sigma-S_\infty}(1-\psi(v)). \tag{63}$$

Since $\Sigma_p = \emptyset$, any $v \in \Sigma - S_\infty$ satisfies

$$\begin{cases} \psi(v) = 0 & \text{if } \psi \text{ is ramified at } v, \\ \psi(v) \equiv \chi(v) \not\equiv 1 \pmod{\pi_E} & \text{if } \psi \text{ is unramified at } v. \end{cases}$$

Here $\pi_E \in \mathcal{O}$ is a uniformizer. It follows that the product on the right in (63) is a $p$-adic unit. Hence Lemma 5.3 and (62) imply that $\prod \psi(x) \in \mathcal{O}^*$. Therefore each $\psi(x) \in \mathcal{O}^*$, which implies that $x \in R^*$ since the $\mathcal{O}$-algebra maps $R \longrightarrow \mathcal{O}$ induced by each character $\psi$ are local homomorphisms of local rings. This is the desired result.

## 5.2 Strategy of Inductive Step

Now consider the case of $\Sigma_p$ nonempty. As in §5.1, the inclusion (57) implies that the principal ideal $\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R)$ is generated by an element of the form $x \cdot \Theta^{\#}_{\Sigma,\Sigma'}$ for some $x \in R$. We must show that $x$ is a unit in $R$.

The equality $\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R) = (x \cdot \Theta^{\#}_{\Sigma,\Sigma'})$ implies that for all characters $\psi$ of $G$ that belong to $\chi$, we have

$$\mathrm{Fitt}_{\mathcal{O}}(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_\psi) = (\psi(x) \cdot L_{\Sigma,\Sigma'}(\psi,0)) \subset (L_{\Sigma,\Sigma'}(\psi,0)). \tag{64}$$

Note here that

$$\begin{aligned} \mathrm{Sel}_\Sigma^{\Sigma'}(H)_\psi &:= \mathrm{Sel}_\Sigma^{\Sigma'}(H) \otimes_{\mathbf{Z}[G]} \mathcal{O}_\psi \\ &= (\mathrm{Sel}_\Sigma^{\Sigma'}(H) \otimes_{\mathbf{Z}} \mathcal{O})/\langle g - \psi(g) \colon g \in G\rangle \end{aligned}$$

denotes the $\psi$-coinvariants of $\mathrm{Sel}_\Sigma^{\Sigma'}(H)$. Suppose we can prove that the inclusion in (64) is an equality for some $\psi$ that belongs to $\chi$ satisfying $L_{\Sigma,\Sigma'}(\psi,0) \neq 0$. This implies that $\psi(x) \in \mathcal{O}^*$, which implies $x \in R^*$, giving the desired result

$$\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R) = (\Theta^{\#}_{\Sigma,\Sigma'}).$$

Now if *every* character $\psi$ belonging to $\chi$ has a trivial zero (i.e. if for each $\psi$ there exists $v \in \Sigma$ with $\psi(G_v) = 1$, so $L_{\Sigma,\Sigma'}(\psi,0) = 0$) then Lemma 3.2 shows that

$$\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R) = 0 = (\Theta^{\#}_{\Sigma,\Sigma'}),$$

again giving the desired result. It therefore suffices to prove that

$$\mathrm{Fitt}_{\mathcal{O}}(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_\psi) = (L_{\Sigma,\Sigma'}(\psi,0)) \tag{65}$$

for every character $\psi$ belonging to $\chi$. We do this in two cases, depending on whether or not $\psi$ is ramified at all places in $\Sigma_p$. In both cases we need the following lemma.

**Lemma 5.4.** *Let $H_\psi \subset H$ denote the subfield of $H$ fixed by the kernel of $\psi$. There is a canonical isomorphism* $\mathrm{Sel}_\Sigma^{\Sigma'}(H)_\psi \cong \mathrm{Sel}_\Sigma^{\Sigma'}(H_\psi)_\psi$.

*Proof.* The proof is nearly identical to Lemma 4.2, replacing $(H_\chi, R)$ with $(H_\psi, \mathcal{O}_\psi)$. We omit the details. □

Since it remains only to prove (65), Lemma 5.4 implies that we may replace $H$ by $H_\psi$ and hence assume $H = H_\psi$ for the remainder of the proof.

## 5.3 Characters unramified at some place in $\Sigma_p$

Let $\psi$ be a character belonging to $\chi$, and suppose that there exists a prime $v \in \Sigma_p$ such that $\psi$ is unramified at $v$. We will prove (65). Let $\Sigma_p^v = \Sigma_p - \{v\}$ and $\Sigma^v = \Sigma - \{v\}$. Since $H_\psi$ is unramified at $v$, the sets $\Sigma^v, \Sigma'$ satisfy the necessary conditions for $H_\psi/F$ and hence by induction (recall we are inducting on $\#\Sigma_p$) we obtain that

$$\mathrm{Fitt}_R(\mathrm{Sel}_{\Sigma^v}^{\Sigma'}(H_\psi)_R) = (\Theta^{\#}_{\Sigma^v,\Sigma'}). \tag{66}$$

There is a short exact sequence of $\mathcal{O}[\mathrm{Gal}(H_\psi/F)]$-modules

$$0 \longrightarrow Y_{H_\psi,\{v\}} \longrightarrow \mathrm{Sel}_\Sigma^{\Sigma'}(H_\psi) \longrightarrow \mathrm{Sel}_{\Sigma_v}^{\Sigma'}(H_\psi) \longrightarrow 0. \tag{67}$$

Note that since $v$ is unramified in $H_\psi/F$, we have

$$\mathrm{Fitt}_R((Y_{H_\psi,\{v\}})_R) = (1 - \sigma_v). \tag{68}$$

Lemma 2.6 applied to the base change of (67) to $R$, combined with (66) and (68) yields

$$\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H_\psi)_R) = (\Theta^{\#}_{\Sigma^v,\Sigma'})(1 - \sigma_v) = (\Theta^{\#}_{\Sigma,\Sigma'}).$$

Passing to the $\mathcal{O}_\psi$-quotient yields the desired equality (65).

## 5.4 Characters ramified at all places in $\Sigma_p$

Next we consider the more difficult case that $\psi$ is ramified at all primes in $\Sigma_p$. In this case, the induction hypothesis is of little use since we cannot remove any primes from $\Sigma_p$. We prove (65) directly.

The extension $H_\psi/F$ is cyclic. Each $v \in \Sigma_p$ satisfies $\psi(G'_v) = \chi(G'_v) = 1$, hence the decomposition group of $v$ in $\mathrm{Gal}(H_\psi/F)$ is a $p$-group. Therefore there exists a $v \in \Sigma_p$ whose inertia group $I_v$ is minimal in the sense that $I_v \subset I_w$ for all $w \in \Sigma_p$, since the subgroups of a cyclic $p$-group are linearly ordered by inclusion. We write $I$ for this minimal $I_v$. The fact that $\psi$ is ramifed at all $v \in \Sigma_p$ and $\Sigma_p$ is nonempty implies that $I \neq 1$.

**Lemma 5.5.** *With notation as above, we have* $\mathrm{Sel}_\Sigma^{\Sigma'}(H_\psi)_R/\mathrm{N}I \cong (\mathrm{Cl}^{\Sigma'}(H_\psi)^\vee)_R/\mathrm{N}I$.

*Proof.* Denote by $\Sigma_{H_\psi}$ the set of places of $H_\psi$ above those in $\Sigma$. First note that from the short exact sequence

$$0 \longrightarrow Y_{H_\psi,\Sigma-\Sigma_p} \longrightarrow \mathrm{Sel}_{\Sigma}^{\Sigma'}(H_\psi) \longrightarrow \mathrm{Sel}_{\Sigma_p}^{\Sigma'}(H_\psi) \longrightarrow 0$$

it follows that

$$\mathrm{Sel}_{\Sigma}^{\Sigma'}(H_\psi)_R \cong \mathrm{Sel}_{\Sigma_p}^{\Sigma'}(H_\psi)_R.$$

Indeed, any place $w \in (\Sigma - \Sigma_p)_{H_\psi}$ has image in $(Y_{H_\psi,\Sigma-\Sigma_p})_R$ that vanishes (if $\sigma \in G'_v$ with $\chi(\sigma) \neq 1$, then $1-\sigma$ acts trivially on the image of $w$ in $Y_{H_\psi,\Sigma-\Sigma_p}$ and has image in $R$ that is a unit).

It therefore suffices to prove the result with $\Sigma$ replaced by $\Sigma_p$. For this, we tensor the exact sequence (58) with $R/\mathrm{N}I$ over $R$. We need to show that the image of

$$(Y_{H_\psi,\Sigma_p})_R/\mathrm{N}I \longrightarrow \mathrm{Sel}_{\Sigma_p}^{\Sigma'}(H_\psi)_R/\mathrm{N}I$$

vanishes. We will show that this already holds on the full minus side over $\mathbf{Z}[1/2]$ (without passing to the $R$-component), i.e. that

$$Y^-_{H_\psi,\Sigma_p}/\mathrm{N}I \longrightarrow \mathrm{Sel}_{\Sigma_p}^{\Sigma'}(H_\psi)^-/\mathrm{N}I \tag{69}$$

vanishes.

Define $M = \mathrm{Cl}^{\Sigma'}(H_\psi)^-/\mathrm{N}I$. The primes $\mathfrak{P} \in (\Sigma_p)_{H_\psi}$ come in pairs $(\mathfrak{P}, \overline{\mathfrak{P}})$ that are associated by complex conjugation, with $\mathfrak{P} \neq \overline{\mathfrak{P}}$ since $\chi(G'_v) = 1$ while $\chi$ is odd. We choose a representative $\mathfrak{P}$ for each pair and denote this set of representatives by $J$. Let $e = \#I$. We claim that the images of $\mathfrak{P}/\overline{\mathfrak{P}}$ are "linearly independent modulo $e$" in $M$, in the following sense:

$$\text{if } \prod_{\mathfrak{P}\in J} (\mathfrak{P}/\overline{\mathfrak{P}})^{a_\mathfrak{P}} \text{ has trivial image in } M, \text{ then } e \mid a_\mathfrak{P} \text{ for all } \mathfrak{P}.$$

To see this, suppose that

$$\prod_{\mathfrak{P}\in J} (\mathfrak{P}/\overline{\mathfrak{P}})^{a_\mathfrak{P}} = (x)\mathfrak{a}^{\mathrm{N}I} \tag{70}$$

for some $x \in H^{*,-}_{\psi,\Sigma'}$ and some fractional ideal $\mathfrak{a} \in I_{\Sigma'}(H_\psi)^-$. Then all items in (70) are invariant under all $\sigma \in I$ except possibly the fractional ideal $(x)$, which implies that $(x)$ is invariant as well; since the generator in $H^{*,-}_{\psi,\Sigma'}$ of a principal ideal on the minus side (i.e. in $I_{\Sigma'}(H_\psi)^-$) is unique, this implies that $x \in (H^I_\psi)^*_{\Sigma'}$. But the ideals $\mathfrak{P}$ are totally ramified over $H^I_\psi$, and hence the valuations of $x$ at these primes must be multiples of $e$; it follows that the $a_\mathfrak{P}$ are multiples of $e$ as well.

Now fix one of the $\mathfrak{P} \in J$. We will show that the image of $\mathrm{ord}_\mathfrak{P} - \mathrm{ord}_{\overline{\mathfrak{P}}}$ in $\mathrm{Sel}_{\Sigma_p}^{\Sigma'}(H_\psi)^-$ is a multiple of $\mathrm{N}I$; this is precisely the desired result that (69) vanishes. The claim just proven

implies that there is a group homomorphism $\tilde{\phi}\colon M \longrightarrow \mathbf{Q}/\mathbf{Z}[\frac{1}{2}]$ such that $\tilde{\phi}(\mathfrak{P} - \overline{\mathfrak{P}}) = 1/e$ and $\tilde{\phi}(\mathfrak{P}' - \overline{\mathfrak{P}}') = 0$ for all $\mathfrak{P}' \in J, \mathfrak{P}' \neq \mathfrak{P}$. Considering $M$ as the quotient:

$$M = I_{\Sigma'}(H_\psi)^- / \langle H^{*,-}_{\psi,\Sigma'}, \mathrm{N}I \cdot I_{\Sigma'}(H_\psi)^- \rangle,$$

we can lift $\tilde{\phi}$ to a $\mathbf{Z}[\frac{1}{2}]$-module homomorphism $\phi\colon I_{\Sigma'}(H_\psi)^- \longrightarrow \mathbf{Q}$, since $I_{\Sigma'}(H_\psi)^-$ is free as a $\mathbf{Z}[\frac{1}{2}]$-module. Furthermore we can choose this lift to satisfy $\phi(\mathfrak{P} - \overline{\mathfrak{P}}) = 1/e$ and $\phi(\mathfrak{P}' - \overline{\mathfrak{P}}') = 0$ for all $\mathfrak{P}' \in J, \mathfrak{P}' \neq \mathfrak{P}$. The restriction of $\phi$ to $H^{*,-}_{\psi,\Sigma'}$ is $\mathbf{Z}[\frac{1}{2}]$-valued (since this group has trivial image in $M$), and hence yields a class $\Phi \in \mathrm{Sel}^{\Sigma'}_{\Sigma_p}(H_\psi)^-$ defined explicitly by

$$\Phi = \sum_{w \notin \Sigma'_{H_\psi}} \phi(w) \operatorname{ord}_w .$$

To conclude the proof, we will show that $\operatorname{ord}_{\mathfrak{P}} - \operatorname{ord}_{\overline{\mathfrak{P}}}$ and $\mathrm{N}I \cdot \Phi$ are equal in $\mathrm{Sel}^{\Sigma'}_{\Sigma}(H_\psi)^-$. From the construction of $\phi$, we see that

$$\Phi = \frac{1}{e}(\operatorname{ord}_{\mathfrak{P}} - \operatorname{ord}_{\overline{\mathfrak{P}}}) + \sum_{w \notin (\Sigma_p \cup \Sigma')_{H_\psi}} \phi(w) \operatorname{ord}_w$$

and hence

$$\begin{aligned} \mathrm{N}I \cdot \Phi &= (\operatorname{ord}_{\mathfrak{P}} - \operatorname{ord}_{\overline{\mathfrak{P}}}) + \mathrm{N}I \sum_{w \notin (\Sigma_p \cup \Sigma')_{H_\psi}} \phi(w) \operatorname{ord}_w \\ &= (\operatorname{ord}_{\mathfrak{P}} - \operatorname{ord}_{\overline{\mathfrak{P}}}) + \sum_{w \notin (\Sigma_p \cup \Sigma')_{H_\psi}} \phi(\mathrm{N}I \cdot w) \operatorname{ord}_w . \end{aligned} \tag{71}$$

Since $\phi \circ \mathrm{N}I$ is $\mathbf{Z}[\frac{1}{2}]$-valued by the definition of $M$, the sum on the right in (71) has trivial image in $\mathrm{Sel}^{\Sigma'}_{\Sigma_p}(H_\psi)^-$, by the definition of this group. The result follows. □

**Lemma 5.6.** *The size of the group* $(\mathrm{Cl}^{\Sigma'}(H_\psi)_R)^\vee / \mathrm{N}I$ *is* $\#\mathcal{O}/L_I$*, where*

$$L_I = \prod_{\substack{\alpha(I) \neq 1 \\ \alpha|_{G'} = \chi}} L_{\Sigma,\Sigma'}(H_\psi/F, \alpha, 0).$$

*Here the product ranges over all characters* $\alpha$ *of* $\mathrm{Gal}(H_\psi/F)$ *that belong to* $\chi$ *such that* $\alpha(I) \neq 1$*.*

*Proof.* Note that in the definition of $L_I$, each character $\alpha$ is ramified at every $v \in \Sigma_p$, while the Euler factor $(1 - \alpha(v))$ is a $p$-adic unit for each finite $v \in \Sigma - \Sigma_p$, hence

$$L_{\Sigma,\Sigma'}(H_\psi/F, \alpha, 0) = L_{S_\infty,\Sigma'}(H_\psi/F, \alpha, 0).$$

For notational simplicity, write $M = \mathrm{Cl}^{\Sigma'}(H_\psi)_R$. By Lemma 5.3, we have $\#M^\vee = \mathcal{O}/L$, where

$$L = \prod_{\alpha|_{G'}=\chi} L_{S_\infty,\Sigma'}(H_\psi/F, \alpha, 0).$$

We therefore need to prove that

$$\#(\mathrm{N}I \cdot M^\vee) = \mathcal{O}/L'_I, \tag{72}$$

where

$$L'_I = \prod_{\substack{\alpha(I)=1 \\ \alpha|_{G'}=\chi}} L_{S_\infty,\Sigma'}(H_\psi/F, \alpha, 0) \tag{73}$$

$$= \prod_{\substack{\alpha\in \mathrm{Gal}(H_\psi^I/F)\hat{} \\ \alpha|_{G'}=\chi}} L_{S_\infty,\Sigma'}(H_\psi^I/F, \alpha, 0). \tag{74}$$

First note that we can replace $M^\vee$ by $M$ in (72) since $M$ is finite; indeed, from the exact sequence

$$0 \longrightarrow M^\vee[\mathrm{N}I] \longrightarrow M^\vee \xrightarrow{\mathrm{N}I} M^\vee \longrightarrow M^\vee/\mathrm{N}I \longrightarrow 0$$

we see that

$$\#M^\vee/\mathrm{N}I = \#M^\vee[\mathrm{N}I] = \#(M/\mathrm{N}I)^\vee = \#(M/\mathrm{N}I)$$

and hence $\#(\mathrm{N}I \cdot M^\vee) = \#(\mathrm{N}I \cdot M)$. Our goal is therefore to prove that

$$\#(\mathrm{N}I \cdot M) = \mathcal{O}/L'_I. \tag{75}$$

Next note that if $N = \mathrm{Cl}^{\Sigma'}(H_\psi^I)_R$, then Lemma 5.3 and (74) imply that

$$\#N = \#\mathcal{O}/L'_I. \tag{76}$$

In view of (75) and (76), it suffices to prove that the canonical map $N \longrightarrow M^I$ given by extension of ideals is an injection that identifies $N$ with $\mathrm{N}I \cdot M$.

For the injectivity one applies the snake lemma to the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (H^{I,*}_{\psi,\Sigma'})_R & \longrightarrow & I_{\Sigma'}(H_\psi^I)_R & \longrightarrow & N & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathfrak{a}\mapsto\mathfrak{a}\mathcal{O}_{H_\psi}} & & \downarrow & & \\
0 & \longrightarrow & (H^*_{\psi,\Sigma'})^I_R & \longrightarrow & I_{\Sigma'}(H_\psi)^I_R & \longrightarrow & M^I & \longrightarrow & 0
\end{array}$$

(Note that the 0 on the bottom right comes from Hilbert's Theorem 90, though it is not necessary here.) The left vertical arrow is an isomorphism by Galois theory, and the middle vertical arrow is clearly an injection. It follows that $N \longrightarrow M^I$ is injective.

To conclude we must show that the norm map $M \longrightarrow N$ is surjective. This follows crucially because we are working on the minus side. There is a commutative diagram

$$\begin{array}{ccc} (C_{H_\psi})_R & \twoheadrightarrow & M \\ \downarrow & & \downarrow \\ (C_{H_\psi^I})_R & \twoheadrightarrow & N \end{array}$$

where $C_H = \mathbf{A}_H^*/H^*$ is the idèle class group of $H$ and both vertical arrows are given by norm maps. It suffices to show that the left vertical map is surjective. Noting that $(C_{H_\psi^I})_R = (C_{H_\psi})_R^I$ by Hilbert's Theorem 90, this surjectivity is equivalent to the statement

$$\hat{H}^0(I, (C_{H_\psi})_R) = 0$$

in Tate cohomology. The calculation of the Tate cohomology of idèle class groups is a fundamental result in Class Field Theory (see [8, Chapter VII, pg. 197]); one has $\hat{H}^0(I, C_{H_\psi}) \cong I$ with $G$ acting trivially. The projection to the $R$ component is therefore trivial, as complex conjugation acts as $-1$ on $R$. The desired result $\hat{H}^0(I, (C_{H_\psi})_R) = 0$ follows, completing the proof. □

We can now apply an analytic argument similar to §5.1 to conclude this case.

**Lemma 5.7.** *Let $R_I = R/\mathrm{N}I$. We have* $\mathrm{Fitt}_{R_I}(\mathrm{Sel}_\Sigma^{\Sigma'}(H_\psi)_{R_I}) = (\Theta_{\Sigma,\Sigma'}^{\#})$.

*Proof.* Projecting (57) from $R$ to $R_I$ we obtain an inclusion

$$\mathrm{Fitt}_{R_I}(\mathrm{Sel}_\Sigma^{\Sigma'}(H_\psi)_{R_I}) \subset (\Theta_{\Sigma,\Sigma'}^{\#}).$$

Note that by Corollary 2.3, the ring $R_I$ is a character-group ring and hence we may apply Lemmas 2.4 and 2.5. If we write $\mathrm{Fitt}_{R_I}(\mathrm{Sel}_\Sigma^{\Sigma'}(H_\psi)_{R_I}) = (x \cdot \Theta_{\Sigma,\Sigma'}^{\#})$ for some $x \in R_I$, then these lemmas imply that

$$\#\,\mathrm{Sel}_\Sigma^{\Sigma'}(H_\psi)_{R_I} = \#\mathcal{O}/\prod_{\substack{\alpha(I)\neq 1 \\ \alpha|_{G'}=\chi}} \alpha(x) L_{\Sigma,\Sigma'}(H_\psi/F, \alpha, 0).$$

Combining this equality with Lemmas 5.5 and 5.6 we find that

$$\prod_{\substack{\alpha(I)\neq 1 \\ \alpha|_{G'}=\chi}} \alpha(x) \in \mathcal{O}^*,$$

and therefore each $\alpha(x) \in \mathcal{O}^*$. This implies $x \in R_I^*$ as desired. □

Projecting the equality of Lemma 5.7 to $\mathcal{O}_\psi$, we obtain (65). We have now completed the proof of Theorem 5.1.

**Remark 5.8.** The remainder of the paper is dedicated to proving the desired inclusion

$$\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R) \subset (\Theta^{\#}_{\Sigma,\Sigma'}).$$

We assume from here on that the image of $\Theta^{\#}_{\Sigma,\Sigma'}$ in $R$ lies in the maximal ideal $\mathfrak{m}_R$. Otherwise, it is a unit in $R$ and the desired inclusion holds trivially.

# 6 The module $\nabla$ and its key properties

The module that appears in our constructions with Hilbert modular forms is not the Selmer module $\mathrm{Sel}_\Sigma^{\Sigma'}(H)$ but a certain canonical transpose in the sense of Jannsen [24]. In this section we state the salient properties of this module, denoted $\nabla_\Sigma^{\Sigma'} = \nabla_\Sigma^{\Sigma'}(H)$. The actual construction of $\nabla_\Sigma^{\Sigma'}$ and details of the proofs are relegated to the appendix.

In the appendix, we work work with general disjoint finite sets $\Sigma$, $\Sigma'$ of places of $F$ such that $\Sigma \supset S_\infty$ and $\Sigma'$ satisfies condition (1) of the introduction. In this section we specialize to the sets $\Sigma$ and $\Sigma'$ defined in (54) and (56). The Ritter–Weiss module $\nabla_\Sigma^{\Sigma'}$ associated to these sets $\Sigma, \Sigma'$ satisfies the following properties.

(P1) There is a short exact sequence of $\mathbf{Z}[G]$-modules

$$0 \longrightarrow \mathrm{Cl}_\Sigma^{\Sigma'}(H) \longrightarrow \nabla_\Sigma^{\Sigma'} \longrightarrow X_{H,\Sigma} \longrightarrow 0. \tag{77}$$

(P2) After tensoring with $\mathbf{Z}[\frac{1}{2}]$ and passing to minus parts, the extension class associated to

$$0 \longrightarrow \mathrm{Cl}_\Sigma^{\Sigma'}(H)^- \longrightarrow \nabla_\Sigma^{\Sigma',-} \longrightarrow X_{H,\Sigma}^- \longrightarrow 0 \tag{78}$$

in

$$\mathrm{Ext}^1_{\mathbf{Z}[G]^-}(X_{H,\Sigma}^-, \mathrm{Cl}_\Sigma^{\Sigma'}(H)^-) \cong \bigoplus_{v\in\Sigma} H^1(G_v, \mathrm{Cl}_\Sigma^{\Sigma'}(H)^-) \tag{79}$$

is equal to a certain tuple of canonical Galois cohomology classes $(\lambda_v)_{v\in\Sigma}$ defined below using class field theory (the isomorphism (79) is explained in (83) below).

To obtain further desired properties, we must base change to $\mathbf{Z}_p$ and consider

$$(\nabla_\Sigma^{\Sigma'})_p = \nabla_\Sigma^{\Sigma'} \otimes \mathbf{Z}_p.$$

(P3) The $\mathbf{Z}_p[G]$-module $(\nabla_\Sigma^{\Sigma'})_p$ has a canonical transpose $(\nabla_\Sigma^{\Sigma'})_p^{\mathrm{tr}}$ that is isomorphic to the Selmer module $\mathrm{Sel}_\Sigma^{\Sigma'}(H)_p$ defined in §3.1.

(P4) The $\mathbf{Z}_p[G]$-module $(\nabla_\Sigma^{\Sigma'})_p$ is quadratically presented.

While most of the content of our construction is contained in the work of Ritter–Weiss [40] and Burns–Kurihara–Sano [5], the construction of our precise module $\nabla_\Sigma^{\Sigma'}$ satisfying properties (P1)–(P4) does not seem to be present in the literature. For instance, Ritter and Weiss do not consider the "smoothing" set $\Sigma'$. As a result they obtain a presentation $P_1 \longrightarrow P_0 \longrightarrow \nabla_\Sigma \longrightarrow 0$ where $P_1$ is projective, but $P_0$ is only cohomologically trivial. Furthermore, they do not consider properties (P2) and (P3) in the form that we need. Meanwhile Burns–Kurihara–Sano define a Selmer module $\mathrm{Sel}_\Sigma^{\Sigma'}(H)^{\mathrm{tr}}$ satisfying properties (P1) and (P3), however (P4) is proved only in the case $\Sigma \supset S_{\mathrm{ram}}$, and property (P2) is not considered.

For these reasons, we describe the construction of $\nabla_\Sigma^{\Sigma'}$ and the proof of properties (P1)–(P4) in detail. This construction, which draws heavily from [40], is described in the appendix and may be of independent interest beyond our applications in this paper. Our construction is closely related to that of Nickel in [33, §2.3]. In the remainder of this section we elaborate on the statement of properties (P2) and (P3).

## 6.1 Transpose

In this section we describe property (P3). For any $\mathbf{Z}[G]$-module $M$, we endow the dual $M^* := \mathrm{Hom}_{\mathbf{Z}[G]}(M, \mathbf{Z}[G])$ with the contragradient action

$$(r \cdot \varphi)(x) := \varphi(r^\# \cdot x), \qquad \text{for } r \in \mathbf{Z}[G], \varphi \in M^*, x \in M. \tag{80}$$

Suppose that $M$ has a presentation by projective $\mathbf{Z}[G]$-modules of finite rank

$$P_0 \longrightarrow P_1 \longrightarrow M \longrightarrow 0. \tag{81}$$

Then each of the modules $P_i^*$ is also projective, and following Jannsen [24] we call the cokernel of the induced map $P_1^* \longrightarrow P_0^*$ a *transpose* of the module $M$. Transpose is only well-defined up to homotopy: if $M'$ and $M''$ are transposes of $M$ arising from different presentations, then there exist projective modules $P$ and $Q$ such that $M' \oplus P \cong M'' \oplus Q$.

Let $R = R_\Psi$ be a character group ring associated to a set $\Psi \subset \hat{G}$. We define $R^\# = R_{\Psi^\#}$, where $\Psi^\# = \{\psi^{-1} \colon \psi \in \Psi\}$. The involution $\#$ on $\mathcal{O}[G]$ induces mutually inverse $\mathcal{O}$-algebra maps $\#\colon R \longrightarrow R^\#, R^\# \longrightarrow R$. If $M$ is an $R$-module, it is then natural to view $M^*$ as an $R^\#$-module via the rule (80). The transpose of $M$ with respect to a projective presentation (81) also naturally has the structure of an $R^\#$-module.

**Lemma 6.1.** *Let $R$ be a character group ring and suppose that $M$ is a quadratically presented $R$-module. Let $M^{\mathrm{tr}}$ be the transpose of $M$ associated with any quadratic presentation of $M$. Then $M^{\mathrm{tr}}$ is quadratically presented and* $\mathrm{Fitt}_{R^\#}(M^{\mathrm{tr}}) = \mathrm{Fitt}_R(M)^\#$.

*Proof.* If $(a_{ij})$ is the square matrix representing a quadratic presentation of $M$ over $R$, then the matrix representing the corresponding quadratic presentation of $M^{\mathrm{tr}}$ over $R^\#$ is $(a_{ji}^\#)$. The result follows. □

In view of (P3) and (P4), if $R$ is any character group ring quotient of $\mathcal{O}[G]$, we have:

**Corollary 6.2.** *The $R$-module $\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R$ has a quadratic presentation. Its Fitting ideal over $R$ is principal and satisfies*

$$\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R) = \mathrm{Fitt}_{R^\#}(\nabla_\Sigma^{\Sigma'}(H)_{R^\#})^\#.$$

Note that Corollary 6.2 was proved in [5, Lemma 2.8] in the case that $\Sigma \supset S_{\mathrm{ram}}$.

## 6.2 Extension class via Galois cohomology

In this section we describe property (P2). This is a description of the module $\nabla_\Sigma^{\Sigma'}(H)$, when projected to the minus side, in terms of a certain canonical Galois cohomology class arising from class field theory. For the remainder of this section we therefore work over $\mathbf{Z}[\frac{1}{2}]$. Let $M = \mathrm{Cl}_\Sigma^{\Sigma'}(H)^-$, and let $L/H$ denote the abelian extension corresponding via class field theory to the group $M$. This is the maximal abelian extension of $H$ of odd degree that is unramified outside places in $\Sigma'_H$ and at most tamely ramified at $\Sigma'_H$, such that the primes in $\Sigma_H$ split completely, and such that the conjugation action of complex conjugation on $\mathrm{Gal}(L/H)$ is inversion. The extension $L/F$ is Galois, as can be seen from this description since the action of any $\sigma \in G_F$ sends $L$ to another field with these properties. The lemma below shows that the short exact sequence of groups

$$1 \longrightarrow M \longrightarrow \mathrm{Gal}(L/F) \longrightarrow G \longrightarrow 1$$

splits (i.e. is a semi-direct product). For this, it is crucial that we are working on the minus side.

**Lemma 6.3.** *Let $N$ be any $\mathbf{Z}[G]^-$-module, e.g. the module $M$ above. The restriction map*

$$\mathrm{res}_{G_H}^{G_F} \colon H^1(G_F, N) \longrightarrow H^1(G_H, N)^G$$

*is an isomorphism.*

*Proof.* The terms preceding and following the map $\mathrm{res}_{G_H}^{G_F}$ in the inflation-restriction sequence are $H^i(G, N)$ for $i = 1, 2$. Yet $H^i(G, N) = 0$ for all $i$. To see this vanishing, note that the action of any $g \in G$ gives a $G$-module map $N \longrightarrow N$ that induces the identity on cohomology (see [8, Proposition 3, pg. 99]); but complex conjugation acts on $N$ as multiplication by $-1$. Since 2 has been inverted, this implies that $H^i(G, N) = 0$ as claimed. □

Let

$$\mathrm{rec}_{L/H} \colon M \xrightarrow{\sim} \mathrm{Gal}(L/H)$$

denote the Artin reciprocity isomorphism. Lemma 6.3 implies that there is a unique cohomology class

$$\lambda \in H^1(G_F, M)$$

whose restriction to $H^1(G_H, M) = \mathrm{Hom}_{\mathrm{cont}}(G_H, M)$ is equal to the canonical homomorphism

$$\varpi\colon G_H \longrightarrow \mathrm{Gal}(L/H) \xrightarrow{\mathrm{rec}_{L/H}^{-1}} M.$$

An explicit formula for a cocycle representing $\lambda$ is given in §A.5.

Let $v \in \Sigma$ and denote by $G_{F,v} \subset G_F$ the decomposition group of $v$ associated to some embedding $\overline{F} \subset \overline{F}_v$. The restriction of $\lambda$ to $G_{H,v} = G_{F,v} \cap G_H$ is the restriction of $\varpi$ to a decomposition group of a prime of $H$ above $v$, and hence trivial by the definition of $M$. It follows from the inflation-restriction sequence that $\mathrm{res}^{G_F}_{G_{F,v}} \lambda$ is the inflation of a unique class

$$\lambda_v \in H^1(G_v, M). \tag{82}$$

Next we note that

$$X^-_{H,\Sigma} \cong Y^-_{H,\Sigma} = \bigoplus_{v\in\Sigma} (\mathrm{Ind}^G_{G_v} \mathbf{Z})^-.$$

Therefore

$$\begin{aligned}
\mathrm{Ext}^1_{\mathbf{Z}[G]^-}(X^-_{H,\Sigma}, M) &\cong \bigoplus_{v\in\Sigma} \mathrm{Ext}^1_{\mathbf{Z}[G]^-}((\mathrm{Ind}^G_{G_v} \mathbf{Z})^-, M) \\
&\cong \bigoplus_{v\in\Sigma} \mathrm{Ext}^1_{\mathbf{Z}[1/2][G_v]}(\mathbf{Z}[\tfrac{1}{2}], M) \\
&\cong \bigoplus_{v\in\Sigma} H^1(G_v, M).
\end{aligned} \tag{83}$$

Let us make explicit how one associates a class in $H^1(G_v, M)$ to the extension $\nabla_\Sigma^{\Sigma',-}$ using the chain of isomorphisms (83). Let $w \in \Sigma_H$ lie over the place $v \in \Sigma$, and consider the element $\frac{1}{2}(w - \overline{w}) \in X^-_{H,\Sigma}$, where $\overline{w}$ denotes the image of $w$ under complex conjugation. Let $x$ denote a lift of this element to $\nabla_\Sigma^{\Sigma',-}$ under the surjection given by (78). For any $g \in G_v$ we define

$$\gamma_v(g) = gx - x \in M. \tag{84}$$

This defines a cocycle representing a class in $H^1(G_v, M)$ that does not depend on the choice of $x$. The tuple $(\gamma_v)_{v\in\Sigma}$ is associated to $\nabla_\Sigma^{\Sigma',-}$ under (83).

In §A.5 we prove the following characterization of the Selmer module $\nabla_\Sigma^{\Sigma',-}$.

**Lemma 6.4.** *Under the isomorphism (83), the extension class in* $\mathrm{Ext}^1_{\mathbf{Z}[G]^-}(X^-_{H,\Sigma}, M)$ *determined by* $\nabla_\Sigma^{\Sigma',-}$ *corresponding to the minus part of the exact sequence (77) is equal to the tuple of canonical classes* $(\lambda_v)_{v\in\Sigma}$ *defined in (82).*

# 7 Group ring valued Hilbert Modular Forms

In the remainder of the paper, we will use Ribet's method in the context of group ring valued Hilbert modular forms to prove the inclusion

$$\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R) \subset (\Theta^\#), \qquad \Theta = \Theta_{\Sigma,\Sigma'},$$

from which all of our main theorems were deduced. Here $R = \mathcal{O}[G_p]_\chi$ is the component of $\mathcal{O}[G]$ corresponding to the totally odd character $\chi$.

## 7.1 Replacing $R$ by its trivial zero free quotient

In our constructions it will be convenient if $\Theta^\#$ is a non-zerodivisor in $R$. In the present context, this may not be the case. Indeed, if there is a character $\psi$ of $G$ belonging to $\chi$ and an element $v \in \Sigma$ such that $\psi(v) = 1$, then the associated $L$-function has a trivial zero: $L_{\Sigma,\Sigma'}(\psi, 0) = 0$. To deal with this, we will replace the component $\mathcal{O}[G_p]_\chi$ with its quotient $R_\Psi$, the character group ring corresponding to characters $\psi$ without a trivial zero:

$$\Psi = \{\psi \in \hat{G} \colon \psi|_{G'} = \chi, \psi(v) \neq 1 \text{ for all } v \in \Sigma\}.$$

We show it suffices to consider this quotient.

**Lemma 7.1.** *Let $R = \mathcal{O}[G_p]_\chi$, and let $R_\Psi$ be the character group ring quotient of $R$ associated to the set $\Psi$ above. Suppose that*

$$\mathrm{Fitt}_{R_\Psi}(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_{R_\Psi}) \subset (\Theta^\#). \tag{85}$$

*Then*

$$\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R) \subset (\Theta^\#). \tag{86}$$

*Proof.* Let $R_{\Psi'}$ be the character group ring quotient of $R$ associated to the set of characters with trivial zeroes:

$$\Psi' = \{\psi \in \hat{G} \colon \psi|_{G'} = \chi, \psi(v) = 1 \text{ for some } v \in \Sigma\}.$$

There is a canonical injection

$$\iota \colon R \longrightarrow R_\Psi \times R_{\Psi'}, \qquad \text{denoted } \iota(x) = (\iota_1(x), \iota_2(x)).$$

By Corollary 6.2, we can write $\mathrm{Fitt}_R(\mathrm{Sel}_\Sigma^{\Sigma'}(H)_R) = (x)$ for some $x \in R$. By Lemma 3.2, we have

$$\iota_2(x) = 0 = \iota_2(\Theta^\#).$$

The given inclusion (85) implies that there exists $y \in R_\Psi$ such that $\iota_1(x) = y \cdot \iota_1(\Theta^\#)$. Let $\tilde{y}$ be any lift of $y$ to $R$. We then have that $x - \tilde{y} \cdot \Theta^\#$ vanishes under both $\iota_1$ and $\iota_2$. It follows that $x = \tilde{y} \cdot \Theta^\#$, giving the desired result (86). □

For the rest of the paper, we will work with the "trivial zero free character group ring quotient" $R_\Psi$ of the component $\mathcal{O}[G_p]_\chi$. For notational simplicity, we will simply write $R$ for this ring $R_\Psi$. The image of $\Theta^\#$ is a non-zerodivisor in $R$.

## 7.2 Definitions and notations on Hilbert modular forms

We follow the definitions of Shimura [43] for the space of classical Hilbert modular forms over the totally real field $F$ (see also [13, §2.1]). Here we recall certain aspects of this definition and set up notation.

### 7.2.1 Hilbert modular forms

Let $\mathcal{H}$ denote the complex upper half plane endowed with the usual action of $\mathrm{GL}_2^+(\mathbf{R})$ via linear fractional transformations, where $\mathrm{GL}_2^+$ denotes the group of matrices with positive determinant. We fix an ordering of the $n$ embeddings $F \hookrightarrow \mathbf{R}$, which yields an embedding $\mathrm{GL}_2^+(F) \hookrightarrow \mathrm{GL}_2^+(\mathbf{R})^n$ and hence an action of $\mathrm{GL}_2^+(F)$ on $\mathcal{H}^n$. Here $\mathrm{GL}_2^+(F)$ denotes the group of matrices with totally positive determinant.

For each class $\lambda$ in the narrow class group $\mathrm{Cl}^+(F)$, we choose a representative fractional ideal $\mathfrak{t}_\lambda$. Let $\mathfrak{n} \subset \mathcal{O}_F$ be an ideal. Define

$$\Gamma_\lambda(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(F) : a, d \in \mathcal{O}_F, c \in \mathfrak{t}_\lambda \mathfrak{d} \mathfrak{n}, \right. \\ \left. b \in (\mathfrak{t}_\lambda \mathfrak{d})^{-1}, ad - bc \in \mathcal{O}_F^*,\ d \equiv 1 \pmod{\mathfrak{n}} \right\}.$$

Here $\mathfrak{d}$ denotes the different of $F$.

Let $k$ be a positive integer. We denote by $M_k(\mathfrak{n})$ the space of Hilbert modular forms for $F$ of level $\mathfrak{n}$ and weight $k$. Each element $f \in M_k(\mathfrak{n})$ is a tuple $f = (f_\lambda)_{\lambda \in \mathrm{Cl}^+(F)}$ of holomorphic functions $f_\lambda \colon \mathcal{H}^n \longrightarrow \mathbf{C}$ such that $f_\lambda|_{\alpha,k} = f_\lambda$ for all $\lambda \in \mathrm{Cl}^+(F)$ and $\alpha \in \Gamma_\lambda(\mathfrak{n})$. Here the weight $k$ slash action is defined in the usual way:

$$f_\lambda|_{\alpha,k}(z_1, \ldots, z_n) = \mathrm{N}(\det(\alpha))^{k/2} \prod_{i=1}^{n} (c_i z_i + d_i)^{-k} f_\lambda \left( \frac{a_1 z_1 + b_1}{c_1 z_1 + d_1}, \ldots, \frac{a_n z_n + b_n}{c_n z_n + d_n} \right),$$

where $a_i$ denotes the image of $a$ under the $i$th real embedding of $F$ and similarly for $b_i, c_i, d_i$.

### 7.2.2 Hecke Operators

The space $M_k(\mathfrak{n})$ is endowed with the action of a Hecke algebra generated by the following operators:

- $T_\mathfrak{q}$ for $\mathfrak{q} \nmid \mathfrak{n}$.
- $U_\mathfrak{q}$ for $\mathfrak{q} \mid \mathfrak{n}$.
- The "diamond operators" $S(\mathfrak{m})$ for each class $\mathfrak{m} \in G_\mathfrak{n}^+ =$ narrow ray class group of $F$ of conductor $\mathfrak{n}$.

We refer to [43, §2] for the definition of these Hecke operators.

### 7.2.3 Cusps, $q$-expansions, and cusp forms

The set of cusps of $\Gamma_\lambda(\mathfrak{n})$ is by definition the finite set

$$\mathrm{cusps}(\Gamma_\lambda(\mathfrak{n})) = \Gamma_\lambda(\mathfrak{n})\backslash \mathrm{GL}_2^+(F)/\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2^+(F) \right\} \leftrightarrow \Gamma_\lambda(\mathfrak{n})\backslash \mathbf{P}^1(F). \tag{87}$$

The bijection in (87) is $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto (a : c)$. We define

$$\mathrm{cusps}(\mathfrak{n}) = \bigsqcup_\lambda \mathrm{cusps}(\Gamma_\lambda(\mathfrak{n})). \tag{88}$$

A pair $\mathcal{A} = (A, \lambda)$ with $A \in \mathrm{GL}_2^+(F)$ and $\lambda \in \mathrm{Cl}^+(F)$ therefore gives rise to a cusp that we denote $[\mathcal{A}] \in \mathrm{cusps}(\mathfrak{n})$, corresponding to the image of the matrix $A$ in $\mathrm{cusps}(\Gamma_\lambda(\mathfrak{n}))$ in the $\lambda$-component of the disjoint union (88).

Given $f = (f_\lambda) \in M_k(\mathfrak{n})$ and a pair $\mathcal{A} = (A, \lambda)$, the function $f_\lambda|_{A,k}$ has a Fourier expansion

$$f_\lambda|_{A,k}(z) = a_{\mathcal{A}}(0) + \sum_{\substack{b \in \mathfrak{a} \\ b \gg 0}} a_{\mathcal{A}}(b) e_F(bz), \tag{89}$$

where $\mathfrak{a}$ is a certain lattice in $F$ depending on $\mathcal{A}$, and

$$e_F(bz) = \exp(2\pi i(b_1 z_1 + \cdots + b_n z_n)).$$

Here $b_i$ is the image in $\mathbf{R}$ of $b$ under the $i$th real embedding of $F$.

We normalize these Fourier coefficients as follows. Write $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and define the fractional ideal

$$\mathfrak{b}_{\mathcal{A}} = a\mathcal{O}_F + c(\mathfrak{t}_\lambda \mathfrak{d})^{-1}.$$

Define

$$c_{\mathcal{A}}(b, f) = a_{\mathcal{A}}(b) \cdot (\mathrm{N}\mathfrak{t}_\lambda)^{-k/2} (\mathrm{N}\mathfrak{b}_{\mathcal{A}})^{-k}.$$

The subspace of *cusp forms* $S_k(\mathfrak{n}) \subset M_k(\mathfrak{n})$ is the space of $f = (f_\lambda) \in M_k(\mathfrak{n})$ such that $c_{\mathcal{A}}(0, f) = 0$ for all pairs $\mathcal{A} = (A, \lambda)$. Note that the definition of this subspace does not depend on the choice of ideal class representatives $\mathfrak{t}_\lambda$.

When $k$ is even, the normalized constant term $c_{\mathcal{A}}(0, f)$ depends only on the cusp $[\mathcal{A}] \in \mathrm{cusps}(\mathfrak{n})$ determined by $\mathcal{A}$ (this motivates our normalizations). When $k$ is odd, this is *almost* true—it holds up to sign. In this case $c_{\mathcal{A}}(0, f)$ is still invariant if $A$ is multiplied on the left by an element of $\Gamma_\lambda(\mathfrak{n})$. But if $A' = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(F)$ then

$$c_{(AA', \lambda)}(0, f) = \mathrm{sgn}(\mathrm{Norm}_{F/\mathbf{Q}}(a)) \cdot c_{(A,\lambda)}(0, f).$$

### 7.2.4 $q$-expansions

When $A = 1$ we write simply

$$c_\lambda(0, f) = a_{(1,\lambda)}(0) \cdot (\mathrm{N}\mathfrak{t}_\lambda)^{-k/2}. \tag{90}$$

Furthermore in this case, the lattice $\mathfrak{a}$ appearing in (89) is the ideal $\mathfrak{t}_\lambda$. Any nonzero integral ideal $\mathfrak{m}$ may be written $\mathfrak{m} = (b)\mathfrak{t}_\lambda^{-1}$ with $b \in \mathfrak{t}_\lambda$ totally positive for a unique $\lambda \in \mathrm{Cl}^+(F)$. We define the normalized Fourier coefficient

$$c(\mathfrak{m}, f) = a_{(1,\lambda)}(b)(\mathrm{N}\mathfrak{t}_\lambda)^{-k/2}. \tag{91}$$

The collection of normalized Fourier coefficients $\{c_\lambda(0, f), c(\mathfrak{m}, f)\}$ is called the *$q$-expansion* of $f$ and determines the form $f$.

### 7.2.5 Cusps above infinity and zero

We recall some notation from [14]. Given a pair $\mathcal{A} = (A, \lambda)$ with $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we define the integral ideal

$$\mathfrak{c}_\mathcal{A} = (c)(\mathfrak{t}_\lambda \mathfrak{d} \mathfrak{b}_\mathcal{A})^{-1} \subset \mathcal{O}_F.$$

The ideal $\mathfrak{c}_\mathcal{A}$ depends only on the cusp $[\mathcal{A}]$ associated to $\mathcal{A}$. As intuition for this definition, consider the case $F = \mathbf{Q}$. If $\mathcal{A}$ represents the cusp $a/c \in \mathbf{P}^1(\mathbf{Q})$ where $a$ and $c$ are relatively prime integers, then $\mathfrak{c}_\mathcal{A} \subset \mathbf{Z}$ is the ideal generated by $c$.

We denote by $C_\infty(\mathfrak{n}) \subset \mathrm{cusps}(\mathfrak{n})$ the set of cusps $[\mathcal{A}]$ such that $\mathfrak{n} \mid \mathfrak{c}_\mathcal{A}$ and more generally for $\mathfrak{b} \mid \mathfrak{n}$ we define

$$C_\infty(\mathfrak{b}, \mathfrak{n}) = \{[\mathcal{A}] \in \mathrm{cusps}(\mathfrak{n})\colon\ \mathfrak{b} \mid \mathfrak{c}_\mathcal{A}\}.$$

Similarly, we let $C_0(\mathfrak{n})$ denote the set of cusps $[\mathcal{A}] \in \mathrm{cusps}(\mathfrak{n})$ such that $\gcd(\mathfrak{c}_\mathcal{A}, \mathfrak{n}) = 1$ and more generally for $\mathfrak{b} \mid \mathfrak{n}$ we define

$$C_0(\mathfrak{b}, \mathfrak{n}) = \{[\mathcal{A}] \in \mathrm{cusps}(\mathfrak{n})\colon\ \gcd(\mathfrak{b}, \mathfrak{c}_\mathcal{A}) = 1\}.$$

The sets $C_\infty(\mathfrak{b}, \mathfrak{n})$ and $C_0(\mathfrak{b}, \mathfrak{n})$ are stable under the action of the diamond operators $S(\mathfrak{m})$. These sets are enumerated in [14].

### 7.2.6 Forms with Nebentypus

Recall that $G_\mathfrak{n}^+$ denotes the narrow ray class group of $F$ attached to the conductor $\mathfrak{n}$. Write $h_\mathfrak{n}^+ = \#G_\mathfrak{n}^+$. Let $\psi$ denote a character $G_\mathfrak{n}^+ \longrightarrow \mathbf{C}^*$ whose associated sign is congruent to $(k, k, \ldots, k)$ in $(\mathbf{Z}/2\mathbf{Z})^n$, i.e. such that if $\alpha \in \mathcal{O}_F$ with $\alpha \equiv 1 \pmod{\mathfrak{n}}$, we have

$$\psi((\alpha)) = \mathrm{sgn}(\mathrm{Norm}_{F/\mathbf{Q}}(\alpha))^k.$$

A form $f \in M_k(\mathfrak{n})$ is said to have nebentypus $\psi$ if

$$f|_{S(\mathfrak{a})} = \psi(\mathfrak{a}) f$$

for all $\mathfrak{a} \in G_{\mathfrak{n}}^+$. The space of forms with nebentypus $\psi$ is denoted $M_k(\mathfrak{n}, \psi)$, and we let $S_k(\mathfrak{n}, \psi) = M_k(\mathfrak{n}, \psi) \cap S_k(\mathfrak{n})$. We have decompositions

$$M_k(\mathfrak{n}) = \bigoplus_{\psi} M_k(\mathfrak{n}, \psi), \qquad S_k(\mathfrak{n}) = \bigoplus_{\psi} S_k(\mathfrak{n}, \psi).$$

### 7.2.7 Raising the level

For a Hilbert modular form $f \in M_k(\mathfrak{n})$ and an integral ideal $\mathfrak{q}$ of $F$, there is a form

$$f|\mathfrak{q} \in M_k(\mathfrak{n}\mathfrak{q})$$

characterized by the fact that for nonzero integral ideals $\mathfrak{a}$ we have

$$c(\mathfrak{a}, f|\mathfrak{q}) = \begin{cases} c(\mathfrak{a}/\mathfrak{q}, f) & \text{if } \mathfrak{q} \mid \mathfrak{a} \\ 0 & \text{if } \mathfrak{q} \nmid \mathfrak{a} \end{cases}$$

and

$$c_\lambda(0, f|\mathfrak{q}) = c_{\lambda\mathfrak{q}}(0, f) \tag{92}$$

for all $\lambda \in \mathrm{Cl}^+(F)$. For the construction of $f|\mathfrak{q}$ see [43, Prop 2.3].

### 7.2.8 Group ring valued Hilbert modular forms

Define $M_k(\mathfrak{n}, \mathbf{Z}) \subset M_k(\mathfrak{n})$ to be the subgroup of forms $f$ such that

$$c(f, \mathfrak{m}) \in \mathbf{Z} \text{ for all nonzero } \mathfrak{m} \subset \mathcal{O}_F, \qquad c_\lambda(f, 0) \in \mathbf{Z} \text{ for all } \lambda \in \mathrm{Cl}^+(F).$$

For any abelian group $A$, define

$$M_k(\mathfrak{n}, A) = M_k(\mathfrak{n}, \mathbf{Z}) \otimes A.$$

Now suppose that $A$ is a ring and that $\psi\colon G_{\mathfrak{n}}^+ \longrightarrow A^*$ is a character. We define the forms of nebentypus $\psi$ by

$$M_k(\mathfrak{n}, A, \psi) = \{f \in M_k(\mathfrak{n}, A)\colon f|_{S(\mathfrak{a})} = \psi(\mathfrak{a}) f \text{ for all } \mathfrak{a} \in G_{\mathfrak{n}}^+\}.$$

These definitions generalize in the obvious way to yield $S_k(\mathfrak{n}, A)$ and $S_k(\mathfrak{n}, A, \psi)$. We are particularly interested in the case where $A$ is the ring $R = R_\Psi$ as in §7.1. If the extension $H/F$ has conductor dividing $\mathfrak{n}$, then $G = \mathrm{Gal}(H/F)$ is canonically a quotient of the narrow ray class group $G_{\mathfrak{n}}^+$. We define

$$\boldsymbol{\psi}\colon G_{\mathfrak{n}}^+ \longrightarrow G \longrightarrow R^*$$

to be the canonical character. The space of "group ring valued Hilbert modular forms" $M_k(\mathfrak{n}, R, \boldsymbol{\psi})$ was first considered by Wiles [53]. In practice, we will define such forms by specifying their Fourier coefficients, as described by the following lemma.

**Lemma 7.2.** *Let $c(\mathfrak{m}) \in R$ for $\mathfrak{m} \subset \mathcal{O}_F, \mathfrak{m} \neq 0$ and $c_\lambda(0) \in R$ for $\lambda \in \mathrm{Cl}^+(F)$ be a collection of elements of $R$ such that for all $\psi \in \Psi$, there exists a form $f_\psi \in M_k(\mathfrak{n}, \mathcal{O}, \psi)$ with*

$$c(f_\psi, \mathfrak{m}) = \psi(c(\mathfrak{m})), \qquad c_\lambda(f_\psi, 0) = \psi(c_\lambda(0)).$$

*Then there exists a unique $f \in M_k(\mathfrak{n}, R, \boldsymbol{\psi})$ such that $\psi(f) = f_\psi$ for all $\psi \in \Psi$.*

*Proof.* Recall that there is an embedding

$$R \hookrightarrow \prod_{\psi \in \Psi} \mathcal{O}, \qquad x \mapsto (\psi(x))_{\psi \in \Psi}. \tag{93}$$

The lemma follows from an important result of Silliman [14, Corollary 7.28], which implies that

$$M_k(\mathfrak{n}, R) = \{f \in M_k(\mathfrak{n}, \prod_{\psi \in \Psi} \mathcal{O}) \colon c(f, \mathfrak{m}), c_\lambda(f, 0) \in R \text{ for all } \mathfrak{m}, \lambda\}. \tag{94}$$

Now

$$M_k(\mathfrak{n}, \prod_{\psi \in \Psi} \mathcal{O}) = \prod_{\psi \in \Psi} M_k(\mathfrak{n}, \mathcal{O}),$$

and we can define $f \in M_k(\mathfrak{n}, \prod_{\psi \in \Psi} \mathcal{O})$ to be the form corresponding to the tuple $(f_\psi)$ under this identification. Then:

$$c(f, \mathfrak{m}) = (c(f_\psi, \mathfrak{m}))_\psi = (\psi(c(\mathfrak{m})))_\psi \tag{95}$$

$$c_\lambda(f, 0) = (c_\lambda(f_\psi, 0))_\psi = (\psi(c_\lambda(0)))_\psi. \tag{96}$$

The elements on the right side of (95) and (96) are the images of $c(\mathfrak{m})$ and $c_\lambda(0)$ under the embedding (93), respectively. By (94), it follows that $f \in M_k(\mathfrak{n}, R)$. The fact that $f \in M_k(\mathfrak{n}, R)$ now follows since $\psi(f) = f_\psi \in M_k(\mathfrak{n}, \mathcal{O}, \psi)$. □

**Remark 7.3.** As this proof shows, a group ring valued modular form $f$ over $R = R_\Psi$ can be viewed as encoding the *family* of modular forms $\{\psi(f)\}$ indexed by the characters $\psi \in \Psi$. The fact that the Fourier coefficients of $f$ lie in $R$, rather than just $\prod_{\psi \in \Psi} \mathcal{O}$, implies that the forms $\psi(f)$ satisfy certain $p$-adic congruences.

The Hecke operators $T_\mathfrak{q}$ for $\mathfrak{q} \nmid \mathfrak{n}$, $U_\mathfrak{q}$ for $\mathfrak{q} \mid \mathfrak{n}$, and $S(\mathfrak{m})$ for $(\mathfrak{m}, \mathfrak{n}) = 1$ preserve the space $M_k(\mathfrak{n}, R, \boldsymbol{\psi})$. To see this, note first that $S(\mathfrak{m})$ acts by $\boldsymbol{\psi}(\mathfrak{m}) \in R^*$. For $\mathfrak{q} \nmid \mathfrak{n}$, we have the formulas:

$$c(\mathfrak{m}, f|_{T_\mathfrak{q}}) = \sum_{\mathfrak{a} | (\mathfrak{m}, \mathfrak{q})} \boldsymbol{\psi}(\mathfrak{a}) \mathrm{N}\mathfrak{a}^{k-1} c(\mathfrak{m}\mathfrak{n}/\mathfrak{a}^2, f), \tag{97}$$

$$c_\lambda(0, f|_{T_\mathfrak{q}}) = c_{\lambda\mathfrak{q}^{-1}}(0, f) + \boldsymbol{\psi}(\mathfrak{q}) \mathrm{N}\mathfrak{q}^{k-1} c_{\lambda\mathfrak{q}}(0, f),$$

which show that $T_\mathfrak{q}$ preserves $M_k(\mathfrak{n}, R, \boldsymbol{\psi})$. In fact the same formulas hold for $U_\mathfrak{q}$ when $\mathfrak{q} \mid \mathfrak{n}$ with the convention that $\boldsymbol{\psi}(\mathfrak{q}) = 0$, implying that $U_\mathfrak{q}$ preserves $M_k(\mathfrak{n}, R, \boldsymbol{\psi})$ as well.

### 7.2.9 Ordinary forms

The ring $R = R_\Psi$ is a complete local $\mathbf{Z}_p$-algebra. Let $\mathfrak{P} = \gcd(p^\infty, \mathfrak{n})$ denote the $p$-part of $\mathfrak{n}$. Let $\mathfrak{p} \mid \mathfrak{P}$. Following Hida, we define the ordinary operators

$$e_{\mathfrak{p}}^{\mathrm{ord}} = \lim_{n\to\infty} U_{\mathfrak{p}}^{n!}, \qquad e_{\mathfrak{P}}^{\mathrm{ord}} = \prod_{\mathfrak{p}\mid\mathfrak{P}} e_{\mathfrak{p}}.$$

For any character $\psi\colon G_{\mathfrak{n}}^+ \longrightarrow R^*$ we have the spaces of $p$-ordinary forms:

$$M_k(\mathfrak{n}, R, \boldsymbol{\psi})^{\mathfrak{P}\text{-ord}} = e_{\mathfrak{P}}^{\mathrm{ord}} M_k(\mathfrak{n}, R, \boldsymbol{\psi}), \qquad S_k(\mathfrak{n}, R, \boldsymbol{\psi})^{\mathfrak{P}\text{-ord}} = e_{\mathfrak{P}}^{\mathrm{ord}} S_k(\mathfrak{n}, R, \boldsymbol{\psi}).$$

By construction, the operator $U_{\mathfrak{p}}$ acts invertibly on the space of $p$-ordinary modular forms for each $\mathfrak{p} \mid \mathfrak{P}$.

## 7.3 Eisenstein series

Let $k \geq 1$ be an odd integer and let $\psi\colon G \longrightarrow \mathcal{O}^*$ be a totally odd character. Let $S$ be a finite set of places of $F$. We denote by $\psi_S$ the character $\psi$ viewed as having modulus divisible by all finite primes in $S$, i.e. $\psi(\mathfrak{a}) = 0$ if $\mathfrak{a}$ is divisible by a prime in $S$. If $\mathfrak{n}$ is the product of $\mathrm{cond}(\psi)$ and the primes in $S$ not dividing $\mathrm{cond}(\psi)$, then there is an "$S$-stabilized" Eisenstein series $E_k(\psi_S, 1) \in M_k(\mathfrak{n}, \mathcal{O}, \psi)$ with Fourier coefficients given by

$$c(\mathfrak{m}, E_k(\psi_S, 1)) = \sum_{\mathfrak{r}\mid\mathfrak{m}} \psi_S\left(\frac{\mathfrak{m}}{\mathfrak{r}}\right) \mathrm{N}\mathfrak{r}^{k-1}.$$

If $k > 1$ and $\mathfrak{n} \neq 1$, we have $c_\lambda(0, E_k(\psi_S, 1)) = 0$. If $k > 1$ and $\mathfrak{n} = 1$, we have

$$c_\lambda(0, E_k(\psi_S, 1)) = \frac{1}{2^n}\psi^{-1}(\lambda) L(\psi^{-1}, 1-k).$$

If $k = 1$, then

$$c_\lambda(0, E_1(\psi_S, 1)) = 2^{-n} \cdot \begin{cases} L(\psi_S, 0) & \text{if } \mathfrak{n} \neq 1, \\ L(\psi, 0) + \psi^{-1}(\lambda) L(\psi^{-1}, 0) & \text{if } \mathfrak{n} = 1. \end{cases} \tag{98}$$

The Eisenstein series $E_k(\psi_S, 1)$ is an eigenvector for the Hecke operators with eigenvalues given by the corresponding Fourier coefficients, i.e.

- $T_{\mathfrak{l}}$ acts as $\psi(\mathfrak{l}) + \mathrm{N}\mathfrak{l}^{k-1}$ for $\mathfrak{l} \nmid \mathfrak{n}$
- $U_{\mathfrak{l}}$ acts as $\mathrm{N}\mathfrak{l}^{k-1}$ for $\mathfrak{l} \mid \mathfrak{n}$.

These Eisenstein series nearly fit into group ring families: the non-constant coefficients belong to the group ring but the constant terms only lie in the fraction field. Let $R$ denote a character group ring associated to $G$, and let $\boldsymbol{\psi}\colon G_{\mathfrak{n}}^+ \longrightarrow G \longrightarrow R$ denote the canonical

character. Let $S$ denote the set of primes dividing $\mathfrak{n}$. There is an Eisenstein series $E_k(\boldsymbol{\psi}, 1)$ whose specialization at a character $\psi$ is $E_k(\psi_S, 1)$. The group ring form $E_k(\boldsymbol{\psi}, 1)$ has $q$-expansion coefficients

$$c(\mathfrak{m}, E_k(\boldsymbol{\psi}, 1)) = \sum_{\substack{\mathfrak{r}|\mathfrak{m} \\ (\mathfrak{m}/\mathfrak{r}, \mathfrak{n})=1}} \boldsymbol{\psi}\left(\frac{\mathfrak{m}}{\mathfrak{r}}\right) \mathrm{N}\mathfrak{r}^{k-1} \in R. \tag{99}$$

Let $H_{\mathfrak{n}}$ denote the narrow ray class field of conductor $\mathfrak{n}$, so $\mathrm{Gal}(H_{\mathfrak{n}}/F) \cong G_{\mathfrak{n}}^{+}$. Let $\Theta$ denote the image in $\mathrm{Frac}(R)$ of $\Theta_S^{H_{\mathfrak{n}}/F} \in \mathbf{Q}[G_{\mathfrak{n}}^{+}]$, the $S$-depleted Stickelberger element for the extension $H_{\mathfrak{n}}/F$. The constant terms of $E_k(\boldsymbol{\psi}, 1)$ lie in $\mathrm{Frac}(R)$ and are given by

$$c_\lambda(0, E_k(\boldsymbol{\psi}, 1)) = 2^{-n} \cdot \begin{cases} 0 & \text{if } k > 1 \text{ and } \mathfrak{n} \neq 1 \\ \boldsymbol{\psi}^{-1}(\lambda)\Theta(1-k) & \text{if } k > 1 \text{ and } \mathfrak{n} = 1 \\ \Theta^{\#}(0) & \text{if } k = 1 \text{ and } \mathfrak{n} \neq 1, \\ \Theta^{\#}(0) + \boldsymbol{\psi}^{-1}(\lambda)\Theta(0) & \text{if } k = 1 \text{ and } \mathfrak{n} = 1. \end{cases}$$

# 8 Construction of cusp forms

In this section we apply certain results appearing in the papers [14], [45] to construct a group ring valued cusp form congruent to an Eisenstein series. First we note the following elementary lemma.

**Lemma 8.1.** *For sufficiently large positive integers $m$, the Stickelberger element $\Theta^{\#}$ divides $p^m$ in $R$.*

*Proof.* Recall that in §7.1 we replaced $R$ by a character group ring quotient in which $\Theta^{\#}$ is not a zerodivisor. Therefore we can consider $(\Theta^{\#})^{-1} \in \mathrm{Frac}(R)$. For sufficiently large $m$, we have $z = p^m(\Theta^{\#})^{-1} \in R$, since $\mathrm{Frac}(R) = R \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Therefore $\Theta^{\#} \cdot z = p^m$ with $z \in R$ as desired. □

For the remainder of the paper, we fix a positive integer $m$ satisfying Lemma 8.1. We also choose a positive integer $k$ such that $k \equiv 1 \pmod{(p-1)p^N}$ for a sufficiently large integer $N > m$. This notion of "sufficiently large" will become apparent as we use it in several instances in our proofs.

## 8.1 Construction of modified Eisenstein series

We introduce some notation. Let $\psi$ be a totally odd character of $G_F$ and $k \geq 1$ an odd integer. Write $\mathfrak{c}_0 = \mathrm{cond}(\psi)$. Let

$$T = \{\mathfrak{l}_1, \ldots, \mathfrak{l}_m\}$$

be a set of distinct primes not dividing $\mathfrak{c}_0$, and write

$$\mathfrak{l} = \prod_{i=1}^{m} \mathfrak{l}_i.$$

Let $\mathfrak{P}$ be an integral ideal coprime to $\mathfrak{l}$. Put

$$\mathfrak{c} = \mathrm{lcm}(\mathfrak{c}_0, \mathfrak{P}), \qquad \mathfrak{n} = \mathfrak{c}\mathfrak{l}.$$

The following construction is of central importance in this paper. We define a certain linear combination $W_k(\psi_{\mathfrak{P}}, 1)$ of Eisenstein series that satisfies the following:

- The $T$-smoothed $L$-function $L_{S_{\mathfrak{P}},T}(\psi, 0)$ appears in the constant terms at infinity $c_\lambda(0)$.
- The constant terms at all $p$-unramified cusps vary nicely with respect to the weight. More precisely, there is a single constant $\lambda = L(\psi^{-1}, 1-k)/L(\psi^{-1}, 0)$, independent of cusp, such that the ratio of the normalized constant terms at these cusps for $W_k$ and $W_1$ is $p$-adically very close to $\lambda$.
- The forms $W_k$ interpolate into a group ring family.

In a fixed level $\mathfrak{n}$, the Fourier coefficients (and constant terms at non-infinite cusps) of Eisenstein series behave differently for characters of different conductor dividing $\mathfrak{n}$. One miracle regarding the forms $W_k(\psi_{\mathfrak{P}}, 1)$ is that there is a single group ring form that interpolates all of these forms regardless of the conductor of $\psi$. For example, this is not the case for the unmodifed Eisenstein series $E_k(\psi_{\mathfrak{P}}, 1)$—note that the group ring form defined in (99) interpolates the $S$-depleted forms $E_k(\psi_S, 1)$ rather than the primitive forms $E_k(\psi, 1)$. Our construction is only robust enough to handle primes in $S$ not dividing $p$, which is why we still deplete at $\mathfrak{P}$.

**Definition 8.2.** With notation as above, let

$$W_k(\psi_{\mathfrak{P}}, 1) = \sum_{\mathfrak{m} \mid \mathfrak{l}} \mu(\mathfrak{m})\psi(\mathfrak{m})\mathrm{N}\mathfrak{m}^k E_k(\psi_{\mathfrak{P}}, 1)|_{\mathfrak{m}} \in M_k(\mathfrak{n}, \psi).$$

The goal of the remainder of this section is to compute the constant terms of $W_k(\psi_{\mathfrak{P}}, 1)$ at all cusps for odd $k \geq 1$. Let $\mathcal{A} = (A, \lambda)$ with $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(F)$ and $\lambda \in \mathrm{Cl}^+(F)$.

**Definition 8.3.** If $[\mathcal{A}] \in C_0(\mathfrak{c}_0, \mathfrak{n})$ and $\mathfrak{m} \mid \mathfrak{l}\mathfrak{P}$, we put $J_{\mathfrak{m}}$ (respectively, $J_{\mathfrak{m}}^c$) for the set of prime divisors $\mathfrak{q} \mid \mathfrak{m}$ such that $[\mathcal{A}] \in C_0(\mathfrak{q}, \mathfrak{n})$ (respectively $[\mathcal{A}] \in C_\infty(\mathfrak{q}, \mathfrak{n})$).

The following result is proved in [14, Theorem 4.7].

**Proposition 8.4.** *Suppose that $k > 1$ and $\mathfrak{m} \mid \mathfrak{l}$. The normalized constant terms $c_{\mathcal{A}}(0)$ of $E_k(\psi_{\mathfrak{P}}, 1)|_{\mathfrak{m}}$ as an element of $M_k(\mathfrak{n}, \psi)$ are as follows.*

- *The constant term at $\mathcal{A}$ is zero if $[\mathcal{A}] \notin C_0(\mathfrak{c}, \mathfrak{n})$.*
- *If $[\mathcal{A}] \in C_0(\mathfrak{c}, \mathfrak{n})$, the normalized constant term at $\mathcal{A}$ is*

$$\frac{\tau(\psi)}{\mathrm{N}\mathfrak{c}^k}\mathrm{sgn}(-\mathrm{N}c)\psi(\mathfrak{c}_{\mathcal{A}})\frac{L(\psi^{-1}, 1-k)}{2^n}\prod_{\mathfrak{p}|\mathfrak{P}}\left(1-\frac{\psi(\mathfrak{p})}{\mathrm{N}\mathfrak{p}^k}\right)\prod_{\mathfrak{q}\in J_{\mathfrak{m}}}\mathrm{N}\mathfrak{q}^{-k}\prod_{\mathfrak{q}\in J_{\mathfrak{m}}^c}\psi^{-1}(\mathfrak{q}). \tag{100}$$

**Remark 8.5.** When considering the expression $\psi(\mathfrak{c}_{\mathcal{A}})$, note that $[\mathcal{A}] \in C_0(\mathfrak{c}, \mathfrak{n})$ implies that $\gcd(\mathfrak{c}_{\mathcal{A}}, \mathfrak{c}_0) = 1$. Note also that one can only have $c = 0$ with $[\mathcal{A}] \in C_0(\mathfrak{c}, \mathfrak{n})$ if $\mathfrak{c} = 1$. In this case, by convention the expression $\mathrm{sgn}(\mathrm{N}c)\psi(\mathfrak{c}_{\mathcal{A}})$ in (100) denotes $\psi^{-1}(\mathfrak{t}_\lambda\mathfrak{d}\mathfrak{b}_{\mathcal{A}}) = \psi^{-1}(\mathfrak{t}_\lambda\mathfrak{d}(a))$, which is the value obtained if one replaces $A$ by a left $\Gamma_{1,\lambda}(\mathfrak{n})$-equivalent matrix for which $c \neq 0$. This convention will remain in force in the sequel. More generally, if $\psi$ is a totally odd character of conductor 1, any expression $\mathrm{sgn}(\mathrm{N}x)\psi(x\mathfrak{m})$ should be interpreted as $\psi(\mathfrak{m})$ even if $x = 0$.

**Proposition 8.6.** *Suppose that $k > 1$ is odd. The modular form $W_k(\psi_{\mathfrak{P}}, 1)$ has constant terms 0 outside the cusps in $C_0(\mathfrak{c}, \mathfrak{n})$. For a cusp $[\mathcal{A}] \in C_0(\mathfrak{c}, \mathfrak{n})$, the normalized constant term $c_{\mathcal{A}}(0, W_k(\psi_{\mathfrak{P}}, 1))$ equals*

$$\frac{\tau(\psi)}{\mathrm{N}\mathfrak{c}^k}\mathrm{sgn}(-\mathrm{N}c)\psi(\mathfrak{c}_{\mathcal{A}})\frac{L(\psi^{-1}, 1-k)}{2^n}\prod_{\mathfrak{p}|\mathfrak{P}}\left(1-\frac{\psi(\mathfrak{p})}{\mathrm{N}\mathfrak{p}^k}\right)\prod_{\mathfrak{q}\in J_{\mathfrak{l}}}(1-\psi(\mathfrak{q}))\prod_{\mathfrak{q}\in J_{\mathfrak{l}}^c}(1-\mathrm{N}\mathfrak{q}^k).$$

*Proof.* This is an application of Proposition 8.4. It is clear that the constant terms of $W_k(\psi_{\mathfrak{P}}, 1)$ are 0 outside $C_0(\mathfrak{c}, \mathfrak{n})$. Consider $[\mathcal{A}] \in C_0(\mathfrak{c}, \mathfrak{n})$. The normalized constant term of $W_k(\psi_{\mathfrak{P}}, 1)$ at $\mathcal{A}$ is

$$\frac{\tau(\psi)}{\mathrm{N}\mathfrak{c}^k}\mathrm{sgn}(-\mathrm{N}c)\psi(\mathfrak{c}_{\mathcal{A}})\frac{L(\psi^{-1}, 1-k)}{2^n}\prod_{\mathfrak{p}|\mathfrak{P}}\left(1-\frac{\psi(\mathfrak{p})}{\mathrm{N}\mathfrak{p}^k}\right)\sum_{\mathfrak{m}|\mathfrak{l}}\mu(\mathfrak{m})\prod_{\mathfrak{q}\in J_{\mathfrak{m}}^c}\mathrm{N}\mathfrak{q}^k\prod_{\mathfrak{q}\in J_{\mathfrak{m}}}\psi(\mathfrak{q}).$$

The result follows from the observation

$$\sum_{\mathfrak{m}|\mathfrak{l}}\mu(\mathfrak{m})\prod_{\mathfrak{q}\in J_{\mathfrak{m}}^c}\mathrm{N}\mathfrak{q}^k\prod_{\mathfrak{q}\in J_{\mathfrak{m}}}\psi(\mathfrak{q}) = \prod_{\mathfrak{q}\in J_{\mathfrak{l}}}(1-\psi(\mathfrak{q}))\prod_{\mathfrak{q}\in J_{\mathfrak{l}}^c}(1-\mathrm{N}\mathfrak{q}^k).$$

□

For $k = 1$, the results of Propositions 8.4 and 8.6 must be slightly modified. Even though we will only require the constant terms of $W_1(\psi_{\mathfrak{P}}, 1)$ at $C_\infty(\mathfrak{P}, \mathfrak{n})$, for completeness we calculate its constant terms at all cusps. The proof of the following proposition is another direct application of [14, Theorem 4.7], similar to that of Proposition 8.6.

**Proposition 8.7.** *The normalized constant terms of $W_1(\psi_{\mathfrak{P}}, 1) \in M_1(\mathfrak{n}, \psi)$ are as follows.*

- *Assume $\mathfrak{c}_0 = 1$.*

– *If* $[\mathcal{A}] \in C_0(\mathfrak{P}, \mathfrak{n}) \cap C_\infty(\mathfrak{l}, \mathfrak{n})$*, the normalized constant term at* $\mathcal{A}$ *is*

$$\psi(\mathfrak{b}_{\mathcal{A}})\frac{L_{S_\infty,T}(\psi,0)}{2^n}\prod_{\mathfrak{p}|\mathfrak{P}}(1-\mathrm{N}\mathfrak{p}^{-1}) + \tau(\psi)\psi^{-1}(\mathfrak{d}\mathfrak{t}_\lambda\mathfrak{b}_{\mathcal{A}})\frac{L(\psi^{-1},0)}{2^n}\prod_{\mathfrak{p}|\mathfrak{P}}\left(1-\frac{\psi(\mathfrak{p})}{\mathrm{N}\mathfrak{p}}\right)\prod_{i=1}^{m}(1-\mathrm{N}\mathfrak{l}_i).$$

– *If* $[\mathcal{A}] \in C_0(\mathfrak{P}, \mathfrak{n})$ *but* $[\mathcal{A}] \notin C_\infty(\mathfrak{l}, \mathfrak{n})$*, the normalized constant term at* $\mathcal{A}$ *is*

$$\tau(\psi)\psi^{-1}(\mathfrak{d}\mathfrak{t}_\lambda\mathfrak{b}_{\mathcal{A}})\frac{L(\psi^{-1},0)}{2^n}\prod_{\mathfrak{p}|\mathfrak{P}}\left(1-\frac{\psi(\mathfrak{p})}{\mathrm{N}\mathfrak{p}}\right)\prod_{\mathfrak{q}\in J_{\mathfrak{l}}}(1-\psi(\mathfrak{q}))\prod_{\mathfrak{q}\in J_{\mathfrak{l}}^c}(1-\mathrm{N}\mathfrak{q}).$$

– *If* $[\mathcal{A}] \notin C_0(\mathfrak{P}, \mathfrak{n})$ *and* $[\mathcal{A}] \in C_\infty(\mathfrak{l}, \mathfrak{n})$*, the normalized constant term at* $\mathcal{A}$ *is*

$$\psi(\mathfrak{b}_{\mathcal{A}})\frac{L_{S_\infty,T}(\psi,0)}{2^n}\prod_{\mathfrak{p}\in J_{\mathfrak{P}}}(1-\mathrm{N}\mathfrak{p}^{-1})\prod_{\mathfrak{p}\in J_{\mathfrak{P}}^c}(1-\psi(\mathfrak{p})).$$

– *If* $[\mathcal{A}] \notin C_0(\mathfrak{P}, \mathfrak{n})$ *and* $[\mathcal{A}] \notin C_\infty(\mathfrak{l}, \mathfrak{n})$*, the normalized constant term at* $\mathcal{A}$ *is 0.*

- *Assume* $\mathfrak{c}_0 \neq 1$.

  – *The constant terms are 0 outside the cusps in* $C_\infty(\mathfrak{c}_0\mathfrak{l}, \mathfrak{n}) \cup C_0(\mathfrak{c}, \mathfrak{n})$.

  – *If* $[\mathcal{A}] \in C_\infty(\mathfrak{c}_0\mathfrak{l}, \mathfrak{n})$*, the normalized constant term at* $\mathcal{A}$ *is*

$$\mathrm{sgn}(\mathrm{N}a)\psi^{-1}(a\mathfrak{b}_{\mathcal{A}}^{-1})\frac{L_{S_\infty,T}(\psi,0)}{2^n}\prod_{\mathfrak{p}\in J_{\mathfrak{P}}}(1-\mathrm{N}\mathfrak{p}^{-1})\prod_{\mathfrak{p}\in J_{\mathfrak{P}}^c}(1-\psi(\mathfrak{p})).$$

  – *If* $[\mathcal{A}] \in C_0(\mathfrak{c}, \mathfrak{n})$*, the normalized constant term at* $\mathcal{A}$ *is*

$$\frac{\tau(\psi)}{\mathrm{N}\mathfrak{c}}\mathrm{sgn}(-\mathrm{N}c)\psi(\mathfrak{c}_{\mathcal{A}})\frac{L(\psi^{-1},0)}{2^n}\prod_{\mathfrak{p}|\mathfrak{P}}\left(1-\frac{\psi(\mathfrak{p})}{\mathrm{N}\mathfrak{p}}\right)\prod_{\mathfrak{q}\in J_{\mathfrak{l}}}(1-\psi(\mathfrak{q}))\prod_{\mathfrak{q}\in J_{\mathfrak{l}}^c}(1-\mathrm{N}\mathfrak{q}).$$

## 8.2 Linear combinations cuspidal modulo high powers of $p$

A result of Hida (see [52, Lemma 1.4.2]) states the existence of a Hilbert modular form congruent to 1 modulo $p$. In [45, Theorem 6.1] Silliman proves the following slightly refined version of this result.

**Theorem 8.8.** *For positive integers* $k \equiv 0 \pmod{(p-1)p^N}$ *with* $N$ *sufficiently large, there is a modular form* $V_k \in M_k(1, \mathbf{Z}_p, 1)$ *such that* $V_k \equiv 1 \pmod{p^m}$*, and such that the normalized constant term* $c_{\mathcal{A}}(0, V_k)$ *for each cusp* $[\mathcal{A}] \in \mathrm{cusps}(1)$ *is congruent to* $1 \pmod{p^m}$.

The congruence $V_k \equiv 1 \pmod{p^m}$ means that $c(\mathfrak{m}, V_k) \equiv 0 \pmod{p^m}$ for all nonzero ideals $\mathfrak{m}$ and $c_\lambda(0, V_k) \equiv 1 \pmod{p^m}$ for all $\lambda \in \mathrm{Cl}^+(F)$.

Let $\mathfrak{P}$ denote the $p$-part of the ideal $\mathfrak{n}$, i.e. $\mathfrak{P} = \gcd(p^\infty, \mathfrak{n})$. The following result is proven in [45, Theorem 8.1].

**Theorem 8.9.** *For sufficiently large odd positive integers $k$, there exists a group ring valued form $G_k(\boldsymbol{\psi}) \in M_k(\mathfrak{n}, R, \boldsymbol{\psi})$ with normalized constant term at $\mathcal{A}$ for $[\mathcal{A}] \in C_\infty(\mathfrak{n})$ equal to $\mathrm{sgn}(\mathrm{N}a)\boldsymbol{\psi}^{-1}(a\mathfrak{b}_A^{-1})$, and constant term at cusps $[\mathcal{A}] \in C_\infty(\mathfrak{P}, \mathfrak{n}) \setminus C_\infty(\mathfrak{n})$ equal to 0.*

**Remark 8.10.** We repeat our convention that if $\mathfrak{n} = 1$ the expression $\mathrm{sgn}(\mathrm{N}a)\boldsymbol{\psi}^{-1}(a\mathfrak{b}_A^{-1})$ is understood to equal $\boldsymbol{\psi}(\mathfrak{b}_\mathcal{A})$ even if $a = 0$.

### 8.2.1 Case 1: $\mathrm{cond}(H/F)$ not divisible by primes above $p$

**Proposition 8.11.** *Suppose that $\mathfrak{n}$ is not divisible by any primes above $p$. Fix a positive integer $m'$. For positive $k \equiv 1 \pmod{(p-1)p^N}$ with $N$ sufficiently large, and each character $\psi$ of $R$, the form*

$$f_k(\psi) = W_1(\psi, 1)V_{k-1} - \frac{L(\psi^{-1}, 0)}{L(\psi^{-1}, 1-k)}W_k(\psi, 1) - \frac{L_{S_\infty, T}(\psi, 0)}{2^n}G_k(\psi)$$

*has normalized constant terms at all cusps divisible by $p^{m'}$. Here $G_k(\psi)$ denotes the specialization of the group ring form $G_k(\boldsymbol{\psi})$ in Theorem 8.9 at the character $\psi$.*

*Proof.* The constant terms of $W_k(\psi, 1), W_1(\psi, 1), V_{k-1}$, and $G_k(\psi)$ are given explicitly by Proposition 8.6, Proposition 8.7, Theorem 8.8, and Theorem 8.9, respectively.

Since $\mathfrak{P} = 1$, the form $G_k(\psi)$ has constant term equal to $\mathrm{sgn}(\mathrm{N}a)\psi^{-1}(a\mathfrak{b}_\mathcal{A}^{-1})$ for $[\mathcal{A}] \in C_\infty(\mathfrak{n})$ and equal to 0 if $[\mathcal{A}] \notin C_\infty(\mathfrak{n})$.

With $\mathfrak{c} = \mathfrak{c}_0 = \mathrm{cond}(\psi)$, it is clear that the constant terms of $f_k(\psi)$ are 0 outside $C_0(\mathfrak{c}, \mathfrak{n}) \cup C_\infty(\mathfrak{c}, \mathfrak{n})$, since the same is true for $W_1(\psi, 1)$, $W_k(\psi, 1)$, and $G_k(\psi)$.

To evaluate the constant terms at other cusps, we first assume that $\mathfrak{c} \neq 1$. If $[\mathcal{A}] \in C_\infty(\mathfrak{c}, \mathfrak{n}) \setminus C_\infty(\mathfrak{n})$, then $W_1(\psi, 1)$, $W_k(\psi, 1)$, and $G_k(\psi)$ all have constant term 0 at $\mathcal{A}$, hence $f_k(\psi)$ does as well. If $[\mathcal{A}] \in C_\infty(\mathfrak{n})$, the constant term of $W_k(\psi, 1)$ at $\mathcal{A}$ is 0. Meanwhile, the constant term of $W_1(\psi, 1)$ at $\mathcal{A}$ is

$$\mathrm{sgn}(\mathrm{N}a)\psi^{-1}(a\mathfrak{b}_\mathcal{A}^{-1})\frac{L_{S_\infty, T}(\psi, 0)}{2^n}$$

and the constant term of $V_{k-1}$ is 1 modulo $p^{m'}$ for positive $k \equiv 1 \pmod{(p-1)p^N}$ with $N$ sufficiently large. The constant term of $G_k(\psi)$ at $\mathcal{A}$ is $\mathrm{sgn}(\mathrm{N}a)\psi^{-1}(a\mathfrak{b}_\mathcal{A}^{-1})$. It follows that the constant term of $f_k(\psi)$ at $\mathcal{A}$ is 0 mod $p^{m'}$. Therefore the constant term of $f_k(\psi)$ is 0 mod $p^{m'}$ at all cusps in $C_\infty(\mathfrak{c}, \mathfrak{n})$.

Next we consider the case $[\mathcal{A}] \in C_0(\mathfrak{c}, \mathfrak{n})$, still maintaining the assumption $\mathfrak{c} \neq 1$. As in §8.1 let $J$ denote the set of indices $i$ such that $[\mathcal{A}]$ belongs to $C_0(\mathfrak{l}_i, \mathfrak{n})$. The normalized constant term of $f_k(\psi)$ at $\mathcal{A}$ is

$$\tau(\psi)\mathrm{sgn}(-\mathrm{N}c)\psi(\mathfrak{c}_{\mathcal{A}})\frac{L(\psi^{-1},0)}{2^n}\prod_{i\in J}(1-\psi(\mathfrak{l}_i))\times \left[c_{\mathcal{A}}(0,V_{k-1}) - \mathrm{N}\mathfrak{c}^{1-k}\prod_{i\notin J}\frac{1-\mathrm{N}\mathfrak{l}_i^k}{1-\mathrm{N}\mathfrak{l}_i}\right]. \tag{101}$$

The expression in brackets in (101) $p$-adically approaches 0, since each term in the difference approaches 1, for positive $k \equiv 1 \pmod{(p-1)p^N}$ with $N$ increasing. It follows that for $N$ sufficiently large, (101) is divisible by $p^{m'}$.

Next we consider the case $\mathfrak{c} = 1$, so $\mathfrak{n} = \mathfrak{l}$. If $[\mathcal{A}] \notin C_\infty(\mathfrak{n})$, the constant term of $G_k(\mathfrak{n})$ at $\mathcal{A}$ is 0, and the normalized constant term of $f_k(\psi)$ at $\mathcal{A}$ is again given by (101). If $[\mathcal{A}] \in C_\infty(\mathfrak{n})$, the normalized constant term of $f_k(\psi)$ at $\mathcal{A}$ is (101) plus the expression

$$\psi(\mathfrak{b}_A)\frac{L_{S_\infty,T}(\psi,0)}{2^n}\left[c_{\mathcal{A}}(0,V_{k-1})-1\right].$$

The result follows. □

### 8.2.2 Case 2: $\mathrm{cond}(H/F)$ is divisible by some primes above $p$

Let $\psi$ be a character of conductor $\mathfrak{c}_0$, with $\mathfrak{c}_0$ possibly divisible by some primes above $p$. Let $\mathfrak{l}_1, \ldots, \mathfrak{l}_d$ be distinct primes not dividing $\mathfrak{c}_0 p$. Let $\mathfrak{n} = \mathfrak{c}_0\mathfrak{l}_1\cdots\mathfrak{l}_d\mathfrak{P}'$, with $\mathfrak{P}'$ the product of powers of some (but not necessarily all) primes dividing $p$. Let $\mathfrak{P}$ denote the $p$-part of $\mathfrak{n}$ i.e. $\mathfrak{P} = \gcd(\mathfrak{n}, p^\infty)$ and put $\mathfrak{c} = \mathrm{lcm}(\mathfrak{c}_0, \mathfrak{P})$. We assume in this section that $\mathfrak{P} \neq 1$. Let $S_\mathfrak{P}$ denote the union of $S_\infty$ and the set of primes dividing $\mathfrak{P}$.

**Proposition 8.12.** *For positive integers $k \equiv 1 \pmod{(p-1)p^N}$ with $N$ sufficiently large, the form*

$$W_1(\psi_\mathfrak{P}, 1)V_{k-1} - \frac{L_{S_\mathfrak{P},T}(\psi,0)}{2^n}G_k(\psi)$$

*has normalized constant terms at all cusps in $C_\infty(\mathfrak{P},\mathfrak{n})$ divisible by $p^m$.*

*Proof.* By Proposition 8.7, the constant terms of $W_1(\psi_\mathfrak{P}, 1)$ are supported on $C_\infty(\mathfrak{c}_0\mathfrak{l}, \mathfrak{n}) \cup C_0(\mathfrak{c}, \mathfrak{n})$. As $\mathfrak{P} \neq 1$, we have

$$(C_\infty(\mathfrak{c}_0\mathfrak{l}, \mathfrak{n}) \cup C_0(\mathfrak{c}, \mathfrak{n})) \cap C_\infty(\mathfrak{P}, \mathfrak{n}) = C_\infty(\mathfrak{n}).$$

By definition, the constant terms of $G_k(\psi)$ are also 0 at cusps in $C_\infty(\mathfrak{P}, \mathfrak{n}) \setminus C_\infty(\mathfrak{n})$.

Suppose now that $[\mathcal{A}] \in C_\infty(\mathfrak{n})$. By definition, the normalized constant term of $G_k(\psi)$ at $\mathcal{A}$ is $\mathrm{sgn}(\mathrm{N}a)\psi^{-1}(a\mathfrak{b}_\mathcal{A}^{-1})$. The normalized constant term of $V_{k-1}$ is congruent to 1 modulo

$p^m$ for $N$ sufficiently large. By Proposition 8.7, the normalized constant term of $W_1(\psi_{\mathfrak{P}}, 1)$ at $\mathcal{A}$ is

$$\mathrm{sgn}(\mathrm{N}a)\psi^{-1}(a\mathfrak{b}_{\mathcal{A}}^{-1})\frac{L_{S_{\mathfrak{P}},T}(\psi, 0)}{2^n}.$$

The result follows. □

## 8.3 Group ring valued forms

We now interpolate the construction of the previous section into a group ring family. Recall our ring $R$ defined in §7.1, a quotient of a connected component $\mathcal{O}[G_p]_\chi$ associated to a totally odd faithful character $\chi$ of $G'$. The level of our forms will be

$$\mathfrak{n} = \mathrm{cond}(H/F)\prod_{\mathfrak{q}\in T}\mathfrak{q}$$

and as above we let

$$\mathfrak{P} = p\text{-part of } \mathfrak{n} = \gcd(p^\infty, \mathfrak{n}).$$

**Lemma 8.13.** *Let $\psi$ be a character of $R$, and let $\mathfrak{c}_0 = \mathrm{cond}(\psi)$. Then we can write*

$$\mathfrak{n} = \mathfrak{c}_0\mathfrak{l}_1\cdots\mathfrak{l}_d\mathfrak{P}'$$

*where the $\mathfrak{l}_i$ are distinct primes not dividing $\mathfrak{c}_0 p$ and $\mathfrak{P}'$ is divisible only by primes above $p$.*

*Proof.* We must show that if $\mathfrak{l}$ is a prime not above $p$ such that $\mathfrak{l}^n \mid \mathrm{cond}(H/F)$ with $n \geq 2$ then $\mathfrak{l}^n \mid \mathrm{cond}(\psi)$. Let $H_p \subset H$ denote the fixed field of $G'$ and $H'$ the fixed field of $G_p$, so

$$\mathrm{Gal}(H_p/F) = G_p \text{ and } \mathrm{Gal}(H'/F) = G'.$$

The field $H$ is the compositum of $H_p$ and $H'$. Since $G_p$ is a $p$-group and $\mathfrak{l} \nmid p$, the prime $\mathfrak{l}$ is at most tamely ramified in $H_p$. Therefore if $\mathfrak{l}^n \mid \mathrm{cond}(H/F)$ with $n \geq 2$ then $H'/F$ must have conductor divisible by $\mathfrak{l}^n$. Since $\chi$ is a faithful character of $G'$, it follows that $\mathfrak{l}^n \mid \mathrm{cond}(\chi)$. Any character $\psi$ of $R$ can be written $\psi = \psi_p\chi$ where $\psi_p$ is a character of $G_p$. As already noted, the $\mathfrak{l}$-part of the conductor of $\psi_p$ is at most $\mathfrak{l}$. Therefore $\mathfrak{l}^n \mid \mathrm{cond}(\psi)$ as desired. □

**Proposition 8.14.** *For all odd $k \geq 1$, the unique form $W_k(\boldsymbol{\psi}, 1) \in M_k(\mathfrak{n}, \mathrm{Frac}(R), \boldsymbol{\psi})$ that specializes to $W_k(\psi_{\mathfrak{P}}, 1)$ for all characters $\psi$ of $R$ has non-constant term $q$-expansion coefficients $c(\mathfrak{m}, W_k(\boldsymbol{\psi}, 1))$ lying in $R$.*

*Proof.* Let $\mathfrak{l}$ denote the product of all primes dividing $\mathfrak{n}/\mathfrak{P}$. For each $\mathfrak{m} \mid \mathfrak{l}$, let $I_{\mathfrak{m}}$ be the subgroup generated by $I_v$ for $v \mid \mathfrak{m}$. Note that $\#I_{\mathfrak{m}} \mid \prod_{v\mid\mathfrak{m}}(1 - \mathrm{N}v^k)$ in $\mathbf{Z}_p$.

Write

$$\boldsymbol{\psi}^{\mathfrak{m}} \colon G^+_{\mathfrak{n}/\mathfrak{m}} \longrightarrow G/I_{\mathfrak{m}} \longrightarrow \mathcal{O}[G/I_{\mathfrak{m}}]^*$$

for the canonical character corresponding to the maximal subextension of $H/F$ in which the primes dividing $\mathfrak{m}$ are unramified. Let $E_k(\boldsymbol{\psi}^{\mathfrak{m}}, 1) \in M_k(\mathfrak{n}/\mathfrak{m}, \boldsymbol{\psi}^{\mathfrak{m}}, \mathcal{O}[G/I_{\mathfrak{m}}]^*)$ be the group ring form defined in (99) associated to the character $\boldsymbol{\psi}^{\mathfrak{m}}$. If $\psi$ is a character of $G$ unramified at all primes dividing $\mathfrak{m}$, then the specialization of $E_k(\boldsymbol{\psi}^{\mathfrak{m}}, 1)$ at $\psi$ is the form $E_k(\psi_{\mathfrak{n}/\mathfrak{m}}, 1)$.

Next note that there is a canonical $\mathcal{O}[G]$-module map

$$\mathcal{O}[G/I_{\mathfrak{m}}] \longrightarrow \mathcal{O}[G] \longrightarrow R$$

given by $x \mapsto \mathrm{N}I_{\mathfrak{m}} \cdot \tilde{x}$, where $\tilde{x}$ is an arbitrary lift of $x$. This map does not depend on the choice of lift. The image of $E_k(\boldsymbol{\psi}^{\mathfrak{m}}, 1)$ under this map is a form

$$\mathrm{N}I_{\mathfrak{m}} \cdot \tilde{E}_k(\boldsymbol{\psi}^{\mathfrak{m}}, 1) \in M_k(\mathfrak{n}/\mathfrak{m}, \mathrm{Frac}(R)),$$

and all of the non-constant term $q$-expansion coefficients lie in $R$. We define

$$W_k(\boldsymbol{\psi}, 1) = \sum_{\mathfrak{m}|\mathfrak{l}} \mathrm{N}I_{\mathfrak{m}} \cdot \tilde{E}_k(\boldsymbol{\psi}^{\mathfrak{m}}, 1)|_{\mathfrak{m}} \boldsymbol{\psi}^{\mathfrak{m}}(\mathfrak{m}) \frac{1}{\#I_{\mathfrak{m}}} \prod_{v|\mathfrak{m}} (1 - \mathrm{N}v^k). \tag{102}$$

It is clear from our construction that the non-constant term $q$-expansion coefficients of $W_k(\boldsymbol{\psi}, 1)$ lie in $R$. To conclude the proof we must show that the specialization of $W_k(\boldsymbol{\psi}, 1)$ at a character $\psi$ of $R$ is equal to $W_k(\psi_{\mathfrak{P}}, 1)$.

Given $\psi$, let $\mathfrak{c}_0 = \mathrm{cond}(\psi)$ and let $\mathfrak{l}'$ be the product of the primes dividing $\mathfrak{l}$ that do not divide $\mathfrak{c}_0$. By Lemma 8.13, we can write $\mathfrak{n} = \mathfrak{c}_0 \mathfrak{l}' \mathfrak{P}'$ where $\mathfrak{P}'$ is divisible only by primes above $p$.

Note that if $\psi$ is nontrivial on $I_{\mathfrak{m}}$, then $\psi(\mathrm{N}I_{\mathfrak{m}}) = 0$. Applying $\psi$ to the sum in (102) gives

$$\begin{aligned}
&\sum_{\mathfrak{m}|\mathfrak{l}'} \psi(\mathfrak{m}) E_k(\psi_{\frac{\mathfrak{l}'}{\mathfrak{m}}\mathfrak{P}}, 1)|_{\mathfrak{m}} \sum_{\mathfrak{m}'|\mathfrak{m}} \mu(\mathfrak{m}') \mathrm{N}\mathfrak{m}'^k \\
=&\sum_{\mathfrak{m}'|\mathfrak{l}'} \mu(\mathfrak{m}') \mathrm{N}\mathfrak{m}'^k \psi(\mathfrak{m}') \sum_{\mathfrak{m}|\frac{\mathfrak{l}'}{\mathfrak{m}'}} \psi(\mathfrak{m}) E_k(\psi_{\frac{\mathfrak{l}'}{\mathfrak{m}'\mathfrak{m}}\mathfrak{P}}, 1)|_{\mathfrak{m}'\mathfrak{m}} \\
=&\sum_{\mathfrak{m}'|\mathfrak{l}'} \mu(\mathfrak{m}') \mathrm{N}\mathfrak{m}'^k \psi(\mathfrak{m}') \left( \sum_{\mathfrak{m}|\frac{\mathfrak{l}'}{\mathfrak{m}'}} \psi(\mathfrak{m}) E_k(\psi_{\frac{\mathfrak{l}'}{\mathfrak{m}'\mathfrak{m}}\mathfrak{P}}, 1)|_{\mathfrak{m}} \right)|_{\mathfrak{m}'}
\end{aligned}$$

To finish the proof that this equals $W(\psi_{\mathfrak{P}}, 1)$, we must show that

$$\sum_{\mathfrak{m}|\frac{\mathfrak{l}'}{\mathfrak{m}'}} \psi(\mathfrak{m}) E_k(\psi_{\frac{\mathfrak{l}'}{\mathfrak{m}'\mathfrak{m}}\mathfrak{P}}, 1)|_{\mathfrak{m}} = E_k(\psi_{\mathfrak{P}}, 1).$$

We do this by induction on the number of prime factors of $\mathfrak{l}'/\mathfrak{m}'$. The statement is clear with

$\mathfrak{l}' = \mathfrak{m}'$. Let $\mathfrak{l}'/\mathfrak{m}' = \mathfrak{l}_1 \cdots \mathfrak{l}_r$ for some $r \geq 1$. Write the sum above as

$$\begin{aligned}
&\sum_{\mathfrak{m}|\mathfrak{l}_1\cdots\mathfrak{l}_r} \psi(\mathfrak{m}) E_k(\psi_{\frac{\mathfrak{l}_1\cdots\mathfrak{l}_r}{\mathfrak{m}}\mathfrak{P}}, 1)|_{\mathfrak{m}} \\
&= \sum_{\mathfrak{m}|\mathfrak{l}_1\cdots\mathfrak{l}_{r-1}} \psi(\mathfrak{m})(E_k(\psi_{\frac{\mathfrak{l}_1\cdots\mathfrak{l}_r}{\mathfrak{m}}\mathfrak{P}}, 1)|_{\mathfrak{m}} + \psi(\mathfrak{l}_r) E_k(\psi_{\frac{\mathfrak{l}_1\cdots\mathfrak{l}_{r-1}}{\mathfrak{m}}\mathfrak{P}}, 1)|_{\mathfrak{m}\mathfrak{l}_r}) \\
&= \sum_{\mathfrak{m}|\mathfrak{l}_1\cdots\mathfrak{l}_{r-1}} \psi(\mathfrak{m}) E_k(\psi_{\frac{\mathfrak{l}_1\cdots\mathfrak{l}_{r-1}}{\mathfrak{m}}\mathfrak{P}}, 1)|_{\mathfrak{m}} \\
&= E_k(\psi_{\mathfrak{P}}, 1),
\end{aligned}$$

where the last equality holds by the induction hypothesis. □

The following result is proved in [45, Theorem 8.2].

**Theorem 8.15.** *Fix a positive integer $m' \geq \mathrm{ord}_p(\#G_p)$. The following holds for all sufficiently large odd integers $k$. Let $f_\psi \in M_k(\mathfrak{n}, E, \psi)$ be a collection of modular forms for characters $\psi$ of $G$ belonging to $\chi$ with the property that the normalized constant terms of each $f_\psi$ at representatives for each cusp $A \in C_\infty(\mathfrak{P}, \mathfrak{n})$ are divisible by $p^{m'}$. There exists a group ring family*

$$h(\boldsymbol{\psi}) \in M_k(\mathfrak{n}, \boldsymbol{\psi}, R)$$

*such that each specialization $h(\psi)$ satisfies the property that*

$$\tilde{f}_\psi = f_\psi - (p^{m'}/\#G_p)h(\psi)$$

*has constant term 0 at all cusps $A \in C_\infty(\mathfrak{P}, \mathfrak{n})$. If $\mathfrak{P} = 1$, so $C_\infty(\mathfrak{P}, \mathfrak{n}) = \mathrm{cusps}(\mathfrak{n})$, then $\tilde{f}_\psi$ is cuspidal. If $\mathfrak{P} \neq 1$, then $e_{\mathfrak{P}}^{\mathrm{ord}}(\tilde{f}_\psi)$ is cuspidal.*

**Lemma 8.16.** *Suppose we are in case 1, i.e. $\gcd(\mathfrak{n}, p) = 1$. For $N$ sufficiently large and positive $k \equiv 1 \pmod{(p-1)p^N}$, the element*

$$x = \frac{\Theta_{S_\infty}(1-k)}{\Theta_{S_\infty}(0)} \in \mathrm{Frac}(R)$$

*lies in $R$ and is a non-zerodivisor satisfying*

$$x \equiv \prod_{\mathfrak{p}|p}(1 - \chi(\mathfrak{p})^{-1}) \pmod{\mathfrak{m}_R}. \tag{103}$$

*Proof.* First note that the specializations $L(\psi^{-1}, 0)$ of the denominator of $x$ are nonzero, so $x$ is a well-defined element of $\mathrm{Frac}(R)$. The same is true of the numerator, so if we can show that $x \in R$, it will follow immediately that it is a non-zerodivisor.

Let $S_p$ denote the union of $S_\infty$ with the set of primes above $p$ in $F$. Note that

$$\Theta_{S_p}(1-k) = \prod_{\mathfrak{p}|p}(1 - \sigma_{\mathfrak{p}}^{-1}\mathrm{N}\mathfrak{p}^{k-1})\Theta_{S_\infty}(1-k),$$

where $\sigma_{\mathfrak{p}} \in G$ denotes the Frobenius at $\mathfrak{p}$ (we are in case 1, where each $\mathfrak{p}$ above $p$ is unramified in $H/F$). Consider the element $y(k) = \Theta_{S_p}(1-k) - \Theta_{S_p}(0) \in \mathrm{Frac}(R)$. By the theory of $p$-adic $L$-functions, this element $p$-adically approaches 0 for positive $k \equiv 1 \pmod{(p-1)p^N}$ as $N \longrightarrow \infty$. In particular, for positive $k \equiv 1 \pmod{(p-1)p^N}$ and $N$ sufficiently large we have that $y(k) \in R$. Furthermore, for any positive integer $m'$ we can take $N$ larger still to ensure that $y(k)$ is divisible by $p^{m'}$ in $R$. Suppose that $m'$ has been chosen large enough that $p^{m'}/\Theta_{S_\infty}(0) \in R$. Then $y(k)/\Theta_{S_\infty}(0) \in R$. But

$$\frac{y(k)}{\Theta_{S_\infty}(0)} = x\prod_{\mathfrak{p}|p}(1-\sigma_{\mathfrak{p}}^{-1}\mathrm{N}\mathfrak{p}^{k-1}) - \prod_{\mathfrak{p}|p}(1-\sigma_{\mathfrak{p}}^{-1}) \in R. \tag{104}$$

Since the Euler factors $1-\sigma_{\mathfrak{p}}^{-1}\mathrm{N}\mathfrak{p}^{k-1}$ are units in $R$ for $k > 1$, it follows that $x \in R$ as desired. To conclude we note that after increasing $m'$ by 1 if necessary, we have that $y(k)/\Theta_{S_\infty}(0) \in \mathfrak{m}_R$. The desired congruence for $x$ then follows from (104).

□

**Theorem 8.17.** *In case 1* ($\gcd(\mathfrak{n}, p) = 1$)*, for positive* $k \equiv 1 \pmod{(p-1)p^N}$ *and* $N$ *sufficiently large, there exists a group ring form* $H_k(\boldsymbol{\psi}) \in M_k(\mathfrak{n}, R, \boldsymbol{\psi})$ *such that*

$$\tilde{F}_k(\boldsymbol{\psi}) = xW_1(\boldsymbol{\psi}, 1)V_{k-1} - W_k(\boldsymbol{\psi}, 1) - x\Theta^{\#}(0)H_k(\boldsymbol{\psi})$$

*lies in* $S_k(\mathfrak{n}, R, \boldsymbol{\psi})$*, where* $x = \Theta_{S_\infty}(1-k)/\Theta_{S_\infty}(0) \in R$ *is as in Lemma 8.16.*

*Proof.* Define

$$f_k(\boldsymbol{\psi}) = W_1(\boldsymbol{\psi}, 1)V_{k-1} - \frac{1}{x}W_k(\boldsymbol{\psi}, 1) - \frac{\Theta^{\#}(0)}{2^n}G_k(\boldsymbol{\psi}) \in M_k(\mathfrak{n}, \mathrm{Frac}(R), \boldsymbol{\psi}).$$

By definition, this is a group ring form whose specialization at a character $\psi$ of $R$ is the form $f_k(\psi)$ defined in Proposition 8.11. This proposition states that for any positive integer $m'$, for positive $k \equiv 1 \pmod{(p-1)p^N}$ and $N$ sufficiently large the constant terms of $f_k(\psi)$ are divisible by $p^{m'}$. Therefore by Theorem 8.15 there exists a group ring form $h_k(\boldsymbol{\psi}) \in M_k(\mathfrak{n}, R, \boldsymbol{\psi})$ such that

$$\tilde{f}_k(\boldsymbol{\psi}) = f_k(\boldsymbol{\psi}) - \frac{p^{m'}}{\#G_p}h_k(\boldsymbol{\psi})$$

is a cusp form. Choose $m'$ large enough that $\#G_p \cdot \Theta^{\#}$ divides $p^{m'}$ in $R$ and define

$$H_k(\boldsymbol{\psi}) = \frac{G_k(\boldsymbol{\psi})}{2^n} - \frac{p^{m'}}{\#G_p \cdot \Theta^{\#}}h_k(\boldsymbol{\psi}) \in M_k(\mathfrak{n}, R, \boldsymbol{\psi}).$$

The form $\tilde{F}_k(\boldsymbol{\psi}) = x \cdot \tilde{f}_k(\boldsymbol{\psi})$ is cuspidal and can be written explicitly as

$$\tilde{F}_k(\boldsymbol{\psi}) = xW_1(\boldsymbol{\psi}, 1)V_{k-1} - W_k(\boldsymbol{\psi}, 1) - x\Theta^{\#}(0)H_k(\boldsymbol{\psi}) \in S_k(\mathfrak{n}, R, \boldsymbol{\psi}).$$

Note that there is a small subtlety in verifying that the $q$-expansion coefficients of $\tilde{F}_k(\boldsymbol{\psi})$ lie in $R$. The constant terms of $W_1(\boldsymbol{\psi}, 1)$ only lie in $\mathrm{Frac}(R)$. But the non-constant $q$-expansion coefficients of $V_{k-1}$ are highly divisible by $p$, so the contribution to the non-constant $q$-expansion coefficients of the product $xW_1(\boldsymbol{\psi}, 1)V_{k-1}$ will be integral for $k \equiv 1 \pmod{(p-1)p^N}$ and $N$ sufficiently large. For the constant terms, there is nothing to check since $\tilde{F}_k(\boldsymbol{\psi})$ is cuspidal. □

In case 2, when there exist primes above $p$ dividing $\mathfrak{n}$, we get the following theorem. It is proven exactly as above, using Theorem 8.15 and building off of Proposition 8.12 in place of Proposition 8.11.

**Theorem 8.18.** *Suppose we are in case 2, i.e.* $\gcd(\mathfrak{n}, p) \neq 1$. *For positive integers* $k \equiv 1 \pmod{(p-1)p^N}$ *and* $N$ *sufficiently large, there exists a group ring form* $H_k(\boldsymbol{\psi}) \in M_k(\mathfrak{n}, R, \boldsymbol{\psi})$ *such that*

$$\tilde{F}_k(\boldsymbol{\psi}) = e_{\mathfrak{P}}^{\mathrm{ord}} \left( W_1(\boldsymbol{\psi}, 1)V_{k-1} - \Theta^{\#}(0)H_k(\boldsymbol{\psi}) \right)$$

*lies in* $S_k(\mathfrak{n}, R, \boldsymbol{\psi})$.

## 8.4 Applying the ordinary operator

In our applications it will be convenient to apply the ordinary operator at all primes above $p$. In addition, in order to ensure that we can work over Hecke algebras that are local rings, we would like to project onto components where the $U_{\mathfrak{p}}$-operator for $\mathfrak{p}$ dividing $p$ acts via certain eigenvalues. In case 1, this latter projection will only be relevant if *all* the primes above $p$ satisfy $\chi(\mathfrak{p}) \neq 1$. By (103), this is precisely the case that $x$ is a unit in $R$. We then apply $U_{\mathfrak{p}} - \boldsymbol{\psi}(\mathfrak{p})$ for each $\mathfrak{p} \mid p$ to our family $\tilde{F}_k(\boldsymbol{\psi})$. Doing so, we obtain the corollary below.

**Corollary 8.19.** *Suppose we are in case 1. Let* $\mathfrak{P}'$ *denote the product of the primes above* $p$. *For positive* $k \equiv 1 \pmod{(p-1)p^N}$ *and* $N$ *sufficiently large, there exists a cuspidal group ring family* $F_k(\boldsymbol{\psi}) \in S_k(\mathfrak{n}\mathfrak{P}', \boldsymbol{\psi}, R)^{p\text{-}ord}$ *such that*

$$F_k(\boldsymbol{\psi}) \equiv \begin{cases} xW_1(\boldsymbol{\psi}, 1) - W_k(\boldsymbol{\psi}, 1_p) & (\mathrm{mod}\ x\Theta^{\#}) \quad \chi(\mathfrak{p}) = 1 \text{ for some } \mathfrak{p} \mid p \\ W_1(\boldsymbol{\psi}_p, 1) & (\mathrm{mod}\ \Theta^{\#}) \quad \chi(\mathfrak{p}) \neq 1 \text{ for all } \mathfrak{p} \mid p. \end{cases} \tag{105}$$

Here the forms $W_k(\boldsymbol{\psi}, 1_p)$ and $W_1(\boldsymbol{\psi}_p, 1)$ are defined like $W_k(\boldsymbol{\psi}, 1)$ and $W_1(\boldsymbol{\psi}, 1)$ but with the characters $1, \boldsymbol{\psi}$ replaced by $1_p, \boldsymbol{\psi}_p$ in the two cases, respectively.

**Remark 8.20.** The congruence (105) should be interpreted as a congruence of Fourier coefficients:

$$c(\mathfrak{m}, F_k(\boldsymbol{\psi})) \equiv x \cdot c(\mathfrak{m}, W_1(\boldsymbol{\psi}, 1)) - c(\mathfrak{m}, W_k(\boldsymbol{\psi}, 1_p)) \pmod{x\Theta^{\#}} \tag{106}$$

for all ideals $\mathfrak{m}$ in the first case, and similarly for the second case.

*Proof.* Consider the first case in (105), which we hereafter refer to as case 1a. For $\mathfrak{p} \mid p$, let

$$z = \prod_{\mathfrak{p}|p} \frac{\boldsymbol{\psi}(\mathfrak{p})}{\boldsymbol{\psi}(\mathfrak{p}) - \mathrm{N}\mathfrak{p}^{k-1}} \equiv 1 \pmod{p^m}.$$

Note that

$$e_{\mathfrak{P}}^{\mathrm{ord}} W_k(\boldsymbol{\psi}, 1) = z \cdot W_k(\boldsymbol{\psi}, 1_p).$$

Since $z \equiv 1 \pmod{p^m}$, we have $z^{-1}x \equiv x \pmod{x\Theta^{\#}}$. The desired result then holds by defining $F_k(\boldsymbol{\psi}) = z^{-1} e_{\mathfrak{P}}^{\mathrm{ord}}(\tilde{F}_k(\boldsymbol{\psi}))$.

In the second case in (105), which we call case 1b, we let

$$z = \prod_{\mathfrak{p}|p} \frac{1}{1 - \boldsymbol{\psi}(\mathfrak{p})} \in R^*.$$

Then

$$e_{\mathfrak{P}}^{\mathrm{ord}} \prod_{\mathfrak{p}|p} (U_{\mathfrak{p}} - \boldsymbol{\psi}(\mathfrak{p}))(W_k(\boldsymbol{\psi}, 1)) = 0$$

whereas

$$e_{\mathfrak{P}}^{\mathrm{ord}} \prod_{\mathfrak{p}|p} (U_{\mathfrak{p}} - \boldsymbol{\psi}(\mathfrak{p}))(W_1(\boldsymbol{\psi}, 1)) = z W_1(\boldsymbol{\psi}_p, 1).$$

Noting that $x, z \in R^*$ in this case, the result follows by letting

$$F_k(\boldsymbol{\psi}) = (xz)^{-1} e_{\mathfrak{P}}^{\mathrm{ord}} \prod_{\mathfrak{p}|p} (U_{\mathfrak{p}} - \boldsymbol{\psi}(\mathfrak{p}))(\tilde{F}_k(\boldsymbol{\psi})).$$

□

In case 2 (there exists a prime above $p$ dividing $\mathfrak{n}$), we must apply (in addition to the ordinary operator at each $\mathfrak{p} \mid p$) the operator $U_{\mathfrak{p}} - \boldsymbol{\psi}(\mathfrak{p})$ for each $\mathfrak{p} \mid p$ not dividing $\mathfrak{n}$ such that $\chi(\mathfrak{p}) \neq 1$. We obtain:

**Corollary 8.21.** *Suppose we are in case 2. Let $\mathfrak{P}'$ denote the product of the primes above $p$ that do not divide $\mathfrak{n}$. Let $\mathfrak{P}''$ denote the product of primes $\mathfrak{p}$ dividing $\mathfrak{P}'$ such that $\chi(\mathfrak{p}) \neq 1$. For positive $k \equiv 1 \pmod{(p-1)p^N}$ and $N$ sufficiently large, there exists a cuspidal group ring family $F_k(\boldsymbol{\psi}) \in S_k(\mathfrak{n}\mathfrak{P}', \boldsymbol{\psi}, R)^{p\text{-}ord}$ such that*

$$F_k(\boldsymbol{\psi}) \equiv W_1(\boldsymbol{\psi}_{\mathfrak{P}\mathfrak{P}''}, 1) \pmod{\Theta^{\#}}. \tag{107}$$

## 8.5 Homomorphism on the Hecke Algebra

For clarity we recall the definition of certain ideals.

$$\begin{aligned}\mathfrak{n} &= \mathrm{cond}(H/F)\prod_{\mathfrak{q}\in T}\mathfrak{q}\\ \mathfrak{P} &= \gcd(p^\infty,\mathfrak{n})\\ \mathfrak{P}' &= \prod_{\mathfrak{p}|p,\ \mathfrak{p}\nmid\mathfrak{P}}\mathfrak{p}\\ \mathfrak{P}'' &= \prod_{\mathfrak{p}|\mathfrak{P}',\chi(\mathfrak{p})\neq 1}\mathfrak{p}.\end{aligned}$$

Recall also our trichotomy of cases.

$$\begin{aligned}\text{Case 1a} &: \mathfrak{P}=1, \mathfrak{P}'\neq\mathfrak{P}''.\\ \text{Case 1b} &: \mathfrak{P}=1, \mathfrak{P}'=\mathfrak{P}''.\\ \text{Case 2} &: \mathfrak{P}\neq 1.\end{aligned}$$

Let

$$\tilde{\mathbf{T}}\subset \mathrm{End}_R(S_k(\mathfrak{n}\mathfrak{P}', R, \boldsymbol{\psi})^{p\text{-ord}})$$

denote the Hecke algebra of the space of $p$-ordinary group ring valued cusp forms generated over $R$ by the operators $T_\mathfrak{l}$ for $\mathfrak{l}\nmid\mathfrak{n}\mathfrak{P}'$, $U_\mathfrak{p}$ for $\mathfrak{p}\mid p$, and the diamond operators $S(\mathfrak{m})$. Note that the operators $S(\mathfrak{m})$ simply act by $\boldsymbol{\psi}(\mathfrak{m})\in R^*$. Let $\mathbf{T}\subset\tilde{\mathbf{T}}$ denote the sub-$R$-algebra generated by $T_\mathfrak{l}$ for $\mathfrak{l}\nmid\mathfrak{n}\mathfrak{P}'$, $U_\mathfrak{p}$ for $\mathfrak{p}\mid\mathfrak{P}$, and the $S(\mathfrak{m})$. In other words, the operators $U_\mathfrak{p}$ for $\mathfrak{p}\mid\mathfrak{P}'$ are excluded in the definition of $\mathbf{T}$.

Since our Hecke algebras include only the operators $T_\mathfrak{l}$ for $\mathfrak{l}$ not dividing the level and the operators $U_\mathfrak{p}$ for primes $\mathfrak{p}$ at which our forms are ordinary, the rings $\mathbf{T}$ and $\tilde{\mathbf{T}}$ are reduced. Let us be more explicit about this fact. Denote by $M$ the set of $p$-ordinary cuspidal newforms of weight $k$, level dividing $\mathfrak{n}\mathfrak{P}'$, and nebentypus $\psi$ for all characters $\psi\in\Psi$ (where $R=R_\Psi$). For each $f\in M$, we denote by $f_p$ the ordinary stabilization of $f$ with respect to all primes $\mathfrak{p}\mid p$. Suppose that the field $E$ with ring of integers $\mathcal{O}$ has been chosen large enough so that all the normalized Fourier coefficients $c(\mathfrak{a},f_p)$ lie in $\mathcal{O}$. Then there are $\mathcal{O}$-algebra injections with finite cokernels:

$$\mathbf{T}\longrightarrow\tilde{\mathbf{T}}\longrightarrow\prod_M\mathcal{O}$$

that send $T_\mathfrak{l}\mapsto(c(\mathfrak{l},f_p))_{f\in M}$, $U_\mathfrak{p}\mapsto(c(\mathfrak{p},f_p))_{f\in M}$; more succinctly we can write

$$t\mapsto(c(1,(f_p)|_t))_{f\in M}.$$

The injectivity of this map follows from the fact that any $p$-ordinary form $g$ of level $\mathfrak{n}\mathfrak{P}'$ can be written as a linear combination

$$g=\sum_{f\in M}\sum_{\mathfrak{b}}c_{f,\mathfrak{b}}(f_p)|_\mathfrak{b}$$

as $\mathfrak{b}$ ranges over the divisors of $\mathfrak{n}$ that are relatively prime to $\mathfrak{p}$ and such that $(f_p)|_{\mathfrak{b}}$ has level dividing $\mathfrak{n}\mathfrak{P}'$. Any element of $\mathbf{T}$ or $\tilde{\mathbf{T}}$ that annihilates every $f_p$ therefore annihilates every $g$. Finally, the fact that $\mathbf{T} \longrightarrow \prod_M \mathcal{O}$ has finite cokernel follows from multiplicity 1; for any distinct $f, f' \in M$, there exists $\mathfrak{l} \nmid \mathfrak{n}\mathfrak{P}'$ such that $c(\mathfrak{l}, f_p) \neq c(\mathfrak{l}, f'_p)$.

Using the group ring valued cusp form $F_k(\boldsymbol{\psi})$ constructed in §8, we now define a certain maximal ideal $\mathfrak{m} \subset \mathbf{T}$, the maximal Eisenstein ideal. Note that $F_k(\boldsymbol{\psi})$ is an eigenvector for the action of $\mathbf{T}$ modulo $x\Theta^{\#}$ or $\Theta^{\#}$, in cases 1 or 2, respectively. More precisely, for $\mathfrak{l} \nmid \mathfrak{n}\mathfrak{P}'$ we have

$$F_k(\boldsymbol{\psi})|_{T_{\mathfrak{l}}} \equiv \begin{cases} (\boldsymbol{\psi}(\mathfrak{l}) + \epsilon_{\mathrm{cyc}}^{k-1}(\mathfrak{l}))F_k(\boldsymbol{\psi}) & (\mathrm{mod}\ x\Theta^{\#}) \text{ in case 1} \\ (\boldsymbol{\psi}(\mathfrak{l}) + 1)F_k(\boldsymbol{\psi}) & (\mathrm{mod}\ \Theta^{\#}) \quad \text{in case 2.} \end{cases} \tag{108}$$

Here $\epsilon_{\mathrm{cyc}}$ is the $p$-adic cyclotomic character satisfying

$$\epsilon_{\mathrm{cyc}}(\mathfrak{l}) = \langle \mathrm{N}\mathfrak{l} \rangle \in \mathbf{Z}_p^*, \qquad \mathfrak{l} \nmid p.$$

We also have for all $\mathfrak{p} \mid \mathfrak{P}\mathfrak{P}''$:

$$F_k(\boldsymbol{\psi})|_{U_{\mathfrak{p}}} \equiv F_k(\boldsymbol{\psi}) \begin{cases} (\mathrm{mod}\ x\Theta^{\#}) & \text{in case 1b} \\ (\mathrm{mod}\ \Theta^{\#}) & \text{in case 2.} \end{cases} \tag{109}$$

Note that the congruences (108) and (109) are to be interpreted as in Remark 8.20.

**Lemma 8.22.** *Let $k_E$ denote the residue field of the $p$-adic local ring $\mathcal{O} = \mathcal{O}_E$. There is an $\mathcal{O}$-algebra homomorphism $\overline{\varphi}\colon \mathbf{T} \longrightarrow k_E$ given by*

- $\overline{\varphi}(T_{\mathfrak{l}}) = 1 + \chi(\mathfrak{l})$ *for* $\mathfrak{l} \nmid \mathfrak{n}p$.
- $\overline{\varphi}(U_{\mathfrak{p}}) = 1$ *for* $\mathfrak{p} \mid \mathfrak{P}$.
- $\overline{\varphi}(S(\mathfrak{m})) = \chi(\mathfrak{m})$.

*Proof.* The form $F_k(\boldsymbol{\psi})$ is an eigenform for the Hecke operators indicated modulo the maximal ideal $\mathfrak{m}_R$ of $R$. Note that $\mathfrak{m}_R$ is generated by the uniformizer $\pi_E$ of $\mathcal{O}$ along with the image of the elements $[g] - \chi(g)$ for $g \in G$, and $R/\mathfrak{m}_R \cong k_E$. The homomorphism $\overline{\varphi}$ is defined by sending each operator to its mod $\mathfrak{m}_R$ eigenvalue. □

We denote by $\mathfrak{m} \subset \mathbf{T}$ the kernel of $\overline{\varphi}$. We denote by $\mathbf{T}_{\mathfrak{m}}$ and $\tilde{\mathbf{T}}_{\mathfrak{m}} = \tilde{\mathbf{T}} \otimes_{\mathbf{T}} \mathbf{T}_{\mathfrak{m}}$ the $\mathfrak{m}$-adic completions of $\mathbf{T}$ and $\tilde{\mathbf{T}}$, respectively. We would also like to identify the $\mathfrak{m}$-adic completion of $\prod_{f \in M} \mathcal{O}$. Let $\overline{M} \subset M$ denote the set of $f \in M$ such that $c(1, (f_p)|_t) \equiv \overline{\varphi}(t) \pmod{\pi_E}$ for all $t \in \mathbf{T}$. We then have

$$\Big( \prod_{f \in M} \mathcal{O} \Big)_{\mathfrak{m}} = \prod_{f \in \overline{M}} \mathcal{O}.$$

The Artin-Rees Lemma ([1, Proposition 10.12]) yields injections with finite cokernel

$$\mathbf{T}_{\mathfrak{m}} \longrightarrow \tilde{\mathbf{T}}_{\mathfrak{m}} \longrightarrow \prod_{f \in \overline{M}} \mathcal{O}.$$

In the statement of the following theorem, $x$ is as in Lemma 8.16 in case 1a, and $x = 1$ in cases 1b and 2.

**Theorem 8.23.** *In both cases 1 and 2, there exists a non-zerodivisor $x \in R$, an $R/x\Theta^{\#}$-algebra $W$, and a surjective $R$-algebra homomorphism $\varphi\colon \tilde{\mathbf{T}}_{\mathfrak{m}} \longrightarrow W$ satisfying the following properties:*

- *The structure map $R/x\Theta^{\#} \longrightarrow W$ is an injection.*
- *The restriction of $\varphi$ to $\mathbf{T}_{\mathfrak{m}}$ takes values in $R/x\Theta^{\#} \subset W$. More precisely,*

$$\begin{aligned} \varphi(S(\mathfrak{m})) &= \boldsymbol{\psi}(\mathfrak{m}) \text{ for } \mathfrak{m} \in G_{\mathfrak{n}}^{+}, \\ \varphi(U_{\mathfrak{p}}) &= 1 \text{ for } \mathfrak{p} \mid \mathfrak{P}, \text{ and} \\ \varphi(T_{\mathfrak{l}}) &= \epsilon_{\mathrm{cyc}}^{k-1}(\mathfrak{l}) + \boldsymbol{\psi}(\mathfrak{l}) \text{ for } \mathfrak{l} \nmid \mathfrak{n}p. \end{aligned}$$

- *Let*

$$\tilde{U} = \prod_{\mathfrak{p} \mid \mathfrak{P}'} (U_{\mathfrak{p}} - \boldsymbol{\psi}(\mathfrak{p})) \in \tilde{\mathbf{T}}_{\mathfrak{m}}$$

  *and let $U = \varphi(\tilde{U})$. If $y \in R$ and $Uy = 0$ in $W$, then $y \in (\Theta^{\#})$.*

*Proof.* We consider case 1a, with $x$ as in Theorem 8.17, as the other cases are similar (and in fact easier). Let $\mathcal{C} = \prod_{\mathfrak{a} \subset \mathcal{O}_F} R/x\Theta^{\#}$ be the product of copies of $R/x\Theta^{\#}$, indexed by the set of nonzero ideals $\mathfrak{a} \subset \mathcal{O}_F$. There is an $R$-module homomorphism $c\colon S_k(\mathfrak{n}, R, \boldsymbol{\psi}) \longrightarrow \mathcal{C}$ that associates to each cusp form its collection of Fourier coefficients $c(\mathfrak{a}, f)$. There is an action of the Hecke operators on $\mathcal{C}$ given by the formula (97), and the map $c$ is Hecke equivariant.

Let $\mathcal{F}$ denote the image of the $\tilde{\mathbf{T}}$-span of the cusp form $F_k(\boldsymbol{\psi})$ given in Theorem 8.17 under the map $c$. This is a finite-type $R/x\Theta^{\#}$-module. We define $W$ to be the image of the canonical $R$-algebra homomorphism $\tilde{\mathbf{T}} \longrightarrow \mathrm{End}_{R/x\Theta^{\#}}(\mathcal{F})$. This construction yields a canonical surjective $R$-algebra map $\varphi\colon \tilde{\mathbf{T}} \longrightarrow W$ that sends a Hecke operator to its action on the Hecke span of $F_k(\boldsymbol{\psi})$ under the map $c$. In view of (108), we obtain

$$\varphi(T_{\mathfrak{l}}) = \epsilon_{\mathrm{cyc}}^{k-1}(\mathfrak{l}) + \boldsymbol{\psi}(\mathfrak{l})$$

for $\mathfrak{l} \nmid \mathfrak{n}p$. In particular the algebra $W$, viewed as a $\mathbf{T}$-module through the homomorphism $\varphi$, is $\mathfrak{m}$-adically complete and we obtain an induced map

$$\varphi\colon \tilde{\mathbf{T}}_{\mathfrak{m}} \longrightarrow W.$$

Let us verify the necessary properties. If $\alpha \in R$ has vanishing image in $W$, then $\alpha F_k(\boldsymbol{\psi}) \equiv 0 \pmod{x\Theta^{\#}}$. Analyzing the congruence (106) for $\mathfrak{m} = 1$ and $\mathfrak{m} = \mathfrak{p}$, for any $\mathfrak{p} \mid p$, yields:

$$\begin{aligned} (x-1)\alpha &\equiv 0 \pmod{x\Theta^{\#}} \\ ((1+\boldsymbol{\psi}(\mathfrak{p}))x - \boldsymbol{\psi}(\mathfrak{p}))\alpha &\equiv 0 \pmod{x\Theta^{\#}}. \end{aligned}$$

Multiplying the first congruence by $(1+\boldsymbol{\psi}(\mathfrak{p}))$ and subtracting the second yields $\boldsymbol{\psi}(\mathfrak{p})\alpha \equiv 0 \pmod{x\Theta^{\#}}$, whence $\alpha \equiv 0 \pmod{x\Theta^{\#}}$. This establishes the injectivity of $R/x\Theta^{\#} \longrightarrow W$.

For the last item we note that (105) yields

$$F_k(\boldsymbol{\psi})|_{\tilde{U}} \equiv xW_1(1,\psi_p) \pmod{x\Theta^{\#}}.$$

Therefore if $yF_k(\boldsymbol{\psi})|_{\tilde{U}} \equiv 0 \pmod{x\Theta^{\#}}$ for $y \in R$, then by considering the Fourier coefficient of $\mathfrak{m}=1$ we see that $xy \in (x\Theta^{\#})$ and hence $y \in (\Theta^{\#})$ since $x$ is a non-zerodivisor in $R$.

The result in cases 1b and 2 can be proved analogously with $x=1$. Note that in these cases, $\epsilon_{\mathrm{cyc}}^{k-1}(\mathfrak{l})=1$ in $W$ since $\Theta^{\#}$ divides $\epsilon_{\mathrm{cyc}}^{k-1}(\mathfrak{l})-1$ for $k-1$ divisible by $(p-1)p^{m'}$ and $m'$ sufficiently large. For this, it is essential that we are working on the trivial zero free quotient $R$, so $\Theta^{\#}$ is a non-zerodivisor. □

# 9 Galois representation and cohomology class

## 9.1 Galois representation associated to each eigenform

Let $f \in \overline{M}$, as defined before Theorem 8.23, and let $\psi$ denote the nebentypus of $f$. The work of Hida and Wiles [52, Theorems 1 and 2] establishes a continuous Galois representation

$$\rho_f \colon G_F \longrightarrow \mathrm{GL}_2(E)$$

satisfying the following properties:

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

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

$$\mathrm{char}(\rho_f(\mathrm{Frob}_{\mathfrak{l}}))(x) = x^2 - c(\mathfrak{l},f)x + \psi(\mathfrak{l})\epsilon_{\mathrm{cyc}}^{k-1}(\mathfrak{l}),$$

where $\epsilon_{\mathrm{cyc}}$ is the cyclotomic character.

(3) For all $\mathfrak{p} \mid p$, we have

$$\rho_f|_{G_{\mathfrak{p}}} \sim \begin{pmatrix} \psi\eta_{\mathfrak{p}}^{-1}\epsilon_{\mathrm{cyc}}^{k-1} & * \\ 0 & \eta_{\mathfrak{p}} \end{pmatrix}, \tag{110}$$

where $\eta_{\mathfrak{p}} \colon G_{\mathfrak{p}} \longrightarrow E^*$ is an unramified character given by $\eta_{\mathfrak{p}}(\mathrm{rec}(\varpi)) = c(\mathfrak{p}, f_p)$. Here $\varpi \in F_{\mathfrak{p}}$ is a uniformizer and $\mathrm{rec} \colon F_{\mathfrak{p}}^* \longrightarrow G_{\mathfrak{p}}^{\mathrm{ab}}$ is the local Artin reciprocity map. We denote by $V_{\mathfrak{p},f}$ the eigenspace of $\rho_f|_{G_{\mathfrak{p}}}$, i.e. the span of the vector $\binom{1}{0}$ in the basis for which (110) holds.

By Čebotarev and property (2) of $\rho_f$, we see that $\mathrm{char}(\rho_f(\sigma)) \in \mathcal{O}[x]$ for all $\sigma \in G_F$, and furthermore (since $f \in \overline{M}$) that

$$\mathrm{char}(\rho_f(\sigma)) \equiv (x-1)(x-\chi(\sigma)) \pmod{\pi_E}.$$

For this, recall that $\psi \equiv \chi \pmod{\pi_E}$.

Suppose that $\tau \in G_F$ such that $\chi(\tau) \neq 1$. For example, we may choose $\tau$ to be an element whose restriction to $H$ is the complex conjugation, so that $\chi(\tau) = -1$. Since $\chi$ is a prime-to-$p$ order character, $\chi(\tau) \neq 1$ implies $\chi(\tau) \not\equiv 1 \pmod{\pi_E}$, so Hensel's Lemma implies that $\rho_f(\sigma)$ has two distinct eigenvalues

$$\lambda_{1,f} \equiv 1 \pmod{\pi_E}, \qquad \lambda_{2,f} \equiv \chi(\tau) \pmod{\pi_E}.$$

Ribet's method involves comparing the "global" basis for $\rho_f$ given by the eigenvectors of $\rho_f(\tau)$ to the "local" basis indicated in (110). This argument, which Mazur [28] has called "Ribet's Wrench," does not succeed in our application if the global basis and local basis are the same. We must show, therefore, that $\tau$ can be chosen so that neither of the eigenspaces of $\rho_f(\tau)$ is equal to the eigenspace $V_{\mathfrak{p},f}$ appearing in property (3) of $\rho_f$, for any $\mathfrak{p} \mid p$. Furthermore, we must do this simultaneously for all the finitely many $f \in \overline{M}$.

For this, we distinguish two cases. We say that $f$ is a CM form if $\rho_f = \mathrm{Ind}_{G_L}^{G_F} \alpha$ where $L$ is a quadratic CM extension of $F$ and $\alpha$ is a $p$-adic Hecke character of $L$. The following lemma of Ribet, proved using a group theoretic study of $\mathrm{GL}_2$, is essential for our analysis:

**Lemma 9.1.** *Let $f$ be a cuspidal eigenform of weight $k > 1$. Suppose that $f$ is not a CM form. Then the restriction of $\rho_f$ to any finite index subgroup of $G_F$ is irreducible.*

*Proof.* Suppose that the restriction of $\rho_f$ to a finite index subgroup of $G_F$ is reducible. Then [37, Theorem 2.3] implies that $\rho_f$ is induced from an index 2 subgroup of $G_F$. Therefore the image of $\rho_f$ is projectively dihedral. Hence the fixed field of this index two subgroup is a CM field by [2, Page 2, Remark (ii)]. □

**Lemma 9.2.** *Let $f \in \overline{M}$ be a CM form associated to a quadratic CM extension $L/F$, and let $\mathfrak{p} \mid p$. The subspace $V_{\mathfrak{p},f}$ is not stable under $\rho_f(\tau)$ for any $\tau$ that restricts to the complex conjugation of $L$.*

*Proof.* Since $f$ is ordinary at $\mathfrak{p}$, the prime $\mathfrak{p}$ splits in the quadratic extension $L/F$. It follows that $G_\mathfrak{p} \subset G_L$. Yet $\rho_f = \mathrm{Ind}_{G_L}^{G_F} \alpha$ has two subspaces that are stable under all of $G_L$, hence $V_{\mathfrak{p},f}$ must be one of these subspaces (note that the characters of the semisimplification of $\rho|_{G_\mathfrak{p}}$ are distinct since one is ramified and the other is not, so $\rho|_{G_\mathfrak{p}}$ cannot be a scalar representation). If this subspace were invariant under any $\tau$ restricting to the complex conjugation of $L$, it would then be invariant under all of $G_F$, contradicting the irreducibility of $\rho_f$. The result follows. □

The following is a modification of Lemma 4.3 in [16].

**Proposition 9.3.** *There exists $\tau \in G_F$ such that $\tau$ restricts to the complex conjugation of $G$, and such that for all $f \in \overline{M}$ and $\mathfrak{p} \mid p$, the subspace $V_{\mathfrak{p},f}$ is not stable under $\rho_f(\tau)$.*

*Proof.* Let $H_0$ denote the compositum of $H$ with the CM fields $L$ associated to each CM form $f \in \overline{M}$. The field $H_0$ is a finite CM abelian extension of $F$. Let $\tau_0 \in \mathrm{Gal}(H_0/F)$ be the complex conjugation. Lemma 9.2 implies that any $\tau$ restricting to $\tau_0$ on $H_0$ satisifies the desired property for the CM forms $f \in \overline{M}$ and all $\mathfrak{p} \mid p$.

Now label the $V_{\mathfrak{p},f}$ for $f \in \overline{M}$ that are not CM forms and $\mathfrak{p} \mid p$ by $V_1, \ldots, V_n$. We will define $\tau$ inductively starting from the $(\tau_0, H_0)$ defined above as the base case. Let $1 \leq i \leq n$. Denote by $G_i \subset G_F$ the stabilizer of $V_i$ under $\rho_f$ (where $V_i = V_{\mathfrak{p},f}$ for some $\mathfrak{p}$). By Lemma 9.1, $G_i$ has infinite index in $G_F$. We can therefore select an element $\alpha_i \in \overline{F}$ that is fixed by $G_i$ and that does not lie in $H_{i-1}$. Let $H_i$ be the Galois closure of $H_{i-1}(\alpha_i)$ over $F$ and let $\tau_i \in \mathrm{Gal}(H_i/F)$ be any element that restricts to $\tau_{i-1}$ on $H_{i-1}$ and such that $\tau_i(\alpha_i) \neq \alpha_i$. Note that any $\tau \in G_F$ restricting to $\tau_i$ on $H_i$ moves $\alpha_i$ and hence does not lie in $G_i$, i.e. does not stabilize $V_i$ under $\rho_f$. It therefore suffices to let $\tau$ be any element that restricts to $\tau_n$ on $H_n$, and the proposition follows. □

We once and for all fix a $\tau$ as in Proposition 9.3 and choose the basis for each $\rho_f$ so that

$$\rho_f(\tau) = \begin{pmatrix} \lambda_{1,f} & 0 \\ 0 & \lambda_{2,f} \end{pmatrix},$$

where $\lambda_{1,f} \equiv 1 \pmod{\pi_E}$ and $\lambda_{2,f} \equiv \chi(\tau) \equiv -1 \pmod{\pi_E}$ as above. We write

$$\rho_f(\sigma) = \begin{pmatrix} a_f(\sigma) & b_f(\sigma) \\ c_f(\sigma) & d_f(\sigma) \end{pmatrix}.$$

For each $\mathfrak{p} \mid p$, we let

$$M_{f,\mathfrak{p}} = \begin{pmatrix} A_{f,\mathfrak{p}} & B_{f,\mathfrak{p}} \\ C_{f,\mathfrak{p}} & D_{f,\mathfrak{p}} \end{pmatrix} \in \mathrm{GL}_2(E)$$

denote a change of basis matrix relating this basis to the one giving the local form (110), i.e. such that

$$\begin{pmatrix} a_f(\sigma) & b_f(\sigma) \\ c_f(\sigma) & d_f(\sigma) \end{pmatrix} M_{f,\mathfrak{p}} = M_{f,\mathfrak{p}} \begin{pmatrix} \psi\eta_{\mathfrak{p}}^{-1}\epsilon_{\mathrm{cyc}}^{k-1}(\sigma) & * \\ 0 & \eta_{\mathfrak{p}}(\sigma) \end{pmatrix}$$

for all $\sigma \in G_{\mathfrak{p}}$. The key point of Proposition 9.3 is the following:

$$\text{for every } f \in \overline{M} \text{ and every } \mathfrak{p} \mid p, \text{ we have } A_{f,\mathfrak{p}} \neq 0 \text{ and } C_{f,\mathfrak{p}} \neq 0. \tag{111}$$

## 9.2 Galois representation associated to $\mathbf{T}_{\mathfrak{m}}$

Let

$$K = \mathrm{Frac}(\mathbf{T}_{\mathfrak{m}}) = \mathrm{Frac}(\prod_{f \in \overline{M}} \mathcal{O}) = \prod_{f \in \overline{M}} E. \tag{112}$$

Consider the Galois representation

$$\rho = \prod_{f \in \overline{M}} \rho_f \colon G_F \longrightarrow \mathrm{GL}_2(K).$$

Note that $\rho$ is continuous with respect to the $p$-adic topology on $K$ (since each factor $\rho_f$ is continuous) and hence continuous with respect to the $\mathfrak{m}$-adic toplogy on $K$, as every ideal $\mathfrak{m}^n$ is finitely generated over $\mathcal{O}$. The representation $\rho$ satisfies:

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

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

$$\mathrm{char}(\rho(\mathrm{Frob}_\mathfrak{l}))(x) = x^2 - T_\mathfrak{l} x + \boldsymbol{\psi}(\mathfrak{l})\epsilon_{\mathrm{cyc}}^{k-1}(\mathfrak{l}), \tag{113}$$

where $\epsilon_{\mathrm{cyc}}$ is the cyclotomic character.

(3) For all $\mathfrak{p} \mid p$, we have

$$\rho|_{G_\mathfrak{p}} \sim \begin{pmatrix} \boldsymbol{\psi}\eta_\mathfrak{p}^{-1}\epsilon_{\mathrm{cyc}}^{k-1} & * \\ 0 & \eta_\mathfrak{p} \end{pmatrix}, \tag{114}$$

where $\eta_\mathfrak{p} \colon G_\mathfrak{p} \longrightarrow \tilde{\mathbf{T}}^*$ is the unramified character given by $\eta_\mathfrak{p}(\mathrm{rec}(\varpi)) = U_\mathfrak{p}$.

By Čebotarev and (113), it follows that $\mathrm{char}\,\rho(\sigma)(x) \in \mathbf{T}_\mathfrak{m}[x]$ for all $\sigma \in G_F$, and furthermore, that

$$\mathrm{char}\,\rho(\sigma)(x) \equiv (x-1)(x-\chi(\sigma)) \pmod{\mathfrak{m}}.$$

Recall the $\tau \in G_F$ fixed in the previous section, for which $\chi(\tau) = -1$. The polynomial $\mathrm{char}(\rho(\tau))$ has two distinct roots modulo $\mathfrak{m}$ and hence by Hensel's lemma has two distinct roots $\lambda_1, \lambda_2 \in \mathbf{T}_\mathfrak{m}^*$, with $\lambda_1 \equiv 1 \pmod{\mathfrak{m}}$ and $\lambda_2 \equiv -1 \pmod{\mathfrak{m}}$.

As in §9.1, we choose the basis for $\rho$ in which $\rho(\tau) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ and for a general $\sigma \in G_F$ we write

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

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

$$\begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} M_\mathfrak{p} = M_\mathfrak{p} \begin{pmatrix} \boldsymbol{\psi}\eta_\mathfrak{p}^{-1}\epsilon_{\mathrm{cyc}}^{k-1} & * \\ 0 & \eta_\mathfrak{p} \end{pmatrix} \tag{115}$$

for all $\sigma \in G_\mathfrak{p}$. Here $A_\mathfrak{p} = (A_{f,\mathfrak{p}})_{f \in \overline{M}}$ under the identification (112), and similarly for $B_\mathfrak{p}, C_\mathfrak{p}, D_\mathfrak{p}$. Therefore, (111) implies that the elements $A_\mathfrak{p}$ and $C_\mathfrak{p}$ are invertible in $K$. Comparing the top left corner elements in (115) gives

$$b(\sigma) = \frac{A_\mathfrak{p}}{C_\mathfrak{p}}(\boldsymbol{\psi}\eta_\mathfrak{p}^{-1}\epsilon_{\mathrm{cyc}}^{k-1}(\sigma) - a(\sigma)) \tag{116}$$

for all $\sigma \in G_\mathfrak{p}$.

## 9.3 Cohomology Class and Ramification away from $p$

In this section we construct a Galois cohomology class associated to the homomorphism $\varphi$ constructed in Theorem 8.23. Let $\tilde{I} \subset \tilde{\mathbf{T}}_{\mathfrak{m}}$ denote the kernel of $\varphi$ and let $I = \tilde{I} \cap \mathbf{T}_{\mathfrak{m}}$ denote the kernel of $\varphi|_{\mathbf{T}_{\mathfrak{m}}}$.

We begin by employing some standard techniques in the theory of pseudo-representations. As noted above, we have $\operatorname{Tr}\rho(\sigma) \in \mathbf{T}_{\mathfrak{m}}$ for all $\sigma \in G_F$. Furthermore, in view of (113) and the property $\varphi(T_{\mathfrak{l}}) = \epsilon_{\mathrm{cyc}}^{k-1}(\mathfrak{l}) + \boldsymbol{\psi}(\mathfrak{l})$, we find from Čebotarev that

$$\operatorname{Tr}\rho(\sigma) = a(\sigma) + d(\sigma) \equiv \epsilon_{\mathrm{cyc}}^{k-1}(\sigma) + \boldsymbol{\psi}(\sigma) \pmod{I} \qquad \text{for all } \sigma \in G_F. \tag{117}$$

In particular, for the fixed element $\tau$ introduced in §9.1–9.2, we obtain

$$\lambda_1 + \lambda_2 \equiv \epsilon_{\mathrm{cyc}}^{k-1}(\tau) + \boldsymbol{\psi}(\tau) \pmod{I}$$

and hence $\lambda_1, \lambda_2$ are roots of the polynomial

$$(x - \epsilon_{\mathrm{cyc}}^{k-1}(\tau))(x - \boldsymbol{\psi}(\tau)) \pmod{I}. \tag{118}$$

Since $\lambda_1 \equiv 1 \equiv \epsilon_{\mathrm{cyc}}^{k-1}(\tau) \pmod{\mathfrak{m}}$ and $\lambda_2 \equiv \chi(\tau) \equiv \boldsymbol{\psi}(\tau) \pmod{\mathfrak{m}}$, with $\lambda_1 \not\equiv \lambda_2 \pmod{\mathfrak{m}}$, it follows from (118) that

$$\lambda_1 \equiv \epsilon_{\mathrm{cyc}}^{k-1}(\tau) \pmod{I}, \qquad \lambda_2 \equiv \boldsymbol{\psi}(\tau) \pmod{I}.$$

The congruence (117) with $\sigma$ replaced by $\sigma\tau$ yields

$$\begin{aligned} a(\sigma)\lambda_1 + d(\sigma)\lambda_2 &\equiv \epsilon_{\mathrm{cyc}}^{k-1}(\sigma\tau) + \boldsymbol{\psi}(\sigma\tau) \\ &\equiv \epsilon_{\mathrm{cyc}}^{k-1}(\sigma)\lambda_1 + \boldsymbol{\psi}(\sigma)\lambda_2. \end{aligned} \tag{119}$$

The two congruences (117) and (119) may be solved, again using $\lambda_1 \not\equiv \lambda_2 \pmod{\mathfrak{m}}$, to yield

$$a(\sigma) \equiv \epsilon_{\mathrm{cyc}}^{k-1}(\sigma) \pmod{I}, \qquad d(\sigma) \equiv \boldsymbol{\psi}(\sigma) \pmod{I} \tag{120}$$

for all $\sigma \in G_F$ (in particular $a(\sigma), d(\sigma) \in \mathbf{T}_{\mathfrak{m}}$).

Let $B_0$ be the $\mathbf{T}_{\mathfrak{m}}$-submodule of $K$ generated by $\{b(\sigma)\colon \sigma \in G_F\}$, and let $B$ be any $\mathbf{T}_{\mathfrak{m}}$-submodule of $K$ containing $B_0$. Let $B' \subset B$ be any $\mathbf{T}_{\mathfrak{m}}$-submodule containing $IB_0$. Put $\overline{B} = B/B'$. Since $\rho$ is a representation, we have

$$b(\sigma\sigma') = a(\sigma)b(\sigma') + b(\sigma)d(\sigma'), \qquad \sigma, \sigma' \in G_F.$$

The congruences (120) imply that

$$\overline{b}(\sigma\sigma') \equiv \epsilon_{\mathrm{cyc}}^{k-1}(\sigma)\overline{b}(\sigma') + \boldsymbol{\psi}(\sigma')\overline{b}(\sigma) \quad \text{in } \overline{B},$$

where $\overline{b}(\sigma)$ denotes the image of $b(\sigma)$ in $\overline{B}$. It follows that the function

$$\sigma \mapsto \overline{b}(\sigma)\boldsymbol{\psi}(\sigma)^{-1} \tag{121}$$

is a 1-cocycle yielding a class $\kappa \in H^1(G_F, \overline{B}(\boldsymbol{\psi}^{-1}\epsilon_{\mathrm{cyc}}^{k-1}))$. If furthermore $p^m B \subset B'$ and $k \equiv 1 \pmod{(p-1)p^N}$ with $N \geq m$ (so that $\epsilon_{\mathrm{cyc}}^{k-1} \equiv 1 \pmod{p^m}$), then multiplication by $\epsilon_{\mathrm{cyc}}^{k-1}$ acts trivially on $\overline{B}$, and $\kappa$ may be viewed as a class

$$\kappa \in H^1(G_F, \overline{B}(\boldsymbol{\psi}^{-1})). \tag{122}$$

**Proposition 9.4.** *Let $\overline{B}$ be as above. The class $\kappa \in H^1(G_F, \overline{B}(\boldsymbol{\psi}^{-1}))$ defined by (121) is unramified away from $\mathfrak{n}p$, i.e. its restriction to*

$$H^1(I_v, \overline{B}(\boldsymbol{\psi}^{-1}))$$

*vanishes for places $v \nmid \mathfrak{n}p$ of $F$. Furthermore, for $v \mid \mathfrak{n}, v \nmid p$, the class $\kappa$ is at most tamely ramified, i.e. its restriction to the wild inertia subgroup $I_{v,1} \subset I_v$ vanishes.*

*Proof.* The first property is trivial, since $\rho$ is unramified outside $\mathfrak{n}p$, so

$$b(\sigma) = 0 \text{ for } \sigma \in I_v, v \nmid \mathfrak{n}p.$$

Now for any $v$, the wild inertia group $I_{v,1}$ is a pro-$v$ group while the module $\overline{B}$ is a pro-$p$-group. It follows from continuity of cocycles that for $v \nmid p$ the entire space

$$H^1(I_{v,1}, \overline{B}(\boldsymbol{\psi}^{-1}))$$

is trivial. □

## 9.4 Surjection from $\nabla$

We recall the sets $\Sigma, \Sigma'$ from §4:

$$\Sigma = \{v \in S_{\mathrm{ram}} \colon v \mid p\} \cup S_\infty,$$
$$\Sigma' = \{v \in S_{\mathrm{ram}} : v \nmid p\} \cup T.$$

Recall from §4.1 that we may assume $T$ contains no primes above $p$.

As above let $B_0$ denote the $\mathbf{T}_{\mathfrak{m}}$-submodule of $K$ generated by the $b(\sigma)$ for all $\sigma \in G_F$. Define $B$ to be the $\mathbf{T}_{\mathfrak{m}}$-submodule of $K$ generated by $B_0$ and by the elements $A_{\mathfrak{p}}/C_{\mathfrak{p}}$ appearing in (115)–(116) for all finite $\mathfrak{p} \in \Sigma$:

$$B = (B_0, A_{\mathfrak{p}}/C_{\mathfrak{p}} \colon \mathfrak{p} \in \Sigma - S_\infty).$$

In case 1, when $\Sigma = S_\infty$, we have $B_0 = B$.

Let $B'$ be the $\mathbf{T}_{\mathfrak{m}}$-submodule of $B$ generated by $b(\sigma)$ for $\sigma \in I_{\mathfrak{p}}$, as $\mathfrak{p}$ ranges over all primes dividing $\mathfrak{P}'$; these are the primes above $p$ that do not ramify in $H/F$. Define

$$\overline{B}_p = B/(IB, B', p^m B).$$

Let $\overline{B}_0 \subset \overline{B}_p$ be the image of $B_0$ in $\overline{B}_p$.

**Proposition 9.5.** *The cohomology class $\kappa \in H^1(G_F, \overline{B}_0(\boldsymbol{\psi}^{-1}))$ defined in (122) is unramified away from $\Sigma'$, tamely ramified at $\Sigma'$, and locally trivial at $\Sigma$.*

*Proof.* We saw in Proposition 9.4 that $\kappa$ is unramified away from $\Sigma \cup \Sigma' \cup \{\mathfrak{p} \mid p\}$, and that it is tamely ramified at $\Sigma'$. For the primes $\mathfrak{p} \mid p$ not in $\Sigma$, the class $\kappa$ is unramified because in the definition of $\overline{B}_p$ we have taken the quotient by the image of inertia under $b$.

The local triviality of $\kappa$ at infinite places is automatic, since $p$ is odd. It remains to show that $\kappa$ is locally trivial at all finite $\mathfrak{p} \in \Sigma$. For this, we use equation (116). By definition, $A_\mathfrak{p}/C_\mathfrak{p} \in B$ and hence $(A_\mathfrak{p}/C_\mathfrak{p})I \equiv 0$ in $\overline{B}$. Furthermore $\eta_\mathfrak{p} \equiv 1 \pmod{I}$ since $\varphi(U_\mathfrak{p}) = 1$ for $\mathfrak{p} \in \Sigma$. This part of the argument is relevant only when $\Sigma \neq S_\infty$, i.e. case 2. As noted at the end of the proof of Theorem 8.23, in this case we have $\epsilon_{\mathrm{cyc}}^{k-1} \equiv 1 \pmod{I}$. Therefore $a(\sigma) \equiv 1 \pmod{I}$ as well.

Combining these observations, we see that

$$b(\sigma)\boldsymbol{\psi}^{-1}(\sigma) \equiv (1 - \boldsymbol{\psi}^{-1}(\sigma))\frac{A_\mathfrak{p}}{C_\mathfrak{p}} \quad \text{in } \overline{B}_p \text{ for } \sigma \in G_\mathfrak{p}. \tag{123}$$

Therefore $\kappa|_{G_\mathfrak{p}}$ is a coboundary as desired. □

As in §6.2, let $L/H$ be the finite abelian extension of $H$ associated to $\mathrm{Cl}_\Sigma^{\Sigma'}(H)^-$ by class field theory, i.e. such that the Artin reciprocity map yields an isomorphism

$$\mathrm{rec}_{L/H} \colon \mathrm{Cl}_\Sigma^{\Sigma'}(H)^- \longrightarrow \mathrm{Gal}(L/H).$$

$L$ is the maximal abelian extension of $H$ of odd degree unramified outside of $\Sigma'_H$, tamely ramified at $\Sigma'_H$, split completely at $\Sigma_H$, and such that the conjugation action of complex conjugation is equal to inversion on $\mathrm{Gal}(L/H)$.

It is natural to consider $\overline{B}_0(\boldsymbol{\psi}^{-1})$ as an $R^\#$-module. This is the space $\overline{B}_0$ in which the action of $R^\#$ is given by

$$(r, b) \mapsto r^\# \cdot b,$$

with the action on the right the usual action of $R$ on $\overline{B}_0$. With this notation, the $G$-module action on $\overline{B}_0(\boldsymbol{\psi}^{-1})$ is consistent with the $R^\#$-module action via the projection $\mathcal{O}[G] \longrightarrow R^\#$.

**Corollary 9.6.** *There is a canonical $R^\#$-module surjection*

$$\alpha \colon \mathrm{Cl}_\Sigma^{\Sigma'}(H)_{R^\#} \longrightarrow \overline{B}_0(\boldsymbol{\psi}^{-1})$$

*induced by $\alpha(\mathfrak{a}) = \overline{b}(\sigma)$ for $\mathfrak{a} \in \mathrm{Cl}_\Sigma^{\Sigma'}(H)$, where $\sigma$ denotes any lift of $\mathrm{rec}_{L/H}(\mathfrak{a})$ to $G_H \subset G_F$.*

*Proof.* The character $\boldsymbol{\psi}$ acts through $G = \mathrm{Gal}(H/F)$, so its restriction to $G_H$ is trivial. We consider the restriction

$$\kappa_H = \mathrm{res}_{G_H}^{G_F} \kappa \in H^1(G_H, \overline{B}_0)^{G=\boldsymbol{\psi}^{-1}} = \mathrm{Hom}_{\mathrm{cont}}(G_H^{\mathrm{ab}}, \overline{B}_0)^{G=\boldsymbol{\psi}^{-1}}.$$

The superscript indicates that we consider the space of continuous homomorphisms that are $G$-equivariant, where $G$ acts on $G_H^{\mathrm{ab}}$ via conjugation by a lift to $G_H$ and on $\overline{B}_0$ via the character $\boldsymbol{\psi}^{-1}$.

By Proposition 9.5, the fixed field of the kernel of the homomorphism $\kappa_H$, which we denote $L'$, is unramified outside of $\Sigma'_H$, tamely ramified at $\Sigma'_H$, and split completely at $\Sigma_H$. Therefore $L' \subset L$ and we get maps

$$\mathrm{Cl}_\Sigma^{\Sigma'}(H)^- \xrightarrow{\mathrm{rec}_{L/H}} \mathrm{Gal}(L/H) \twoheadrightarrow \mathrm{Gal}(L'/H) \xrightarrow{\kappa_H} \overline{B}_0(\boldsymbol{\psi}^{-1}). \tag{124}$$

Furthermore these maps are $G$-equivariant (where on the middle two terms $G$ acts by conjugation, and as indicated $G$ acts on $\overline{B}_0$ via $\boldsymbol{\psi}^{-1}$). By construction, the composition of maps in (124) is given by $\mathfrak{a} \mapsto \overline{b}(\sigma)$, with notation as in the statement of the corollary. It remains to prove that if we extend scalars to $R^\#$, then the induced map

$$\alpha\colon \mathrm{Cl}_\Sigma^{\Sigma'}(H)_{R^\#} \longrightarrow \overline{B}_0(\boldsymbol{\psi}^{-1})$$

is surjective. Denote by $B_\alpha$ the image of $\alpha$, and write $\overline{B}^\alpha = \overline{B}_0/B_\alpha$. By construction, $B_\alpha$ contains $\overline{b}(\sigma)$ for all $\sigma \in G_H$, so the image of $\kappa_H$ in $H^1(G_H, \overline{B}^\alpha)$ is trivial. By Lemma 6.3, this implies that the image of $\kappa$ in $H^1(G_F, \overline{B}^\alpha(\boldsymbol{\psi}^{-1}))$, denoted $\kappa^\alpha$, is trivial. Yet if we write $\kappa^\alpha$ as a coboundary:

$$\kappa^\alpha(\sigma) = (1 - \boldsymbol{\psi}^{-1}(\sigma))t$$

for $t \in \overline{B}^\alpha$, then evaluating at $\sigma = \tau$ shows that $t = 0$ (since $\kappa(\tau) = 0$ and $\boldsymbol{\psi}(\tau) = -1$). Therefore $\kappa^\alpha$ is zero as a cocycle, not just as a cohomology class. But the values of the cocycle $\kappa$ generate the module $B_0$, and hence $\kappa^\alpha$ generates the module $\overline{B}^\alpha$. It follows that $\overline{B}^\alpha = 0$, i.e. that $\alpha$ is surjective. □

Next we consider the quotient $\mathbf{T}_\mathfrak{m}$-module $\overline{B}_1 = \overline{B}_p/\overline{B}_0$. This module is generated by the $A_\mathfrak{p}/C_\mathfrak{p}$ for finite $\mathfrak{p} \in \Sigma$. In fact, since the definition of $\varphi$ implies that every element of $\mathbf{T}_\mathfrak{m}$ is congruent modulo $I$ to an element of $R$, it follows that $\overline{B}_1$ is generated over $R$ by the $A_\mathfrak{p}/C_\mathfrak{p}$.

**Proposition 9.7.** *There is a canonical $R^\#$-module surjection*

$$\gamma\colon (X_{H,\Sigma})_{R^\#} \longrightarrow \overline{B}_1(\boldsymbol{\psi}^{-1}).$$

*Proof.* By construction there is a canonical $R$-module surjection

$$\gamma\colon \bigoplus_{\mathfrak{p}\in\Sigma} R^\# \longrightarrow \overline{B}_1(\boldsymbol{\psi}^{-1})$$

that sends a basis vector associated to $\mathfrak{p} \in \Sigma$ to $-A_\mathfrak{p}/C_\mathfrak{p}$.

Since $R^{\#}$ is a quotient of a component of $\mathcal{O}[G]$ corresponding to an odd (and in particular nontrivial) character $\chi^{-1}$, we have

$$(X_{H,\Sigma})_{R^{\#}} \cong (Y_{H,\Sigma})_{R^{\#}} = \bigoplus_{\mathfrak{p}\in\Sigma} (\mathbf{Z}[G/G_{\mathfrak{p}}] \otimes_{\mathbf{Z}[G]} R^{\#}) \cong \bigoplus_{\mathfrak{p}\in\Sigma} R^{\#}/\Delta G_{\mathfrak{p}}.$$

Here $G_{\mathfrak{p}} \subset G$ is the decomposition group at $\mathfrak{p}$ in $G$ and $\Delta G_{\mathfrak{p}} \subset R^{\#}$ is the ideal generated by $\boldsymbol{\psi}(g) - 1$ for $g \in G_{\mathfrak{p}}$. To show that the map $\gamma$ factors through $(X_{H,\Sigma})_{R^{\#}}$, we must show that

$$(\boldsymbol{\psi}(g) - 1)\frac{A_{\mathfrak{p}}}{C_{\mathfrak{p}}} \equiv 0 \quad \text{in } \overline{B}_1(\boldsymbol{\psi}^{-1}).$$

This follows directly from (123). The left side of that congruence vanishes in the quotient $\overline{B}_1$ of $\overline{B}_p$. □

Combining Corollary 9.6, Proposition 9.7, and the sequence (77), we have constructed the solid arrows in a commutative diagram as follows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Cl}_{\Sigma}^{\Sigma'}(H)_{R^{\#}} & \longrightarrow & \nabla_{\Sigma}^{\Sigma'}(H)_{R^{\#}} & \longrightarrow & (X_{H,\Sigma})_{R\#} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \vdots{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & \overline{B}_0(\boldsymbol{\psi}^{-1}) & \longrightarrow & \overline{B}_p(\boldsymbol{\psi}^{-1}) & \longrightarrow & \overline{B}_1(\boldsymbol{\psi}^{-1}) & \longrightarrow & 0. \end{array} \tag{125}$$

**Theorem 9.8.** *There exists an $R$-module surjection $\beta\colon \nabla_{\Sigma}^{\Sigma'}(H)_{R^{\#}} \twoheadrightarrow \overline{B}_p(\boldsymbol{\psi}^{-1})$ completing the commutative diagram (125).*

*Proof.* As we now explain, the essential content of this theorem is property (P2), i.e. Lemma 6.4, which gives a Galois cohomological interpretation of the extension class corresponding to $\nabla_{\Sigma}^{\Sigma'}(H)^{-}$. Let

$$\eta_1 \in \mathrm{Ext}^1_{R^{\#}}((X_{H,\Sigma})_{R^{\#}}, \mathrm{Cl}_{\Sigma}^{\Sigma'}(H)_{R^{\#}}),$$
$$\eta_2 \in \mathrm{Ext}^1_{R^{\#}}(\overline{B}_1(\boldsymbol{\psi}^{-1}), \overline{B}_0(\boldsymbol{\psi}^{-1}))$$

be the extension classes corresponding to the rows of the diagram (125). Pushout by $\alpha$ and pullback by $\gamma$, respectively, yield classes

$$\alpha_*\eta_1, \gamma^*\eta_2 \in \mathrm{Ext}^1_{R^{\#}}((X_{H,\Sigma})_{R^{\#}}, \overline{B}_0(\boldsymbol{\psi}^{-1})).$$

Proving that $\alpha_*\eta_1 = \gamma^*\eta_2$ will yield the desired result. For then, if we let $Z_1, Z_2$ denote

$R$-modules representing these extension classes, we obtain a commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Cl}_\Sigma^{\Sigma'}(H)_{R^\#} & \longrightarrow & \nabla_\Sigma^{\Sigma'}(H)_{R^\#} & \longrightarrow & (X_{H,\Sigma})_{R^\#} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow & & \| & & \\
0 & \longrightarrow & \overline{B}_0(\boldsymbol{\psi}^{-1}) & \longrightarrow & Z_1 & \longrightarrow & (X_{H,\Sigma})_{R^\#} & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \wr} & & \| & & \\
0 & \longrightarrow & \overline{B}_0(\boldsymbol{\psi}^{-1}) & \longrightarrow & Z_2 & \longrightarrow & (X_{H,\Sigma})_{R^\#} & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow{\scriptstyle \gamma} & & \\
0 & \longrightarrow & \overline{B}_0(\boldsymbol{\psi}^{-1}) & \longrightarrow & \overline{B}_p(\boldsymbol{\psi}^{-1}) & \longrightarrow & \overline{B}_1(\boldsymbol{\psi}^{-1}) & \longrightarrow & 0.
\end{array} \tag{126}$$

The desired surjection $\beta$ is given by composition of the middle vertical arrows.

To prove $\alpha_*\eta_1 = \gamma^*\eta_2$, we interpret these extension classes in terms of Galois cohomology using the isomorphism

$$\mathrm{Ext}^1_{R^\#}((X_{H,\Sigma})_{R^\#}, \overline{B}_0(\boldsymbol{\psi}^{-1})) \cong \bigoplus_{v\in\Sigma} H^1(G_v, \overline{B}_0(\boldsymbol{\psi}^{-1})) \tag{127}$$

described in (83). We will show that the component at $v$ for both $\alpha_*\eta_1$ and $\gamma^*\eta_2$ is equal to the unique class whose inflation to $H^1(G_{F_v}, \overline{B}_0(\boldsymbol{\psi}^{-1}))$ is $\mathrm{res}^{G_F}_{G_{F,v}}\kappa$.

Lemma 6.4 implies that under the isomorphism (127), we have $\alpha_*\eta_1 = (\alpha_*\lambda_v)_{v\in\Sigma}$ where $\lambda_v$ is the cohomology class defined in §6.2. Reviewing this definition, the class $\alpha_*\lambda_v$ is given as follows. Consider the class in

$$H^1(G_H, \overline{B}_0(\boldsymbol{\psi}^{-1})) = \mathrm{Hom}_{\mathrm{cont}}(G_H, \overline{B}_0(\boldsymbol{\psi}^{-1}))$$

given by the composition of the homomorphisms

$$G_H \longrightarrow \mathrm{Gal}(L/H) \xrightarrow{\mathrm{rec}^{-1}_{L/H}} \mathrm{Cl}_\Sigma^{\Sigma'}(H)^- \xrightarrow{\alpha} \overline{B}_0(\boldsymbol{\psi}^{-1}).$$

By the explicit formula for $\alpha$ given in Corollary 9.6, this composition is simply $\sigma \mapsto \bar{b}(\sigma)$ for $\sigma \in G_H$. Next we must lift this homomorphism to a (unique) class in $H^1(G_F, \overline{B}_0(\boldsymbol{\psi}^{-1}))$; but of course we already have a specific lift, namely $\kappa$. The class $\alpha_*\lambda_v \in H^1(G_v, \overline{B}_0(\boldsymbol{\psi}^{-1}))$ is then by definition the unique class whose inflation is equal to $\mathrm{res}^{G_F}_{G_{F,v}}\kappa \in H^1(G_{F_v}, \overline{B}_0(\boldsymbol{\psi}^{-1}))$.

Next we compute $\gamma^*\eta_2$ in these Galois cohomological terms using the explication of the isomorphism (127) given in the discussion between (83) and Lemma 6.4. Let

$$\gamma_v \in H^1(G_v, \overline{B}_0(\boldsymbol{\psi}^{-1}))$$

denote the component at $v \in \Sigma$ of $\gamma^*\eta_2$. Then by the definition of $\gamma$ and in view of (84), we have

$$\gamma_v(g) = (1 - \boldsymbol{\psi}^{-1}(g))\frac{A_v}{C_v}, \quad g \in G_v.$$

By our favorite equation (123), the right hand side has image $\kappa(\sigma)$ in $\overline{B}_0(\boldsymbol{\psi}^{-1})$, where $\sigma$ is any lift of $g$ to $G_{F,v}$. In other words, $\gamma_v$ is the unique class whose inflation is equal to $\mathrm{res}^{G_F}_{G_{F,v}} \kappa \in H^1(G_{F_v}, \overline{B}_0(\boldsymbol{\psi}^{-1}))$. This was the same description of $\alpha_*\lambda$ given above.

This concludes the proof that $\alpha_*\eta_1 = \gamma^*\eta_2$ and completes the proof of the theorem. □

## 9.5 Calculation of Fitting Ideal

In this section we will prove that

$$\mathrm{Fitt}_R(\overline{B}_p) \subset (\Theta^{\#})$$

(note we have not twisted by $\boldsymbol{\psi}^{-1}$ here) and use this to conclude the desired result

$$\mathrm{Fitt}_R(\mathrm{Sel}^{\Sigma'}_{\Sigma}(H)_R) \subset (\Theta^{\#}).$$

**Lemma 9.9.** *The module $B_0$ can be generated over $R$ by finitely many elements $b_1, \ldots, b_n$ that are non-zerodivisors (i.e. invertible) in $K = \mathrm{Frac}(\mathbf{T}_{\mathfrak{m}})$.*

*Proof.* Recall that $K = \mathrm{Frac}(\mathbf{T}_{\mathfrak{m}}) = \prod_{f \in \overline{M}} E$, with each factor corresponding to a cuspidal eigenform $f$, and $E = \mathrm{Frac}(\mathcal{O})$ a finite extension of $\mathbf{Q}_p$. We will denote the $i$th factor $E$ in this finite product as $E_i$, and the corresponding eigenform by $f_i$. The homomorphism $\rho$ is continuous and hence $B_0$ is a compact subset of $K$. It is therefore finitely generated over $\mathcal{O}$ and hence finitely generated over $R$.

Suppose we start with any finite generating set $b_1, \ldots, b_n$. We claim we can alter these generators such that each $b_i$ is a non-zerodivisor in $K$, i.e. such that the projection of each $b_i$ to each factor $E_j$ is nonzero. We prove this by induction on the total number of zero projections of the $b_i$ onto the $E_j$. Suppose that $b_i$ has zero projection onto some factor $E_j$. Since the individual representations $\rho_{f_j}$ are irreducible, some other $b_k$ must have nonzero projection onto $E_j$. If we replace $b_i$ by $b_i + tb_k$ for any nonzero $t \in \mathcal{O}$, the new $b_i$ has nonzero projection onto $E_j$. Furthermore, at most finitely many $t$ introduce a new zero projection of $b_i$ onto some other $E_{j'}$. Avoiding these finitely many $t$, we can choose a $t$ that decreases the total number of zeros. Furthermore, the replacement $b_i \mapsto b_i + tb_k$ does not change the span of the $b_i$, and hence preserves the property that they generate $B_0$ over $R$. Continuing in this fashion, we can repeatedly reduce the number of zero projections of the $b_i$ on to the $E_j$ until there are none remaining. This concludes the proof. □

**Theorem 9.10.** *We have* $\mathrm{Fitt}_R(\overline{B}_p) \subset (\Theta^{\#})$.

*Proof.* Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ denote the primes of $F$ above $p$ not contained in $\Sigma$ (i.e. those dividing $\mathfrak{P}'$). For each $\mathfrak{p}_i$, choose an element $\sigma_i \in G_{\mathfrak{p}_i} \subset G_F$ that lifts $\mathrm{rec}(\varpi_i^{-1}) \in G^{\mathrm{ab}}_{\mathfrak{p}_i}$, where $\varpi_i$ is a uniformizer for $F_{\mathfrak{p}_i}$. By (116) we have

$$c_i := b(\sigma_i)\boldsymbol{\psi}(\mathfrak{p}_i)\epsilon^{1-k}_{\mathrm{cyc}}(\sigma_i) = \frac{A_i}{C_i}(U_{\mathfrak{p}_i} - \boldsymbol{\psi}(\mathfrak{p}_i) + I) \in B.$$

Here and throughout this proof, we use the notation $a = b + I$ to mean $a = b + z$ for some $z \in I$ to avoid needing to add distinct variable names for each such $z$ that appears. We have also written $A_i/C_i$ for $A_{\mathfrak{p}_i}/C_{\mathfrak{p}_i}$.

Let $b_1, \dots, b_n$ be $R$-module generators of $B$ that are not zerodivisors in $K$; we can choose the generators of $B_0$ as given by Lemma 9.9 along with the $A_{\mathfrak{p}}/C_{\mathfrak{p}}$ for finite $\mathfrak{p} \in \Sigma$. To calculate $\mathrm{Fitt}_R(\overline{B}_p)$ we use the generating set $c_1, \dots, c_r, b_1, \dots, b_n$ for $\overline{B}_p$. Of course, these first $r$ generators are not necessary, but including them will aid us in proving the theorem. Suppose we have a matrix

$$M \in M_{(n+r)\times(n+r)}(R)$$

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

$$M(c_1, \dots, c_r, b_1, \dots, b_n)^T \equiv 0 \text{ in } (\overline{B}_p)^{n+r}.$$

By definition of Fitting ideal, the theorem will follow if we can show that $\det(M) \in (\Theta^{\#})$.

Write $M = (W|Z)$ in block matrix form, where

$$W = (w_{ij}) \in M_{(n+r)\times r}(R), \qquad Z = (z_{ij}) \in M_{(n+r)\times n}(R).$$

Note that by (116), since $\boldsymbol{\psi}$ and $\eta_{\mathfrak{p}_i}$ are unramified at $\mathfrak{p}_i$ and $a(\sigma) \equiv \epsilon_{\mathrm{cyc}}^{k-1} \pmod{I}$, we have

$$b(I_{\mathfrak{p}_i}) \subset \frac{A_i}{C_i} I.$$

Also, since the $b_i$ generate $B$, every element of $IB$ can be written as a sum of elements of the form $b_i t_i$ with $t_i \in I$. Therefore each relation

$$\sum_{j=1}^{r} w_{ij} c_j + \sum_{j=1}^{n} z_{ij} b_j \equiv 0 \text{ in } \overline{B}_p$$

can be expressed as in equality in $B$ as

$$\sum_{j=1}^{r} \frac{A_j}{C_j}(w_{ij}(U_{\mathfrak{p}_j} - \boldsymbol{\psi}(\mathfrak{p}_j)) + I) + \sum_{j=1}^{n}(z_{ij} + I + p^m R) b_j = 0. \tag{128}$$

Here, as above, we use the notation " $+ I$" as shorthand for " $+ z$ for some $z \in I$," and similarly for " $+ p^m R$." It follows from (128) that if we define a matrix $M' \in M_{(n+r)\times(n+r)}(K)$ in block form by

$$M' = \left( \frac{A_j}{C_j}(w_{ij}(U_{\mathfrak{p}_j} - \boldsymbol{\psi}(\mathfrak{p}_j)) + I) \quad | \quad (z_{ij} + I + p^m R) b_j \right),$$

then $\det(M') = 0$ in $K$ since it has rows that sum to 0. We can cancel the factors $A_j/C_j$ and $b_j$ scaling the columns of $M'$, since these are non-zerodivisors in $K$. We obtain that $\det(M'') = 0$ where

$$M'' = \big( (w_{ij}(U_{\mathfrak{p}_j} - \boldsymbol{\psi}(\mathfrak{p}_j)) + I) \quad | \quad (z_{ij} + I + p^m R) \big) \in M_{(n+r)\times(n+r)}(\tilde{\mathbf{T}}_{\mathfrak{m}}).$$

Recall from the notation of Theorem 8.23, we have

$$\prod_{i=1}^{r}(U_{\mathfrak{p}_j} - \boldsymbol{\psi}(\mathfrak{p}_j)) = \tilde{U} \in \tilde{\mathbf{T}}_{\mathfrak{m}}.$$

Taking the determinant of $M''$ and applying $\varphi$, we obtain

$$0 = \varphi(\det(M'')) = \tilde{U}(\det(M) + p^m R) \text{ in } W.$$

Therefore, by the last statement in Theorem 8.23, we obtain that

$$\det(M) + p^m R \in (\Theta^{\#}). \tag{129}$$

Since $\Theta^{\#}$ divides $p^m$, $\det(M) \in (\Theta^{\#})$ as desired. □

It is worth noting that the last statement of Theorem 8.23, which allowed for the deduction of (129), was heavily dependent on the presence of the factor $x$ in our congruence (105) in case 1a. The fact that we are able to construct a "higher congruence" (i.e. modulo $x\Theta^{\#}$ rather than just $\Theta^{\#}$) is essential for our proof.

**Corollary 9.11.** *We have*

$$\mathrm{Fitt}_R(\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)_R) \subset (\Theta^{\#}).$$

*Proof.* Theorem 9.10 states that $\mathrm{Fitt}_R(\overline{B}_p) \subset (\Theta^{\#})$, hence

$$\mathrm{Fitt}_{R^{\#}}(\overline{B}_p(\boldsymbol{\psi}^{-1})) \subset (\Theta).$$

Theorem 9.8 states that there is an $R$-module surjection $\nabla_{\Sigma}^{\Sigma'}(H)_{R^{\#}} \twoheadrightarrow \overline{B}_p(\boldsymbol{\psi}^{-1})$, whence

$$\mathrm{Fitt}_{R^{\#}}(\nabla_{\Sigma}^{\Sigma'}(H)_{R^{\#}}) \subset (\Theta).$$

Finally, by Corollary 6.2, we obtain

$$\mathrm{Fitt}_R(\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)_R) \subset (\Theta^{\#})$$

as desired. □

# A Appendix: Construction and Properties of $\nabla$

Let $\Sigma, \Sigma'$ denote finite disjoint sets of places of $F$ with $\Sigma \supset S_\infty$, such that $\Sigma'$ satisfies condition (1) from the introduction.

In this section we define the module $\nabla_{\Sigma}^{\Sigma'} = \nabla_{\Sigma}^{\Sigma'}(H)$ following the methods of Ritter–Weiss [40]. We do not yet enforce any additional assumptions on the sets $\Sigma, \Sigma'$. Later in this appendix we will impose assumptions as necessary to obtain certain desirable properties of $\nabla_{\Sigma}^{\Sigma'}$.

## A.1 Construction of $\nabla$

To define $\nabla_\Sigma^{\Sigma'}$, we introduce an auxiliary finite set of primes $S'$ of $F$ satisfying the following properties:

- $S' \supset \Sigma$ and $S' \cap \Sigma' = \emptyset$.
- $S' \cup \Sigma' \supset S_{\mathrm{ram}}$.
- $\mathrm{Cl}_{S'}^{\Sigma'}(H) = 1$.
- $\cup_{w \in S'_H} G_w = G$, where $G_w \subset G$ is the decomposition group at $w$.

Although it is not used in this work, we prove in §A.2 that the construction of $\nabla_\Sigma^{\Sigma'}$ is independent of the chosen auxiliary set $S'$.

For each place $v$ of $F$, we fix a place $w$ of $H$ above $v$. Ritter–Weiss define a $\mathbf{Z}[G]$-module $V_w$ sitting in an exact sequence:

$$0 \longrightarrow H_w^* \longrightarrow V_w \longrightarrow \Delta G_w \longrightarrow 0, \tag{130}$$

where as usual $\Delta G_w \subset \mathbf{Z}[G_w]$ denotes the augmentation ideal. For $w$ finite, they define a $\mathbf{Z}[G]$-module $W_w$ sitting in an exact sequence

$$0 \longrightarrow \mathcal{O}_w^* \longrightarrow V_w \longrightarrow W_w \longrightarrow 0. \tag{131}$$

We recall the construction of these modules. Let $H_w^{\mathrm{ab}} \supset L_w^{\mathrm{nr}}$ denote the maximal abelian and unramified extensions of $H_w$, respectively. There are canonical short exact sequences

$$\begin{aligned} 0 \longrightarrow \mathrm{W}(H_w^{\mathrm{ab}}/H_w) \cong H_w^* \longrightarrow \mathrm{W}(H_w^{\mathrm{ab}}/F_v) \xrightarrow{\pi_V} G_w \longrightarrow 0 \\ 0 \longrightarrow \mathrm{W}(H_w^{\mathrm{nr}}/H_w) \cong \mathbf{Z} \longrightarrow \mathrm{W}(H_w^{\mathrm{nr}}/F_v) \xrightarrow{\pi_W} G_w \longrightarrow 0, \end{aligned} \tag{132}$$

where W denotes the Weil group. Let $\Delta V$ denote the (absolute) augmentation ideal of $\mathrm{W}(H_w^{\mathrm{ab}}/F_v)$ and let $\Delta(V, H_w^*)$ denote the relative augmentation ideal corresponding to $\pi_V$. Define $\Delta W$ and $\Delta(W, \mathbf{Z})$ similarly from the corresponding terms in the second exact sequence in (132). Then we define

$$\begin{aligned} V_w = V_w(H_w) = \Delta V/(\Delta V)\Delta(V, H_w^*), \\ W_w = W_w(H_w) = \Delta W/(\Delta W)\Delta(W, \mathbf{Z}). \end{aligned} \tag{133}$$

We adopt the following notation of [19]: for a collection of $G_w$-modules $M_w$, we define

$$\widetilde{\prod_v} M_w := \prod_v \mathrm{Ind}_{G_w}^G M_w.$$

Let $U_w \subset \mathcal{O}_w^*$ denote the group of 1-units. Define

$$J = \widetilde{\prod_{v \notin \Sigma \cup \Sigma'}} \mathcal{O}_w^* \widetilde{\prod_{v \in \Sigma}} H_w^* \widetilde{\prod_{v \in \Sigma'}} U_w,$$
$$V = \widetilde{\prod_{v \notin S' \cup \Sigma'}} \mathcal{O}_w^* \widetilde{\prod_{v \in S'}} V_w \widetilde{\prod_{w \in \Sigma'}} U_w,$$
$$W = \widetilde{\prod_{v \in S' - \Sigma}} W_w \widetilde{\prod_{v \in \Sigma}} \Delta G_w,$$

so that we have an exact sequence of $G$-modules

$$0 \longrightarrow J \longrightarrow V \longrightarrow W \longrightarrow 0. \tag{134}$$

Next, we consider the canonical extension (see pg. 148 of [40])

$$0 \longrightarrow C_H = \mathbf{A}_H^*/H^* \longrightarrow \mathfrak{O} \longrightarrow \Delta G \longrightarrow 0 \tag{135}$$

associated to the global fundamental class in $H^2(G, C_H)$.

As in [40, Theorem 1], there is a map between the extensions (134) and (135):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J & \longrightarrow & V & \longrightarrow & W & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta_J} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \theta_W} & & \\ 0 & \longrightarrow & C_H & \longrightarrow & \mathfrak{O} & \longrightarrow & \Delta G & \longrightarrow & 0. \end{array} \tag{136}$$

Our map $\theta$ is the restriction of the map $\theta$ appearing in [40]; in the context of [40], the map $\theta$ is shown to be surjective. We must show that it remains surjective after restricting to our module $V$.

**Lemma A.1.** *The map $\theta$ in* (136) *is surjective.*

*Proof.* The same proof as in [40, Page 162] works, and for completeness we recall it. Define

$$J' = \widetilde{\prod_{v \notin \Sigma' \cup S'}} \mathcal{O}_w^* \widetilde{\prod_{v \in S'}} H_w^* \widetilde{\prod_{v \in \Sigma'}} U_w,$$
$$W' = \widetilde{\prod_{v \in S'}} \Delta G_w.$$

We then obtain

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J' & \longrightarrow & V & \longrightarrow & W' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta_{J'}} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \theta_{W'}} & & \\ 0 & \longrightarrow & C_H & \longrightarrow & \mathfrak{O} & \longrightarrow & \Delta G & \longrightarrow & 0. \end{array} \tag{137}$$

where the middle vertical arrow $\theta$ is the same as in (136). Yet now $\theta_{J'}$ is surjective, since its cokernel is $\mathrm{Cl}_{S'}^{\Sigma'}(H) = 1$, by our assumption on $S'$. It remains to see that $\theta_{W'}$ is surjective, and this follows easily from the other assumptions on $S'$ (see the argument below diagram 3 on page 162 of [40]). □

Applying the snake lemma to (136) yields an exact sequence

$$0 \longrightarrow \mathcal{O}_{H,\Sigma,\Sigma'}^{*} \longrightarrow V^{\theta} \longrightarrow W^{\theta} \longrightarrow \mathrm{Cl}_{\Sigma}^{\Sigma'}(H) \longrightarrow 0, \tag{138}$$

where $V^{\theta} = \ker\theta$, $W^{\theta} = \ker\theta_W$.

We next construct an injection from $W$ to a free $\mathbf{Z}[G]$-module. Write $W_w^* = \mathrm{Hom}_{\mathbf{Z}}(W_w, \mathbf{Z})$. By [40, Lemma 5], there is a commutative diagram of $\mathbf{Z}[G_w]$-modules with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W_w & \xrightarrow{(\alpha_w,\beta_w)} & \mathbf{Z}[G_w]^2 & \longrightarrow & W_w^* & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_w} & & \downarrow{\scriptstyle \pi_1} & & \downarrow & & \\ 0 & \longrightarrow & \Delta G_w & \longrightarrow & \mathbf{Z}[G_w] & \longrightarrow & \mathbf{Z} & \longrightarrow & 0. \end{array} \tag{139}$$

Here $\pi_1$ denotes projection onto the first factor. Let us recall the definition of the maps $\alpha_w, \beta_w$. The map $\alpha_w$ is induced by the canonical projection $\pi_W \colon \Delta W \longrightarrow \Delta G_w$ (see (132) and (133)) and sits in a short exact sequence

$$0 \longrightarrow \mathbf{Z} \longrightarrow W_w \xrightarrow{\alpha_w} \Delta G_w \longrightarrow 0 \tag{140}$$

[40, Lemma 5(b)]. To define $\beta_w$, we first define a map

$$\beta_w^0 \colon W_w \longrightarrow \mathbf{Z}[G_w/I_w].$$

Let $\sigma \in \mathrm{W}(H_w^{\mathrm{nr}}/F_v)$ and write $\overline{\sigma}$ for the image of $\sigma$ in $G_w/I_w = \mathrm{Gal}(H_w^{I_w}/F_v)$. Define the integer $n$ by $\sigma|_{F_v^{\mathrm{nr}}} = \sigma_v^n$, where $\sigma_v \in \mathrm{W}(F_v^{\mathrm{nr}}/F_v) \cong \mathbf{Z}$ is the Frobenius element. Writing $x = \sigma - 1$, we define $\beta_w^0(x) \in \mathbf{Z}[G_w/I_w]$ to be the unique element whose augmentation is equal to $n$ and such that

$$\overline{\alpha_w(x)} = \overline{\sigma} - 1 = (\sigma_w - 1)\beta_w^0(x) \tag{141}$$

in $\mathbf{Z}[G_w/I_w]$, where $\sigma_w = \overline{\sigma}_v \in G_w/I_w$ is the Frobenius element. To be explicit, we have

$$\beta_w^0(\sigma - 1) = \begin{cases} 1 + \sigma_w + \sigma_w^2 + \cdots + \sigma_w^{n-1} & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -(\sigma_w^{-1} + \sigma_w^{-2} + \cdots + \sigma_w^{n}) & \text{if } n < 0. \end{cases}$$

We define

$$\beta_w(x) = \mathrm{N}I_w \cdot \beta_w^0(x) \in \mathbf{Z}[G_w]. \tag{142}$$

The maps $\alpha_w, \beta_w$ allow us to give an injection from $W$ to a finite free $\mathbf{Z}[G]$-module. Write

$$S'_{\mathrm{ram}} = S_{\mathrm{ram}} \setminus (\Sigma \cap \Sigma') \subset S'.$$

Define

$$B = \prod_{v \in S' \setminus S'_{\mathrm{ram}}} \mathbf{Z}[G] \prod_{v \in S'_{\mathrm{ram}}} \mathbf{Z}[G]^2.$$

We then have an injection $\gamma \colon W \longrightarrow B$ defined componentwise as follows:

- For $v \in \Sigma$, the map $\gamma_v$ is induced by the canonical injection $\Delta G_w \subset \mathbf{Z}[G_w]$.
- For $v \in S'_{\mathrm{ram}}$, the map $\gamma_v$ is induced by the injection $(\alpha_w, \beta_w)$ in (139).
- For $v \in S' \setminus (\Sigma \cup S'_{\mathrm{ram}})$, the map $\gamma_v$ is induced by $\beta_w$, which is an isomorphism since $v$ is unramified in $H$ (see [40, Lemma 5]).

Let

$$Z = \widetilde{\prod_{v \in \Sigma}} \mathbf{Z} \widetilde{\prod_{S'_{\mathrm{ram}}}} W_w^*.$$

We then have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W & \xrightarrow{\gamma} & B & \longrightarrow & Z & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta_W} & & \downarrow{\scriptstyle \theta_B} & & \downarrow{\scriptstyle \theta_Z} & & \\ 0 & \longrightarrow & \Delta G & \longrightarrow & \mathbf{Z}[G] & \longrightarrow & \mathbf{Z} & \longrightarrow & 0. \end{array} \tag{143}$$

The vertical maps are defined componentwise as follows:

- If $v \in \Sigma$, then $\theta_W$ and $\theta_B$ are the identity map, and $\theta_Z$ is the augmentation.
- If $v \in S'_{\mathrm{ram}}$, then $\theta_W$, $\theta_B$, and $\theta_Z$ are induced from the vertical maps in (139).
- If $v \in S' \setminus (\Sigma \cup S'_{\mathrm{ram}})$, then $\theta_W$ is again induced from the first vertical map in (139), namely $\alpha_w = (\sigma_w - 1) \cdot \beta_w$. The map $\theta_B$ is multiplication by $\sigma_w - 1$.

Since $\theta_W$ is surjective, taking kernels in (143) yields a short exact sequence

$$0 \longrightarrow W^\theta \longrightarrow B^\theta \longrightarrow Z^\theta \longrightarrow 0. \tag{144}$$

Since $\theta_B$ is the identity on each component corresponding to $v \in \Sigma$, and $\Sigma \supset S_\infty$ is nonempty, it follows that:

$$B^\theta \text{ is a free } \mathbf{Z}[G]\text{-module of rank } \#S' + \#S'_{\mathrm{ram}} - 1. \tag{145}$$

**Definition A.2.** We define $\nabla_\Sigma^{\Sigma'}$ to be the cokernel of the composite map

$$V^\theta \longrightarrow W^\theta \longrightarrow B^\theta.$$

Comparing (138) and (144) we obtain two exact sequences

$$0 \longrightarrow \mathcal{O}^*_{H,\Sigma,\Sigma'} \longrightarrow V^\theta \longrightarrow B^\theta \longrightarrow \nabla_\Sigma^{\Sigma'} \longrightarrow 0, \tag{146}$$

$$0 \longrightarrow \mathrm{Cl}_\Sigma^{\Sigma'}(H) \longrightarrow \nabla_\Sigma^{\Sigma'} \longrightarrow Z^\theta \longrightarrow 0. \tag{147}$$

Consider now the following assumption:

(A1) $\Sigma \cup \Sigma' \supset S_{\mathrm{ram}}$.

If assumption (A1) holds, then $S'_{\mathrm{ram}} = \emptyset$ so $Z = Y_{H,\Sigma}$ and $Z^\theta = X_{H,\Sigma}$. The exact sequence (147) can then be written:

$$0 \longrightarrow \mathrm{Cl}_\Sigma^{\Sigma'}(H) \longrightarrow \nabla_\Sigma^{\Sigma'} \longrightarrow X_{H,\Sigma} \longrightarrow 0. \tag{148}$$

We have therefore constructed the $\mathbf{Z}[G]$-module $\nabla_\Sigma^{\Sigma'}$ satisfying property (P1) of §6. We now explore the other properties.

## A.2 Independence of $S'$

We prove in this section that the module $\nabla_\Sigma^{\Sigma'}$—moreover, the extension class it defines via the sequence (147)—is independent of the choice of auxiliary set $S'$ used in the construction. This follows (by identifying the construction for two different sets $S'_1$ and $S'_2$ with the one for $S'_1 \cup S'_2$) from the following lemma.

**Lemma A.3.** *Let $\nabla$ and $\nabla'$ be constructed as in §A.1 with the same sets $\Sigma$, $\Sigma'$, but different auxiliary sets $S'$ and $S' \cup \{v\}$. Then there is an equivalence between the extensions* (147) *associated to $\nabla$ and $\nabla'$, i.e. an isomorphism $\nabla \longrightarrow \nabla'$ fitting into a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Cl}_\Sigma^{\Sigma'}(H) & \longrightarrow & \nabla & \longrightarrow & Z^\theta & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & \mathrm{Cl}_\Sigma^{\Sigma'}(H) & \longrightarrow & \nabla' & \longrightarrow & Z^\theta & \longrightarrow & 0. \end{array} \tag{149}$$

*Proof.* Let $V, W, B$ denote the modules defined above in the construction of $\nabla_\Sigma^{\Sigma'}$ using the auxiliary set $S'$, and let $V', W', B'$ denote these same modules when $S'$ is replaced by $S' \cup \{v\}$. Then it follows from the definitions that there is an exact sequence

$$0 \longrightarrow V \longrightarrow V' \longrightarrow \mathrm{Ind}_{G_v}^G W_w \longrightarrow 0,$$

with $\mathrm{Ind}_{G_v}^G W_w \cong \mathbf{Z}[G]$ since $v$ is unramified in $H$ ([40, Lemma 5]). Since the homomorphisms $\theta\colon V, V' \longrightarrow \mathfrak{O}$ are surjective and compatible with the map $V \longrightarrow V'$, it follows that we obtain

$$0 \longrightarrow V^\theta \longrightarrow (V')^\theta \longrightarrow \mathbf{Z}[G] \longrightarrow 0.$$

It is similarly clear from the definitions that we obtain the same exact sequences with $(V, V')$ replaced by $(W, W')$ and $(B, B')$; in fact in these cases the exact sequences are split. The induced maps on the quotients $\mathbf{Z}[G]$ associated to $(V^\theta, (V')^\theta) \longrightarrow (W^\theta, (W')^\theta)$ and $(W^\theta, (W')^\theta) \longrightarrow (B^\theta, (B')^\theta)$ are the identity. It follows that the induced map $\nabla \longrightarrow \nabla'$ is an isomorphism.

The fact that this isomorphism fits into the commutative diagram (149) is a similar arrow chase. The map $B^\theta \longrightarrow Z^\theta$ forgets the components away from $\Sigma \cup S'_{\mathrm{ram}}$, so commutativity of the right square of (149) is clear. For the left square, recall how the map $\mathrm{Cl}_\Sigma^{\Sigma'}(H) \longrightarrow V$ is defined using the snake lemma. Fix an element $x \in C_H$ representing a class $\overline{x} \in \mathrm{Cl}_\Sigma^{\Sigma'}(H)$. Its image in $\mathfrak{O}$ may be written $\theta(y)$ for some $y \in V$, whose image $\overline{y}$ in $W$ necessarily lies in $W^\theta$. The image of $\overline{y}$ in $\nabla$ is the definition the image of $\overline{x}$ under $\mathrm{Cl}_\Sigma^{\Sigma'}(H) \longrightarrow \nabla$. When making the same calculation for $\nabla'$, we may choose the lift $\theta(y')$ for the image of $x$ in $\mathfrak{O}$, where $y'$ is the image of $y$ under $V \longrightarrow V'$. Then the image of $\overline{y}'$ in $\nabla'$ is the image of $\overline{y}$ in $\nabla$, and we obtain commutativity of the left square of (149). □

## A.3 Projectivity of Presentation

In this section, we show that under an appropriate assumption, the module $V^\theta$ is projective over $\mathbf{Z}[G]$.

(A2) $\Sigma'$ contains no primes of wild ramification, i.e. for every $v \in \Sigma'$, the inertia group $I_v \subset G_v \subset G$ has prime-to-$\ell$ order, where $\ell$ is the residue characteristic of $v$.

We also consider the following simpler condition that is useful, for instance, when working over $\mathbf{Z}_p$ as in the main body of the paper.

(A2′) We work over a $\mathbf{Z}[G]$-algebra $R$ such that for every $v \in \Sigma' \cap S_{\mathrm{ram}}$, the rational prime $\ell$ below $v$ is invertible in $R$.

**Lemma A.4.** *Assuming condition (A2), the $\mathbf{Z}[G]$-module $V^\theta$ is projective with constant rank equal to $\#S' - 1$. Assuming condition (A2′), the $R$-module $V_R^\theta = V^\theta \otimes_{\mathbf{Z}[G]} R$ is projective with constant rank equal to $\#S' - 1$.*

*Proof.* Recall that a $G$-module $M$ is called *cohomologically trivial* if the Tate cohomology $\hat{H}^i(H, M)$ vanishes for all subgroups $H \subset G$ and all integers $i$. We first claim that $V^\theta$ is cohomologically trivial. For this, it suffices to show that $V$ is cohomologically trivial, since it is known that $\mathfrak{O}$ is cohomologically trivial [31, Theorem 3.1.4(i)].

As we now explain, the module $V$ is the product of cohomologically trivial modules. Any $v \notin S' \cup \Sigma'$ is unramified and hence $\mathrm{Ind}_{G_w}^G \mathcal{O}_w^*$ is cohomologically trivial [8, §VI.1.2, Proposition 1]. Ritter–Weiss show that the module $\mathrm{Ind}_{G_v}^G V_w$ is cohomologically trivial [40, §3, Proposition 2].

It remains to show that $U_w$ is $G_v$-cohomologically trivial for $v \in \Sigma'$. The argument of [8, §VI.1.2, Proposition 1] again shows that $U_w^{I_w}$ is cohomologically trivial as a $(G_w/I_w)$-module. By inflation-restriction, it therefore suffices to show that $U_w$ is cohomologically trivial as an $I_w$-module. The assumption (A2) states that $I_w$ has prime-to-$\ell$ order, where $\ell$ is the residue characteristic of $v$. Therefore multiplication by $\#I_v$ is invertible on the pro-$\ell$ group $U_w$, so cohomological triviality is automatic. This proves the claim that $V^\theta$ is $G$-cohomologically trivial.

Next we note that (146) implies that $V^\theta$ is $\mathbf{Z}$-torsion free, since the modules $\mathcal{O}^*_{H,\Sigma,\Sigma'}$ and $B^\theta$ are $\mathbf{Z}$-torsion free. A theorem of Nakayama then implies that $V^\theta$ is $\mathbf{Z}[G]$-projective ([30, Theorem 1]).

To adapt this argument when assuming (A2′) instead of (A2), note that by the argument of [8, Chapter VI, Proposition 3], $U_w$ contains an open subgroup $U'_w$ that is cohomologically trivial. But the index $[U_w \colon U_{w'}]$ is a power of $\ell$, which is invertible in $R$, so $(U_w)_R \cong (U'_w)_R$. We can therefore replace $U_w$ by $U'_w$ and proceed as above.

To conclude, we show that $V^\theta$ has constant rank equal to $\#S' - 1$. It suffices to show that for every character

$$\chi \colon \mathbf{Z}[G] \longrightarrow \overline{\mathbf{Q}}^*$$

we have

$$\dim_{\overline{\mathbf{Q}}} V^\theta_\chi = \#S' - 1,$$

where

$$V^\theta_\chi = V^\theta \otimes_{\mathbf{Z}[G]} \overline{\mathbf{Q}}(\chi).$$

Here $\overline{\mathbf{Q}}(\chi)$ denotes the 1-dimensional $\overline{\mathbf{Q}}$-vector space on which $G$ acts by $\chi$. Note that $\overline{\mathbf{Q}}(\chi)$ is flat over $\mathbf{Z}[G]$.

The sequence (147) implies that

$$\begin{aligned}\dim_{\overline{\mathbf{Q}}}(\nabla^{\Sigma'}_{\Sigma})_\chi &= \dim_{\overline{\mathbf{Q}}} Z^\theta_\chi \\ &= \dim_{\overline{\mathbf{Q}}}(X_{H,\Sigma})_\chi + \sum_{v \in S'_{\mathrm{ram}}} \dim_{\overline{\mathbf{Q}}}(\mathrm{Ind}_{G_w}^G W_w^*)_\chi.\end{aligned}$$

Yet the Dirichlet unit theorem implies $\dim_{\overline{\mathbf{Q}}}(\mathcal{O}^*_{H,\Sigma,\Sigma'})_\chi = \dim_{\overline{\mathbf{Q}}}(X_{H,\Sigma})_\chi$, so (146) implies that

$$\dim_{\overline{\mathbf{Q}}} V^\theta_\chi = \dim_{\overline{\mathbf{Q}}} B^\theta_\chi - \sum_{v \in S'_{\mathrm{ram}}} \dim_{\overline{\mathbf{Q}}}(\mathrm{Ind}_{G_w}^G W_w^*)_\chi. \tag{150}$$

Now combining (130) and (131) one obtains a short exact sequence (see also [40, Lemma 5])

$$0 \longrightarrow \mathbf{Z} \longrightarrow W_w \longrightarrow \Delta G_w \longrightarrow 0,$$

from which it follows that each term in the sum on the right of (150) is equal to 1.

Therefore

$$\dim_{\overline{\mathbf{Q}}} V^\theta_\chi = \dim_{\overline{\mathbf{Q}}} B^\theta_\chi - \#S'_{\mathrm{ram}} = \#S' - 1.$$

□

As an immediate corollary, we find:

**Lemma A.5.** *Assuming (A1) and (A2), the exact sequence*

$$V^\theta \longrightarrow B^\theta \longrightarrow \nabla_\Sigma^{\Sigma'}(H) \longrightarrow 0 \tag{151}$$

*is a locally quadratic presentation of* $\nabla_\Sigma^{\Sigma'}(H)$ *over* $\mathbf{Z}[G]$.

*Assuming (A1) and (A2′), the exact sequence*

$$V_R^\theta \longrightarrow B_R^\theta \longrightarrow \nabla_\Sigma^{\Sigma'}(H)_R \longrightarrow 0 \tag{152}$$

*is a locally quadratic presentation of* $\nabla_\Sigma^{\Sigma'}(H)_R$ *over* $R$.

**Remark A.6.** In view of the proof of Lemma A.4, perhaps the "right" thing to do when $\Sigma'$ contains wildly ramified primes is to replace $U_w$ in the definition of $V$ by a $G_w$-cohomologically trivial open subgroup $U'_w$. This will yield a different module $\nabla_\Sigma^{\Sigma'}$, sitting in exact sequences analogous to (146) and (147), where $\mathrm{Cl}_\Sigma^{\Sigma'}(H)$ is replaced by a more general ray class group and $\mathcal{O}^*_{H,\Sigma,\Sigma'}$ is replaced by a subgroup. Then (151) would remain a projective presentation of $\nabla_\Sigma^{\Sigma'}$. Since we have no present applications of such a construction, we do not pursue this further here.

**Remark A.7.** In the main body of the paper, we work over a $\mathbf{Z}_p[G]$-algebra $R$. Furthermore the sets $\Sigma$ and $\Sigma'$ defined in (54) and (56) are easily seen to satisfy (A1) and (A2′). Since $\mathbf{Z}_p[G]$ is a product of local rings, the projective module of constant rank $V_R^\theta$ is free.

## A.4 Transpose of $\nabla$

In this section we assume (A2), but not (A1). In the previous section we showed that $V^\theta$ is projective under the assumption of (A2). We now compute the transpose of $\nabla_\Sigma^{\Sigma'}(H)$ associated to the projective presentation (151), namely,

$$\nabla_\Sigma^{\Sigma'}(H)^{\mathrm{tr}} = \mathrm{coker}((B^\theta)^* \longrightarrow (V^\theta)^*). \tag{153}$$

**Lemma A.8.** *Assume (A2). With* $\nabla_\Sigma^{\Sigma'}(H)^{\mathrm{tr}}$ *defined as in* (153)*, we have*

$$\nabla_\Sigma^{\Sigma'}(H)^{\mathrm{tr}} \cong \mathrm{Sel}_\Sigma^{\Sigma'}(H).$$

*Similarly if we assume (A2′) instead of (A2), the transpose of* $\nabla_\Sigma^{\Sigma'}(H)_R$ *associated to the projective presentation (152) satisfies*

$$\nabla_\Sigma^{\Sigma'}(H)_R^{\mathrm{tr}} \cong \mathrm{Sel}_\Sigma^{\Sigma'}(H)_R.$$

*Proof.* Assume (A2). We will relate (153) to the presentation for $\mathrm{Sel}_\Sigma^{\Sigma'}(H)$ given in (31). There is a natural isomorphism of functors from the category of $\mathbf{Z}[G]$-modules to itself

$$\mathrm{Hom}_{\mathbf{Z}}(-,\mathbf{Z}) \cong \mathrm{Hom}_{\mathbf{Z}[G]}(-,\mathbf{Z}[G]), \qquad \varphi \mapsto (m \mapsto \sum_g \varphi(gm)[g^{-1}]).$$

Applying $\mathcal{F} = \mathrm{Hom}_{\mathbf{Z}}(-,\mathbf{Z})$ to (144) and noting that $Z^\theta$ is $\mathbf{Z}$-free, we see that

$$\mathcal{F}(B^\theta) \longrightarrow \mathcal{F}(W^\theta)$$

is surjective, and hence our transpose fits into a short exact sequence

$$0 \longrightarrow \mathcal{F}(W^\theta) \longrightarrow \mathcal{F}(V^\theta) \longrightarrow \nabla_\Sigma^{\Sigma'}(H)^{\mathrm{tr}} \longrightarrow 0. \tag{154}$$

The injectivity of the first nontrivial arrow in (154) follows since $\mathrm{Cl}_\Sigma^{\Sigma'}(H)$ is finite.

Next we revisit (137) and apply the snake lemma. Since $\mathrm{Cl}_{S'}^{\Sigma'}(H)$ is trivial, we extract an exact sequence

$$0 \longrightarrow \mathcal{O}^*_{H,S',\Sigma'} \longrightarrow V^\theta \longrightarrow (W')^\theta \longrightarrow 0. \tag{155}$$

Since $(W')^\theta$ is $\mathbf{Z}$-free, we obtain

$$0 \longrightarrow \mathcal{F}((W')^\theta) \longrightarrow \mathcal{F}(V^\theta) \longrightarrow \mathcal{F}(\mathcal{O}^*_{H,S',\Sigma'}) \longrightarrow 0. \tag{156}$$

Now, the map $V^\theta \longrightarrow (W')^\theta$ factors through $W^\theta$. Indeed, this map is the composition of $V^\theta \longrightarrow W^\theta$ with the map $W^\theta \longrightarrow (W')^\theta$ induced by $\alpha_w$ on the components corresponding to $v \in S' - \Sigma$ and the identity on the components corresponding to $v \in \Sigma$. By inducing (140) from $G_w$ to $G$ and taking the product over $v \in S' - \Sigma$, we find that this latter map sits in a short exact sequence

$$0 \longrightarrow Y_{H,S'-\Sigma} \longrightarrow W^\theta \longrightarrow (W')^\theta \longrightarrow 0. \tag{157}$$

Since $(W')^\theta$ is $\mathbf{Z}$-free, applying $\mathcal{F}$ to (157) gives another short exact sequence that fits together with (154) and (156) in the following commutative diagram.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \mathcal{F}((W')^\theta) & \longrightarrow & \mathcal{F}(V^\theta) & \longrightarrow & \mathcal{F}(\mathcal{O}^*_{H,S',\Sigma'}) & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow & & \\
0 & \longrightarrow & \mathcal{F}(W^\theta) & \longrightarrow & \mathcal{F}(V^\theta) & \longrightarrow & \nabla_\Sigma^{\Sigma'}(H)^{\mathrm{tr}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & \mathcal{F}(Y_{H,S'-\Sigma}) & & 0 & & & &
\end{array}$$

The snake lemma therefore yields an isomorphism

$$\nabla_{\Sigma}^{\Sigma'}(H)^{\mathrm{tr}} \cong \mathrm{coker}(\mathcal{F}(Y_{H,S'-\Sigma}) \xrightarrow{\alpha} \mathcal{F}(\mathcal{O}^*_{H,S',\Sigma'})). \tag{158}$$

It is easy to explicitly describe the map $\alpha$ appearing in (158). Given $\varphi \in \mathcal{F}(Y_{H,S'-\Sigma})$, we have

$$\alpha(\varphi)(x) = \varphi((\mathrm{ord}_w(x))_{w\in(S'-\Sigma)_H}).$$

Therefore, (158) is exactly the description of $\mathrm{Sel}_{\Sigma}^{\Sigma'}(H)$ given in (31).

The statement for (A2′) follows similarly. □

## A.5 Extension class via Galois cohomology

In this section we assume (A1) but not (A2). As in §6.2 we set $M = \mathrm{Cl}_{\Sigma}^{\Sigma'}(H)^-$ and let $L$ denote the field extension of $H$ corresponding to $M$ via class field theory. In Lemma 6.3 we gave a formal proof that the Artin reciprocity map

$$\varphi\colon G_H \longrightarrow \mathrm{Gal}(L/H) \cong M,$$

viewed as an element of $H^1(G_H, M)$, lifts to a unique class $\lambda \in H^1(G_F, M)$. A cocycle representing $\lambda$ is given by

$$\lambda(g) = \varphi(gcg^{-1}c^{-1})^{1/2}, \tag{159}$$

where $c$ is any fixed complex conjugation in $G_F$ and $m^{1/2}$ denotes the unique square root of the element $m$ in the finite abelian group of odd order $M$. It is elementary to check that the function defined by (159) is a well-defined cocycle representing a class in $H^1(G_F, M)$. Furthermore, if $g \in G_H$, then since complex conjugation acts as inversion on $M$ we have $\varphi(cg^{-1}c^{-1}) = \varphi(g)$ and hence $\lambda(g) = \varphi(g^2)^{1/2} = \varphi(g)$.

Recall that in §6.2 we explained how restriction to the decomposition group at $v$ in $G_F$ gives rise to classes $\lambda_v \in H^1(G_v, M)$. We now prove Lemma 6.4, restated below.

**Lemma A.9.** *The extension class in* $\mathrm{Ext}^1_{\mathbf{Z}[G]^-}(X^-_{H,\Sigma}, M)$ *determined by* $\nabla_{\Sigma}^{\Sigma'}(H)^-$ *corresponding to the minus part of the exact sequence* (77) *is equal to* $(\lambda_v)_{v\in\Sigma}$ *under the isomorphism* (83).

*Proof.* Recall the explicit description of the isomorphism (83) given in §6.2. With $\gamma_v$ defined as in (84), it suffices to show that we can choose $x$ such that $\gamma_v = \lambda_v$.

This requires the explicit construction of $\nabla_{\Sigma}^{\Sigma',-}$ in §A.1. Recall that $S'$ was chosen so that the $G_{v'}$ for $v' \in S'$ cover $G$; in particular, there exists $v' \in S'$ such that $c \in G_{v'}$ (here $c$ is complex conjugation). For notational simplicity we assume that the Frobenius of $v'$ in $G$ is equal to $c$ (we are of course free to add a $v'$ with this property to the set $S'$). The restriction of $\theta_B$ to the factor corresponding to $v'$ is therefore $y \mapsto y\cdot(c-1)$. Hence an explicit element

$\tilde{x} \in B^{\theta,-} \subset \prod_{S'} \mathbf{Z}[G]^-$ lifting $\frac{1}{2}(w - \overline{w}) \in X^-_{H,\Sigma}$ is the tuple having coordinate at $v$ equal to $(1-c)/2$, coordinate at $v'$ equal to $1/2$, and all other coordinates equal to 0. For $g \in G_v$,

$$\gamma_v(g) = (g-1)\tilde{x} = ((1-c)(g-1))/2, (g-1)/2, 0)_{v,v',v'' \neq v,v'}.$$

This is an element of $W^{\theta,-}$ and to conclude we must compute its image in $M$ under the snake map $W^\theta \longrightarrow M$ associated to (136). This snake map was described explicitly in [40, Theorem 5], as follows. Write $\tilde{G} = \mathrm{Gal}(L/F)$, where as above $L$ is the extension of $H$ corresponding to $M$ via class field theory. Write $(\Delta\tilde{G})$ for the augmentation ideal of $\mathbf{Z}[\tilde{G}]$ and let $\Delta(\tilde{G}, M)$ denote the kernel of the canonical map $\mathbf{Z}[\tilde{G}] \longrightarrow \mathbf{Z}[G]$. There is a canonical short exact sequence

$$0 \longrightarrow M \cong \frac{\Delta(\tilde{G}, M)}{\Delta(\tilde{G}, M)\Delta\tilde{G}} \longrightarrow \frac{\Delta\tilde{G}}{\Delta(\tilde{G}, M)\Delta\tilde{G}} \longrightarrow \Delta G \longrightarrow 0. \tag{160}$$

Ritter and Weiss associate to an element $w \in W$ an element $\rho(w) \in \Delta\tilde{G}/\Delta(\tilde{G}, M)\Delta\tilde{G}$. When $w \in W^\theta$, the element $\rho(w)$ has trivial image in $\Delta G$ and hence gives rise to an element of $M$; this is the explicit description of the snake map $W^\theta \longrightarrow M$.

The components $\rho_v, \rho_{v'}$ of the map $\rho$ have slightly different definitions in the case $v \in \Sigma$, when the corresponding component of $W$ is

$$\mathrm{Ind}_{G_v}^G \Delta G_v = \mathbf{Z}[G] \otimes_{\mathbf{Z}[G_v]} \Delta G_v \subset \mathbf{Z}[G] \otimes_{\mathbf{Z}[G_v]} \mathbf{Z}[G_v] = \mathbf{Z}[G],$$

and the case $v' \in S' - \Sigma$ when the corresponding component of $W$ is

$$\mathbf{Z}[G] \otimes_{\mathbf{Z}[G_v]} \mathbf{Z}[G_v] = \mathbf{Z}[G].$$

To describe these, let $\tilde{g}$ and $\tilde{c}$ represent lifts to $\tilde{G}$ of $g$ and $c$ lying in the decomposition group associated to $v$ and $v'$, respectively. For $v$, we write the corresponding component of $2\gamma_v(x) = 2(g-1)\tilde{x}$ as $(1-c) \otimes (g-1)$, and then

$$\rho_v((1-c) \otimes (g-1)) = (1-\tilde{c})(\tilde{g}-1).$$

Meanwhile for $v'$ the corresponding component of $2(g-1)\tilde{x}$ is simply $(g-1) \otimes 1$ and

$$\rho_{v'}((g-1) \otimes 1) = (\tilde{g}-1)(\tilde{c}-1).$$

Adding these, we obtain

$$\rho(2(g-1)\tilde{x}) = \tilde{g}\tilde{c} - \tilde{c}\tilde{g}.$$

The explicit description of the isomorphism $\Delta(\tilde{G}, M)/\Delta(\tilde{G}, M)\Delta\tilde{G} \cong M$ given in [40, Page 155] shows that the element

$$\tilde{g}\tilde{c} - \tilde{c}\tilde{g} = (\tilde{g}\tilde{c}\tilde{g}^{-1}\tilde{c}^{-1} - 1)(\tilde{c}\tilde{g})$$

corresponds to $\tilde{g}\tilde{c}\tilde{g}^{-1}\tilde{c}^{-1} \in M$. Therefore

$$\gamma_v(g) = (\tilde{g}\tilde{c}\tilde{g}^{-1}\tilde{c}^{-1})^{1/2} = \lambda_v(g)$$

as desired (see (159)). □

# B Appendix: Kurihara's Conjecture

In this section, we prove Kurihara's Conjecture on the Fitting ideal of $\mathrm{Cl}^T(H)^{\vee,-}$, bootstrapping from the partial version proven in Theorem 3.7. We first recall the statement of the conjecture, starting with notation from Lemma 3.4. For $S_\infty \subset J \subset S_\infty \cup S_{\mathrm{ram}}$, write $\overline{J} = S_{\mathrm{ram}} \setminus J$. Let $H^{\overline{J}}$ denote the maximal subextension of $H/F$ that is unramified at primes in $\overline{J}$. This is the field $H^{I_{\overline{J}}}$, where $I_{\overline{J}}$ is the subgroup of $G$ generated by the inertia groups $I_v$ for $v \in \overline{J}$. Note that the extension $H^{\overline{J}}/F$ is unramified outside $J$, and hence

$$\Theta_{J,T}(H^{\overline{J}}/F) \in \mathbf{Z}[G/I_{\overline{J}}].$$

Since $\mathrm{N}I_{\overline{J}}$ divides $\prod_{v\in\overline{J}} \mathrm{N}I_v$, multiplication by $\prod_{v\in\overline{J}} \mathrm{N}I_v$ yields a well-defined map

$$\mathbf{Z}[G/I_{\overline{J}}] \longrightarrow \mathbf{Z}[G].$$

As noted in (34), the version of Kurihara's conjecture stated in the introduction is equivalent to the equality

$$\mathrm{Fitt}_{\mathbf{Z}[G]^-} \mathrm{Cl}^T(H)^{\vee,-} = \left( \prod_{v\in\overline{J}} \mathrm{N}I_v \cdot \Theta_{J,T}(H^{\overline{J}}/F)^{\#} \colon S_\infty \subset J \subset S_\infty \cup S_{\mathrm{ram}} \right) \subset \mathbf{Z}[G]^-. \quad (161)$$

## B.1 Functorial properties

We begin with some functorial properties of the construction of $\nabla_\Sigma^{\Sigma'}$. Throughout this section we assume (A2). In our application to Kurihara's conjecture we will have $\Sigma' = T$, which contains no ramified primes, so (A2) is satisfied.

**Lemma B.1.** *For any subgroup $\Gamma \subset G$, we have*

$$V^\theta(H)^\Gamma = (\mathrm{N}\Gamma)V^\theta(H) \cong V^\theta(H^\Gamma).$$

*Proof.* As $V^\theta(H)$ is projective over $\mathbf{Z}[G]$, by [3, Chapter I, Proposition 10] it follows that $V^\theta(H)^\Gamma = \mathbf{Z}[G]^\Gamma \otimes_{\mathbf{Z}[G]} V^\theta(H)$. The equality $V^\theta(H)^\Gamma = (\mathrm{N}\Gamma)V^\theta(H)$ follows from the fact that $\mathbf{Z}[G]^\Gamma = (\mathrm{N}\Gamma)\mathbf{Z}[G]$. We must show $V^\theta(H)^\Gamma \cong V^\theta(H^\Gamma)$.

We first check that $V(H)^\Gamma \cong V(H^\Gamma)$, which we can do componentwise over all places $v$. Each component of $V(H)$ is of the form $\mathrm{Ind}_{G_w}^G N_w(H_w)$ for a $G_w$-module $N_w(H_w)$. If we write $\Gamma_w = \Gamma \cap G_w$, then we claim that

$$(\mathrm{Ind}_{G_w}^G N_w(H_w))^\Gamma \cong \mathrm{Ind}_{G_w/\Gamma_w}^{G/\Gamma} N_w(H_w)^{\Gamma_w} \quad (162)$$

as $G/\Gamma$-modules. To see this note that by [51, Lemma 6.3.4], the induced modules can be identified with co-induced modules, and therefore the isomorphism (162) is equivalent to the following natural isomorphism

$$\mathrm{Hom}_\Gamma(\mathbf{Z}, \mathrm{Hom}_{G_w}(\mathbf{Z}[G], N_w(H_w))) \cong \mathrm{Hom}_{G_w/\Gamma_w}(\mathbf{Z}[G/\Gamma], \mathrm{Hom}_{\Gamma_w}(\mathbf{Z}, \mathrm{N}_w(H_w))).$$

So it suffices to prove that in each case

$$N_w(H_w)^{\Gamma_w} \cong N_w(H_w^{\Gamma_w}).$$

as $G_w/\Gamma_w$-modules.

For $v \notin S'$, we have $N_w(H_w) = H_w^*$ or $\mathcal{O}_w^*$, so this holds trivially. For $v \in S'$ there is a map

$$V_w(H_w^{\Gamma_w}) \xrightarrow{\mathrm{N}\Gamma_w} V_w(H_w)^{\Gamma_w}$$

given by

$$(\sigma - 1) \mapsto \mathrm{N}\Gamma_w(\tilde{\sigma} - 1)$$

for any $\sigma \in \mathrm{W}((H_w^{\Gamma_w})^{\mathrm{ab}}/F_v)$ and any lift $\tilde{\sigma} \in \mathrm{W}(H_w^{\mathrm{ab}}/F_v)$ of $\sigma$. This map is well-defined because of the isomorphism

$$\mathrm{W}(H_w^{\mathrm{ab}}/(H_w^{\Gamma_w})^{\mathrm{ab}}) \cong \ker(\mathrm{N}\Gamma_w \colon H_w^* \longrightarrow (H_w^{\Gamma_w})^*).$$

We have a commutative diagram connecting the exact sequences (130) for $H_w$ and $H_w^{\Gamma_w}$:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & (H_w^{\Gamma_w})^* & \longrightarrow & V_w(H_w^{\Gamma_w}) & \longrightarrow & \Delta(G_w/\Gamma_w) & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \mathrm{N}\Gamma_w} & & \downarrow{\scriptstyle \mathrm{N}\Gamma_w} & & \\ 1 & \longrightarrow & (H_w^*)^{\Gamma_w} & \longrightarrow & V_w(H_w)^{\Gamma_w} & \longrightarrow & (\Delta G_w)^{\Gamma_w} & \longrightarrow & 1. \end{array} \tag{163}$$

The exactness of the bottom row follows from Hilbert's Theorem 90. The flanking vertical arrows are easily seen to be isomorphisms, so the central vertical arrow is as well. The right square is cartesian and we use this below.

We have therefore proven that $V(H)^\Gamma \cong V(H^\Gamma)$. To conclude we claim that there is a commutative diagram

$$\begin{array}{ccc} V(H^\Gamma) & \xrightarrow{\sim} & V(H)^\Gamma \\ \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \theta} \\ \mathfrak{O}(H^\Gamma) & \xrightarrow{\sim} & \mathfrak{O}(H)^\Gamma, \end{array} \tag{164}$$

from which the desired isomorphism $V^\theta(H)^\Gamma = V^\theta(H^\Gamma)$ follows.

To prove the claim we need to construct the bottom arrow giving a commutative square. Taking $\Gamma$-invariants of the sequence in equation (135) and noting that $H^1(\Gamma, C_H) = 1$ (see for example, [32, Theorem III.4.7]), we get the short exact sequence

$$1 \longrightarrow C_H^\Gamma \longrightarrow \mathfrak{O}(H)^\Gamma \longrightarrow \Delta(G)^\Gamma \longrightarrow 1. \tag{165}$$

Using the isomorphisms $\mathrm{N}\Gamma \colon \Delta(G/\Delta) \longrightarrow \Delta(G)^\Gamma$ and $C_H^\Gamma \cong C_{H^\Gamma}$ (see [32, Theorem III.2.7] for the latter), we can write this as

$$1 \longrightarrow C_{H^\Gamma} \longrightarrow \mathfrak{O}(H)^\Gamma \longrightarrow \Delta(G/\Gamma) \longrightarrow 1. \tag{166}$$

Let $\alpha \in H^2(G/\Gamma, C_{H^\Gamma})$ be the cohomology class representing the extension class of (166). Note that the image of $\alpha$ under the inflation map

$$\mathrm{infl} : H^2(G/\Gamma, C_{H^\Gamma}) \longrightarrow H^2(G, C_H)$$

is given by first pulling back the short exact sequence in equation (165) along the map $\Delta(G) \xrightarrow{\mathrm{N}\Gamma} \Delta(G)^\Gamma$ and then pushing it forward along the inclusion $C_{H^\Gamma} \longrightarrow C_H$. Denote the fundamental classes in $H^2(G, C_H)$ and $H^2(G/\Gamma, C_{H^\Gamma})$ by $u_G$ and $u_{G/\Gamma}$, respectively. We have

$$\mathrm{infl}(\alpha) = u_G^{\#\Gamma} = \mathrm{infl}(u_{G/\Gamma}).$$

The first equality follows since $\mathrm{N}\Gamma$ acts as multiplication by $\#\Gamma$ on $\Gamma$-invariants. For the second equality see [32, Proposition I.1.6]. As infl is injective, we find that $\alpha = u_{G/\Gamma}$. Hence we obtain a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_{H^\Gamma} & \longrightarrow & \mathfrak{O}(H^\Gamma) & \longrightarrow & \Delta(G/\Gamma) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{N}\Gamma} & & \\ 1 & \longrightarrow & C_H^\Gamma & \longrightarrow & \mathfrak{O}(H)^\Gamma & \longrightarrow & (\Delta G)^\Gamma & \longrightarrow & 1, \end{array} \tag{167}$$

with square on the right cartesian and all vertical arrows isomorphisms. The commutativity of (164) follows since the right squares in (163) and (167) are cartesian. We must only note the following commutative diagram, whose vertical arrows are isomorphisms:

$$\begin{array}{ccc} \mathrm{Ind}_{G_w}^G(\Delta G_w/\Gamma_w) & \longrightarrow & \Delta(G/\Gamma) \\ \downarrow{\scriptstyle \mathrm{N}\Gamma_w} & & \downarrow{\scriptstyle \mathrm{N}\Gamma} \\ \mathrm{Ind}_{G_w}^G(\Delta G_w)^{\Gamma_w} & \xrightarrow{\mathrm{N}(\Gamma/\Gamma_w)} & \Delta(G)^\Gamma. \end{array}$$

This completes the proof. □

Recall from (139) that we have an injection

$$(\alpha_w, \beta_w) \colon W_w(H_w) \longrightarrow \mathbf{Z}[G_w]^2.$$

We denote by $(\alpha_v, \beta_v)$ the induced map

$$(\alpha_v, \beta_v) \colon W_v(H) := \mathrm{Ind}_{G_w}^G W_w(H_w) \longrightarrow \mathbf{Z}[G]^2. \tag{168}$$

The following lemma follows immediately from the definition of $\alpha_w, \beta_w^0$, and $\beta_w$ given in (139)–(142).

**Lemma B.2.** *Let $\Gamma \subset G$ be a subgroup. Let $x \in W_v(H)$, and let $\overline{x}$ denote the image of $x$ under the canonical map $W_v(H) \longrightarrow W_v(H^\Gamma)$ induced by restriction.*

- *We have*
$$\overline{\alpha_v(x)} = \alpha_v(\overline{x}) \tag{169}$$
*in* $\mathbf{Z}[G/\Gamma]$. *Here the left side denotes the reduction modulo* $\Gamma$ *of* $\alpha_v(x)$. *On the right side, the map* $\alpha_v$ *is the map of (168) with* $(H, G)$ *replaced by* $(H^\Gamma, G/\Gamma)$.

- *Suppose that* $\Gamma \supset I_w$. *We have*
$$\overline{\beta_v^0(x)} = \beta_v(\overline{x}) \tag{170}$$
*in* $\mathbf{Z}[G/\Gamma]$, *with notation as in the previous item.*

The lemma below follows since the isomorphism $\mathrm{N}\Gamma \cdot V^\theta(H) \cong V^\theta(H^\Gamma)$ sends $\mathrm{N}\Gamma \cdot x$ to the restriction of $x$, denoted $\overline{x} \in V^\theta(H^\Gamma)$.

**Lemma B.3.** *Let* $\Gamma \subset G$ *be a subgroup. Let* $x \in V^\theta(H)$, *and let* $\overline{x}$ *denote the image of* $\mathrm{N}\Gamma \cdot x$ *under the isomorphism* $\mathrm{N}\Gamma \cdot V^\theta(H) \cong V^\theta(H^\Gamma)$ *described in Lemma B.1. Then the congruences (169) and (170) hold, with the latter under the assumption* $\Gamma \supset I_w$.

## B.2 Proof of Kurihara's Conjecture

For a nonnegative integer $i$ and finitely presented $R$-module $M$, we write $\mathrm{Fitt}_R^i(M)$ for the $i$th Fitting ideal of $M$. Throughout this text, $\mathrm{Fitt}_R(M)$ has denoted $\mathrm{Fitt}_R^0(M)$, and we continue this convention. The connection between $\mathrm{Cl}^T(H)^\vee$ and Ritter–Weiss modules is provided by the following lemma.

**Lemma B.4.** *Let* $s = \#S_{ram}$. *We have*
$$\mathrm{Fitt}_{\mathbf{Z}[G]^-}(\mathrm{Cl}^T(H)^{\vee,-}) = (\mathrm{Fitt}^s_{\mathbf{Z}[G]^-} \nabla^T_{S_\infty}(H)^-)^\#.$$

*Proof.* By Lemma A.8, the transpose of $\nabla^T_{S_\infty}(H)$ associated to the presentation (151) is $\mathrm{Sel}^T_{S_\infty}(H)$. Since $\Sigma = S_\infty$, we have $S'_{\mathrm{ram}} = S_{\mathrm{ram}}$. Therefore (145) and Lemma A.4 imply that this presentation of $\nabla^T_{S_\infty}(H)$ has precisely $s$ more generators than relations. It follows that
$$\mathrm{Fitt}_{\mathbf{Z}[G]}(\mathrm{Sel}^T_{S_\infty}(H)) = (\mathrm{Fitt}^s_{\mathbf{Z}[G]} \nabla^T_{S_\infty}(H))^\#. \tag{171}$$
It remains to observe that we showed in (30) an isomorphism
$$\mathrm{Sel}^T_{S_\infty}(H)^- \cong \mathrm{Cl}^T(H)^{\vee,-}$$
of $\mathbf{Z}[G]^-$-modules. □

To prove Kurihara's conjecture (161), it therefore remains to prove that
$$\mathrm{Fitt}^s_{\mathbf{Z}[G]^-} \nabla^T_{S_\infty}(H)^- = \left( \prod_{v \in \overline{J}} \mathrm{N}I_v \cdot \Theta_{J,T}(H^{\overline{J}}/F) \colon S_\infty \subset J \subset S_\infty \cup S_{\mathrm{ram}} \right). \tag{172}$$

It suffices to prove (172) after tensoring with $\mathbf{Z}_p[G]^-$ over $\mathbf{Z}[G]^-$ for every odd prime $p$. We therefore fix an odd prime $p$ and write $R = \mathbf{Z}_p[G]$.

As $R$ is a product of local rings, $V_p^\theta = V^\theta \otimes_{\mathbf{Z}} \mathbf{Z}_p$ is free of rank $t = \#S' - 1$ over $R$ by Lemma A.4. We fix an $R$-basis $v_1, \dots, v_t$ of $V_p^\theta$. We denote the canonical basis of

$$B_p = R^{s+t+1} = \prod_{v \in S' \setminus S_{\mathrm{ram}}} R \prod_{v \in S_{\mathrm{ram}}} R^2$$

by $\{e_v\}_{v \in S' - S_{\mathrm{ram}}} \cup \{e_{v,0}, e_{v,1}\}_{v \in S_{\mathrm{ram}}}$. Fix an infinite place $\infty$ of $F$ and consider the basis

$$\{f_v = e_v - e_\infty\}_{v \in S' \setminus S_{\mathrm{ram}}, v \neq \infty} \cup \{f_{v,0} = e_{v,0} - e_\infty, f_{v_1} = e_{v,1} - e_\infty\}_{v \in S_{\mathrm{ram}}}$$

of $B_p^\theta$. Let $A$ denote the matrix of the map $V_p^\theta \longrightarrow B_p^\theta$ with respect to these bases. By definition, $\mathrm{Fitt}^s_{R^-} \nabla^T_{S_\infty}(H)_p^-$ is the ideal generated by the determinants of the submatrices of $A$ determined by selecting any $t$ of its columns. These columns are indexed by the basis vectors of $B_p^\theta$. We first show that if the columns associated to the basis vectors $f_{v,0}, f_{v,1}$ of a place $v \in S_{\mathrm{ram}}$ are selected, then the resulting determinant vanishes.

**Lemma B.5.** *Let $x_1, x_2 \in W_v(H)$. Then*

$$\det \begin{pmatrix} \alpha_v(x_1) & \beta_v(x_1) \\ \alpha_v(x_2) & \beta_v(x_2) \end{pmatrix} = 0$$

*in* $\mathbf{Z}[G]$.

*Proof.* It suffices to prove that if $x_1, x_2 \in W_w(H_w)$ then

$$\det \begin{pmatrix} \alpha_w(x_1) & \beta_w(x_1) \\ \alpha_w(x_2) & \beta_w(x_2) \end{pmatrix} = 0$$

in $\mathbf{Z}[G_w]$. We have

$$\det \begin{pmatrix} \alpha_w(x_1) & \beta_w(x_1) \\ \alpha_w(x_2) & \beta_w(x_2) \end{pmatrix} = \mathrm{N}I_w \cdot \det \begin{pmatrix} \overline{\alpha_w(x_1)} & \beta_w^0(x_1) \\ \overline{\alpha_w(x_2)} & \beta_w^0(x_2) \end{pmatrix},$$

where the bar denotes reduction modulo $I_w$. The determinant on the right vanishes since $\overline{\alpha_w(x)} = (\sigma_w - 1)\beta_w^0(x)$, as we noted in (141). □

Lemma B.5 allows for the following calculation.

**Lemma B.6.** *Let $S_\infty \subset J \subset S_\infty \cup S_{ram}$ be any subset and write $j = \#(J \setminus S_\infty)$. Recall the notation $\overline{J} = S_{ram} \setminus J$. We have*

$$\mathrm{Fitt}^{s-j}_R \nabla^T_J(H)_p = \left( \prod_{v \in \overline{J \cup J'}} \mathrm{N}I_v \cdot \mathrm{Fitt}_R \nabla^T_{J \cup J'}(H^{\overline{J \cup J'}})_p \colon J' \subset \overline{J} \right).$$

*Proof.* The matrix $A_J$ for the presentation $V_p^\theta \longrightarrow B_p^\theta$ of $\nabla_J^T(H)_p$ is simply the matrix $A$ with the columns corresponding to the basis vectors $f_{v,2}$ removed for $v \in J$. It has dimension $t \times (t+s-j)$. The $(s-j)$th Fitting ideal is computed by choosing $t$ of the columns, computing the determinant, and taking the ideal generated by all such choices. The columns of $A_J$ can be partitioned into $t-(s-j)$ columns corresponding to the $v \in S' \setminus \overline{J}$, $v \neq \infty$, and $(s-j)$ pairs of columns corresponding to the $v \in \overline{J}$. Lemma B.5 implies that if we choose both columns in the pair corresponding to some $v \in \overline{J}$, then the resulting determinant vanishes. It follows that

$$\mathrm{Fitt}_R^{s-j} \nabla_J^T(H)_p = (\det(A_{J,J'}) \colon J' \subset \overline{J}) \tag{173}$$

where $A_{J,J'}$ is the square matrix obtained by choosing the following $t$ columns of $A_J$:

- All $t-(s-j)$ columns corresponding to the $v \in S' \setminus \overline{J}$.
- The first column of the pair corresponding to the $v \in J'$.
- The second column of the pair corresponding to the $v \in \overline{J \cup J'}$.

The second column for $v \in \overline{J \cup J'}$ is the column vector $(\beta_v(v_i))_{i=1}^t$, where we recall that $v_1, \ldots, v_t$ is our basis for $V^\theta(H)$. Since $\beta_v(x) = \mathrm{N}I_v \cdot \beta_v^0(x)$, we pull out the factors $\mathrm{N}I_v$ from these columns and find that

$$\det(A_{J,J'}) = \left( \prod_{v \in \overline{J \cup J'}} \mathrm{N}I_v \right) \det(A_{J,J'}^0), \tag{174}$$

where $A_{J,J'}^0$ is the matrix $A_{J,J'}$ with $\beta_v(x)$ replaced by $\beta_v^0(x)$ for $v \in \overline{J \cup J'}$. Note that $A_{J,J'}^0$ is well-defined as a matrix over $\mathbf{Z}_p[G/I_{\overline{J \cup J'}}]$, and multiplication by $\prod_{v \in \overline{J \cup J'}} \mathrm{N}I_v$ yields a well-defined element of $R$.

By Lemma B.1, the module $V^\theta(H^{\overline{J \cup J'}})_p$ has a $\mathbf{Z}_p[G/I_{\overline{J \cup J'}}]$-module basis

$$\overline{v}_1 = \mathrm{N}I_{\overline{J \cup J'}} \cdot v_1, \ldots, \overline{v}_t = \mathrm{N}I_{\overline{J \cup J'}} \cdot v_t.$$

It then follows from Lemma B.3 that the matrix

$$A_{J,J'}^0 \in M_{t \times t}(\mathbf{Z}_p[G/I_{\overline{J \cup J'}}])$$

is precisely the square matrix for the presentation $V_p^\theta \longrightarrow B_p^\theta$ of the module $\nabla_{J \cup J'}^T(H^{\overline{J \cup J'}})_p$. For this, note that $H^{\overline{J \cup J'}}$ is unramified at $v \in \overline{J \cup J'}$, so by definition the corresponding column in the matrix of the presentation is $(\beta_v(\overline{v}_i))_{i=1}^t$. Meanwhile by definition the other columns are $(\alpha_v(\overline{v}_i))_{i=1}^t$. Therefore,

$$(\det(A_{J,J'}^0)) = \mathrm{Fitt}_R \nabla_{J \cup J'}^T(H^{\overline{J \cup J'}})_p. \tag{175}$$

Combining (173), (174), and (175) yields the desired result. □

Note that Lemma B.6 did not require $p$ to be odd, or to project to the minus side; in particular the result holds over $\mathbf{Z}[G]$. In what follows we do require $p$ to be odd, and where necessary we project to the minus side.

As in §3.2, let

$$\Sigma = S_\infty \cup \{v \in S_{\mathrm{ram}}, v \mid p\}.$$

The following is the major input from the main text of the paper, namely Theorem 3.7.

**Lemma B.7.** *Let $S_\infty \subset \Sigma_0 \subset \Sigma$, and let $s_0 = \#(\Sigma_0 \setminus S_\infty)$. Let $R_0 = \mathbf{Z}_p[G/I_{\Sigma\setminus\Sigma_0}]$.*

$$\mathrm{Fitt}^{s-s_0}_{R_0^-} \nabla^T_{\Sigma_0}(H^{\Sigma\setminus\Sigma_0})^-_p = \left( \Theta_{\Sigma_0\cup J_0,T}(H^{\overline{\Sigma_0\cup J_0}}) \prod_{v\in\overline{\Sigma\cup J_0}} \mathrm{N}I_v \colon J_0 \subset \overline{\Sigma} \right).$$

*Proof.* By the same argument as in (171), we have

$$\mathrm{Fitt}^{s-s_0}_{R_0^-} \nabla^T_{\Sigma_0}(H^{\Sigma\setminus\Sigma_0})^-_p = (\mathrm{Fitt}_{R_0^-} \mathrm{Sel}^T_{\Sigma_0}(H^{\Sigma\setminus\Sigma_0})^-_p).^\#$$

The result then follows directly from Theorem 3.7. □

We can now prove Kurihara's conjecture, which in view of Lemma B.4, is equivalent to the following statement.

**Theorem B.8.** *We have*

$$\mathrm{Fitt}^s_{R^-} \nabla^T_{S_\infty}(H)^-_p = \left( \prod_{v\in\overline{J}} \mathrm{N}I_v \cdot \Theta_{J,T}(H^{\overline{J}}/F) \colon S_\infty \subset J \subset S_\infty \cup S_{ram} \right). \tag{176}$$

*Proof.* By Lemma B.6, we have

$$\mathrm{Fitt}^s_R \nabla^T_{S_\infty}(H)_p = \left( \prod_{v\in\overline{J}} \mathrm{N}I_v \cdot \mathrm{Fitt}_R \nabla^T_J(H^{\overline{J}})_p \colon S_\infty \subset J \subset S_\infty \cup S_{\mathrm{ram}} \right). \tag{177}$$

We partition each set $J = \Sigma_0 \cup J_0$, where

$$\Sigma_0 = J \cap \Sigma, \qquad J_0 = J \setminus \Sigma.$$

Then (177) can be written

$$\mathrm{Fitt}^s_R \nabla^T_{S_\infty}(H)_p = \left( \prod_{v\in\overline{\Sigma_0\cup J_0}} \mathrm{N}I_v \cdot \mathrm{Fitt}_R \nabla^T_{\Sigma_0\cup J_0}(H^{\overline{\Sigma_0\cup J_0}})_p \colon S_\infty \subset \Sigma_0 \subset \Sigma, J_0 \subset \overline{\Sigma} \right). \tag{178}$$

Now apply Lemma B.6 with $J = \Sigma_0$ and $H$ replaced by $H^{\Sigma\setminus\Sigma_0}$. Note that

$$S^{\mathrm{ram}}(H^{\Sigma\setminus\Sigma_0}/F) \subset \overline{\Sigma} \cup \Sigma_0.$$

Writing $s_0 = \#(\Sigma_0 \setminus S_\infty)$ and $R_0 = \mathbf{Z}_p[G/I_{\Sigma\setminus\Sigma_0}]$, we obtain

$$\mathrm{Fitt}^{s-s_0}_{R_0}\, \nabla^T_{\Sigma_0}(H^{\Sigma\setminus\Sigma_0})_p = \left( \prod_{v\in\overline{\Sigma\cup J_0}} \mathrm{N}I_v \cdot \mathrm{Fitt}_{R_0}\, \nabla^T_{\Sigma_0\cup J_0}(H^{\overline{\Sigma\cup J_0}})_p \colon J_0 \subset \overline{\Sigma} \right) \subset R_0.$$

If we multiply by $\prod_{v\in\Sigma\setminus\Sigma_0} \mathrm{N}I_v$, we obtain exactly the terms in (178) corresponding to $\Sigma_0$. We therefore obtain

$$\mathrm{Fitt}^s_R\, \nabla^T_{S_\infty}(H)_p = \left( \prod_{v\in\Sigma\setminus\Sigma_0} \mathrm{N}I_v \cdot \mathrm{Fitt}^{s-s_0}_{R_0}\, \nabla^T_{\Sigma_0}(H^{\Sigma\setminus\Sigma_0})_p : S_\infty \subset \Sigma_0 \subset \Sigma \right). \tag{179}$$

To conclude, we project to the minus side and apply Lemma B.7:

$$\mathrm{Fitt}^s_{R^-}\, \nabla^T_{S_\infty}(H)^-_p = \left( \prod_{v\in\Sigma\setminus\Sigma_0} \mathrm{N}I_v \prod_{v\in\overline{\Sigma\cup J_0}} \mathrm{N}I_v \cdot \Theta_{\Sigma_0\cup J_0,T}(H^{\overline{\Sigma_0\cup J_0}}) \colon S_\infty \subset \Sigma_0 \subset \Sigma, J_0 \subset \overline{\Sigma} \right).$$

Writing $J = \Sigma_0 \cup J_0$, we obtain the expression (176). □

# References


[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] Baskar Balasubramanyam, Eknath Ghate, and Vinayak Vatsal. On local Galois representations associated to ordinary Hilbert modular forms. *Manuscripta Math.* 142 (3-4):513–524, 2013.

[3] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1989. Translated from the French; Reprint of the 1972 edition.

[4] David Burns. On derivatives of $p$-adic $L$-series at $s = 0$. *J. Reine Angew. Math.* 762:53–104, 2020.

[5] David Burns, Masato Kurihara, and Takamichi Sano. On zeta elements for $\mathbb{G}_m$. *Doc. Math.* 21:555–626, 2016.

[6] _____. On Iwasawa theory, zeta elements for $\mathbb{G}_m$, and the equivariant Tamagawa number conjecture. *Algebra Number Theory* 11 (7):1527–1571, 2017.

[7] David Burns and Takamichi Sano. On the theory of higher rank Euler, Kolyvagin and Stark systems, to appear in *Int. Math. Res. Notices*.

[8] J. W. S. Cassels and A. Fröhlich, editor. *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union. Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967.

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

[10] John Coates, June 4, 2020. Personal Communication.

[11] John Coates and Warren Sinnott. On $p$-adic $L$-functions over real quadratic fields. *Invent. Math.* 25:253–279, 1974.

[12] Samit Dasgupta. Shintani zeta functions and Gross-Stark units for totally real fields. *Duke Math. J.* 143 (2):225–279, 2008.

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

[14] Samit Dasgupta and Mahesh Kakde. On Constant Terms of Eisenstein Series, preprint.

[15] ———. The Integral Gross–Stark conjecture, Exact Formulae for Brumer–Stark units, and Hilbert's 12th Problem, in preparation.

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

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

[18] Ralph Greenberg. Trivial zeros of $p$-adic $L$-functions. $p$-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991). Contemp. Math., vol. 165. Amer. Math. Soc., Providence, RI., pages 149–174. 1994.

[19] Cornelius Greither. Determining Fitting ideals of minus class groups via the equivariant Tamagawa number conjecture. *Compos. Math.* 143 (6):1399–1426, 2007.

[20] ———. Some cases of Brumer's conjecture for abelian CM extensions of totally real fields. *Math. Z.* 233 (3):515–534, 2000.

[21] Cornelius Greither and Masato Kurihara. Stickelberger elements, Fitting ideals of class groups of CM-fields, and dualisation. *Math. Z.* 260 (4):905–930, 2008.

[22] Cornelius Greither and Cristian D. Popescu. An equivariant main conjecture in Iwasawa theory and applications. *J. Algebraic Geom.* 24 (4):629–692, 2015.

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

[24] Uwe Jannsen. Iwasawa modules up to isomorphism. Algebraic number theory. Adv. Stud. Pure Math., vol. 17. Academic Press, Boston, MA., pages 171–207. 1989.

[25] Henri Johnston and Andreas Nickel. Noncommutative Fitting invariants and improved annihilation results. *J. Lond. Math. Soc. (2)* 88 (1):137–160, 2013.

[26] Helmut Klingen. Über den arithmetischen Charakter der Fourierkoeffizienten von Modulformen. *Math. Ann.* 147:176–188, 1962.

[27] Masato Kurihara. Notes on the dual of the ideal class groups of CM-fields. `http://arxiv.org/abs/2006.05803`.

[28] Barry Mazur. How can we construct abelian Galois extensions of basic number fields?. *Bull. Amer. Math. Soc. (N.S.)* 48 (2):155–209, 2011.

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

[30] Tadasi Nakayama. On modules of trivial cohomology over a finite group. II. Finitely generated modules. *Nagoya Math. J.* 12:171–176, 1957.

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

[32] Jürgen Neukirch. *Class field theory*. Springer, Heidelberg, 2013. The Bonn lectures, edited and with a foreword by Alexander Schmidt; Translated from the 1967 German original by F. Lemmermeyer and W. Snyder; Language editor: A. Rosenschon.

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

[34] Cristian D. Popescu. On the Rubin-Stark conjecture for a special class of CM extensions of totally real number fields. *Math. Z.* 247 (3):529–547, 2004.

[35] ———. The Rubin-Stark conjecture for a special class of function field extensions. *J. Number Theory* 113 (2):276–307, 2005.

[36] ———. Integral and $p$-adic refinements of the abelian Stark conjecture. Arithmetic of $L$-functions. IAS/Park City Math. Ser., vol. 18. Amer. Math. Soc., Providence, RI., pages 45–101. 2011.

[37] Kenneth A. Ribet. On $l$-adic representations attached to modular forms. *Invent. Math.* 28:245–275, 1975.

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

[39] Donald Eric Rideout. *On a Generalization of a Theorem of Stickelberger*. ProQuest LLC, Ann Arbor, MI, 1970. Thesis (Ph.D.)–McGill University (Canada).

[40] Jürgen Ritter and Alfred Weiss. A Tate sequence for global units. *Compositio Math.* 102 (2):147–178, 1996.

[41] Karl Rubin. A Stark conjecture "over $\mathbf{Z}$" for abelian $L$-functions with multiple zeros. *Ann. Inst. Fourier (Grenoble)* 46 (1):33–62, 1996.

[42] Goro Shimura. On some arithmetic properties of modular forms of one and several variables. *Ann. of Math. (2)* 102 (3):491–515, 1975.

[43] ———. The special values of the zeta functions associated with Hilbert modular forms. *Duke Math. J.* 45 (3):637–679, 1978.

[44] Carl Ludwig Siegel. Über die Fourierschen Koeffizienten von Modulformen. *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* 1970:15–56, 1970.

[45] Jesse Silliman. Group Ring Valued Hilbert Modular Forms, in preparation.

[46] Harold M. Stark. $L$-functions at $s = 1$. IV. First derivatives at $s = 0$. *Adv. in Math.* 35 (3):197–235, 1980.

[47] ———. The origin of the "Stark conjectures". In Arithmetic of $L$-functions, pages 33–44. 2011.

[48] L. Stickelberger. Ueber eine Verallgemeinerung der Kreistheilung. *Math. Ann.* 37 (3):321–367, 1890.

[49] John Tate. *Les conjectures de Stark sur les fonctions L d'Artin en s = 0*. Progress in Mathematics, vol. 47. Birkhäuser Boston, Inc., Boston, MA, 1984. Lecture notes edited by Dominique Bernardi and Norbert Schappacher.

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

[51] Charles A. Weibel. *An introduction to homological algebra*. Cambridge Studies in Advanced Mathematics, vol. 38. Cambridge University Press, Cambridge, 1994.

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

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

[54] ———. On a conjecture of Brumer. *Ann. of Math. (2)* 131 (3):555–565, 1990.