On The Equivariant Tamagawa Number Conjecture

Samit Dasgupta, Mahesh Kakde, and Jesse Silliman

Abstract. Let F be a totally real field and K a finite abelian CM extension of F. Using class field theory, we show that our previous result giving a strong form of the Brumer–Stark conjecture implies the minus part of the equivariant Tamagawa number conjecture for the Tate motive associated to K/F. We work integrally over $\mathbf{Z}$, in particular the prime 2 is not inverted. This note can be viewed as our perspective on the recent work of Bullach, Burns, Daoud, and Seo. Following their philosophy, we show that the functorial properties (i.e. norm compatibilities) connecting the strong Brumer–Stark conjecture for varying number fields actually implies the minus part of the equivariant Tamagawa number conjecture.

Contents

1 Introduction

Let F be a totally real field and K a finite abelian CM extension of F. Write

$$G_K = \mathrm{Gal}(K/F).$$

In a previous paper with Jiuya Wang [8], we proved refined versions of the Brumer–Stark conjecture for K/F. In this note, we consider the minus part of the Equivariant Tamagawa Number Conjecture for the Tate motive attached to K/F, and call this "the ETNC." In a recent preprint [3], Bullach, Burns, Daoud, and Seo develop the theory of *scarcity of Euler systems* and as a consequence prove that our results on the strong Brumer–Stark conjecture proved in [6] actually imply the ETNC over $\mathbf{Z}[1/2]$. The purpose of this note is to give our perspective on this implication yielding a concise proof of the ETNC. We work integrally over $\mathbf{Z}$ rather than $\mathbf{Z}[1/2]$. While we do not directly apply any results or arguments of [3], our method is directly inspired by theirs—by passing to a suitable inverse limit, the discrepancy between strong Brumer–Stark and the ETNC becomes a non-zerodivisor and hence can be inverted.

We begin by stating the ETNC, following Kurihara's formulation [12]. First we must set some notation. Let $c \in G_K$ denote the unique complex conjugation and define

$$\mathbf{Z}[G_K]_- = \mathbf{Z}[G_K]/(c+1).$$

For any G_K-module M, we write

$$M_- = M \otimes_{\mathbf{Z}[G_K]} \mathbf{Z}[G_K]_- = M/(c+1)M.$$

Let S_∞ denote the set of infinite primes of F, and let $S_{\mathrm{ram}}(K/F)$ denote the set of finite primes of F ramified in K. Let

$$S = S(K) = S_\infty \cup S_{\mathrm{ram}}(K/F).$$

Let T denote a finite set of primes of F, disjoint from $S(K)$, satisfying the usual condition of Deligne–Ribet. Let $\nabla_S^T(K)$ denote the Ritter–Weiss G_K-module defined in [6, Appendix A]. This is a transpose of the Selmer group denoted $\mathcal{S}_{K,S}^T$ in [12] and $\mathcal{S}_{S,T}(\mathbb{G}_{m/K})$ in [4].

The module $\nabla_S^T(K)$ is the cokernel of a map

$$f_S^T(K) \colon V_{S'}^T(K) \longrightarrow B_{S'}(K),$$

where S' is an auxiliary set of places containing S satisfying certain conditions, and $V_{S'}^T(K)$ and $B_{S'}(K)$ are free $\mathbf{Z}[G_K]$-modules of rank $(\#S' - 1)$. All of these objects are defined in §2.1. For any CM subfield $E \subset K$ containing F, the G_E-module $V_{S'}^T(E)$ may be canonically identified with the space of $\mathrm{Gal}(K/E)$ co-invariants of $V_{S'}^T(K)$, and similarly for the modules denoted B. Therefore, a choice of bases for the domain and codomain of $f_K = f_S^T(K)$ naturally induces bases for the domain and codomain of $f_E = f_{S(E)}^T(E)$. Let $f_{K,-}$ denote the map obtained from f_K after projecting to the minus side (i.e. tensoring with $\mathbf{Z}[G_K]_-$ over $\mathbf{Z}[G_K]$). The formulation of the minus part of the ETNC that we prove in this paper is the following.

Theorem 1. *Fix bases for the domain and codomain of $f_K = f_S^T(K)$, thereby inducing bases for the domain and codomain of $f_E = f_{S(E)}^T(E)$ for all CM fields $E \subset K$ containing F. There exists a unit $y_K \in (\mathbf{Z}[G_K]_-)^*$ such that*

$$\det(f_{E,-}) = \mathrm{red}_{K/E}(y_K) \cdot \Theta_{S(E),T}(E/F) \ in \ \mathbf{Z}[G_E]_- \tag{1}$$

for all E, where $\mathrm{red}_{K/E}(y_K)$ denotes the canonical reduction of y_K in $(\mathbf{Z}[G_E]_-)^*$.

Here $\Theta_{S(E),T}(E/F)$ is the usual Stickelberger element (see [8, §1]).

1.1 Consequences

Before sketching our proof of Theorem 1, we connect our formulation to others and describe some important consequences.

- The statement of Theorem 1 is clearly equivalent to the projection to the minus side of Kurihara's conjecture given in [12, Conjecture 3.4].

- In [12, Proposition 3.5], Kurihara proves that the minus part of his statement is equivalent to the minus part of the "Leading Term Conjecture" (LTC) stated in [4].

- Burns, Kurihara, and Sano prove that their LTC is equivalent to the original form of the ETNC stated by Burns and Flach in [5].

Theorem 1 is known to imply the following:

- The Brumer–Stark conjecture and the higher rank Brumer–Stark conjecture due to Rubin [16].

- The integral Gross-Stark conjecture stated by Gross as a refinement to his p-adic Stark conjecture [11], and the higher rank version due to Popescu [15, Conjecture 5.3.3].

- The minus part of the "refined class number formula for $\mathbf{G}_m$" due independently to Mazur and Rubin [13] and Sano [18].

In fact, using the refined construction of Ritter-Weiss modules at $p = 2$ given in our previous work [8], one obtains stronger versions of all of these results, where $\Theta_{S,T}$ is replaced by

$$\begin{cases} \Theta_{S,T}/2^{n-2} & \text{if } K/F \text{ is unramified at all finite places,} \\ \Theta_{S,T}/2^{n-1} & \text{if } K/F \text{ is ramified at some finite place.} \end{cases}$$

This is discussed in Appendix B.

Finally, while a proof of the implication does not seem to appear in the literature, the ETNC should imply the Iwasawa Main Conjecture at $p = 2$ for totally real fields (see [1] for the statement and discussion of the Main Conjecture at $p = 2$).

1.2 Altering the smoothing and depletion sets

In the remainder of the introduction, we sketch the proof of Theorem 1. As is well-known, one may prove the result prime by prime. In Appendix A we prove the following elementary lemma.

Lemma 2. *In order to prove Theorem 1, it suffices to prove the statement tensored with $\mathbf{Z}_p$ (Theorem 3 below) for every prime p.*

Theorem 3. *Let p be a prime. Fix notation as in Theorem 1. There exists a unit $y_K \in (\mathbf{Z}_p[G_K]_-)^*$ such that*

$$\det(f_{E,-}) = \mathrm{red}_{K/E}(y_K) \cdot \Theta_{S(E),T}(E/F) \ in \ \mathbf{Z}_p[G_E]_-$$

for all E.

Note that we are working with all primes p, including $p = 2$. In order to apply the results of [8], we must alter the smoothing and depletion sets to mirror the setting there. Define

$$\Sigma(K) = S_\infty \cup \{v \in S_{\mathrm{ram}}(K/F) \colon v \mid p\}, \quad \Sigma'(K) = T \cup \{v \in S_{\mathrm{ram}}(K/F) \colon v \nmid p\}. \tag{2}$$

Write $\Sigma = \Sigma(K), \Sigma' = \Sigma'(K)$. As above, there are $\mathbf{Z}[G_K]$-modules $V_{S'}^{\Sigma'}(K)$ and $B_{S'}(K)$ and a canonical map

$$f_\Sigma^{\Sigma'}(K) \colon V_{S'}^{\Sigma'}(K) \longrightarrow B_{S'}(K).$$

The Ritter–Weiss module $\nabla_\Sigma^{\Sigma'}(K)$ is defined to be the cokernel of the map $f_\Sigma^{\Sigma'}(K)$.

If we note by a subscript p the tensor product with $\mathbf{Z}_p$, then we prove in [6] that the $\mathbf{Z}_p[G_K]$-modules $V_{S'}^{\Sigma'}(K)_p$ and $B_{S'}(K)_p$ are both free of rank ($\#S' - 1$). Therefore $\nabla_\Sigma^{\Sigma'}(K)_p$ is quadratically presented, and we proved (in [6] for p odd and in [8] for $p = 2$):

Theorem 4. *We have*

$$\mathrm{Fitt}_{\mathbf{Z}_p[G_K]_-}(\nabla_\Sigma^{\Sigma'}(K)_{p,-}) = (\Theta_{\Sigma,\Sigma'}(K/F)). \tag{3}$$

The left side of (3) is by definition the image in $\mathbf{Z}_p[G_K]_-$ of the ideal generated by the determinant of $f_\Sigma^{\Sigma'}(K)_p$ with respect to any choice of bases for its domain and codomain. As above, fixing such bases induces canonical bases for the domain and codomain of

$$f_{\Sigma(E)}^{\Sigma'(K)}(E)_p \colon V_{S'}^{\Sigma'(K)}(E)_p \longrightarrow B_{S'}(E)_p$$

for any CM subfield $E \subset K$ containing F. Note that we have altered the depletion set Σ, but have intentionally left the smoothing set Σ' and the auxiliary set S' the same to ensure that the co-invariance property mentioned above holds. Our altered version of the p-part of the ETNC is the following.

4

Theorem 5. *Fix bases for the domain and codomain of $f_K = f_\Sigma^{\Sigma'}(K)_p$, thereby inducing bases for the domain and codomain of $f_E = f_{\Sigma(E)}^{\Sigma'(K)}(E)_p$ for all CM fields $E \subset K$ containing F. There exists a unit $y_K \in (\mathbf{Z}_p[G_K]_-)^*$ such that*

$$\det(f_{E,-}) = \mathrm{red}_{K/E}(y_K) \cdot \Theta_{\Sigma(E),\Sigma'(K)}(E/F) \quad in \ \mathbf{Z}_p[G_E]_- \tag{4}$$

for all E.

In Appendix A, we show:

Lemma 6. *Theorem 5 implies Theorem 3.*

1.3 Euler Systems

In view of the discussion above, to prove Theorem 1 it suffices to prove that Theorem 4 implies Theorem 5. Theorem 4 (or more precisely, an easily deduced corollary that replaces the smoothing set $\Sigma'(E)$ by $\Sigma'(K)$) implies that for each $E \subset K$ we have a unit $y_E \in (\mathbf{Z}_p[G_E]_-)^*$ such that

$$\det(f_{E,-}) = y_E \cdot \Theta_{\Sigma(E),\Sigma'(K)}(E/F). \tag{5}$$

We need to show that the y_E can be chosen to equal $\mathrm{red}_{K/E}(y_K)$. As we explain below, functorial properties imply that the y_E satisfy certain norm compatibilities, also known as *Euler system relations*. To describe this, it is convenient to work for each E with the quotient of $\mathbf{Z}_p[G_E]_-$ on which $\Theta_{\Sigma(E),\Sigma'(K)}(E/F)$ is a non-zerodivisor. To this end, define $R_E = e_E \cdot \mathbf{Z}_p[G_E]_-$, where

$$e_E = \prod_{v \in \Sigma(E)} (1 - \mathrm{N}G_{E,v}/\#G_{E,v}) \tag{6}$$

is the idempotent corresponding to the factor on which $\Theta_{\Sigma(E),\Sigma'(K)}(E/F)$ is supported. Here $G_{E,v} \subset G_E$ denotes the decomposition group at v, and

$$\mathrm{N}G_{E,v} = \sum_{\sigma \in G_{E,v}} \sigma$$

is its norm. It suffices to prove (4) after projecting to R_E, since it is easy to show that the projection to $(1 - e_E)\mathbf{Z}_p[G_E]_-$ of both sides of the equation vanish. In §3.1, we prove:

Proposition 7. *The images of $\mathrm{red}_{K/E}(y_K)$ and y_E in R_E satisfy*

$$(\mathrm{red}_{K/E}(y_K) - y_E)P(K/E) = 0 \quad in \ R_E, \tag{7}$$

where

$$P(K/E) = \prod_{v \in \Sigma(K) - \Sigma(E)} (1 - \sigma_v^{-1}). \tag{8}$$

5

The troublesome Euler factor $P(K/E)$, which can be a zerodivisor, is all that prevents one from immediately deducing the ETNC. This leads to the following definition.

Definition 8. Consider a set of elements $(z_E)_{E \subset K}$ with $z_E \in R_E$, indexed by the CM fields $E \subset K$ containing F. We say this family is *norm compatible* if for every pair of CM fields E', E such that $F \subset E \subset E' \subset K$, we have

$$(e_E \operatorname{red}_{E'/E}(\tilde{z}_{E'}) - z_E)P(E'/E) = 0 \text{ in } R_E.$$

Here $\tilde{z}_{E'}$ denotes any lift of $z_{E'}$ to $\mathbf{Z}_p[G_{E'}]_-$. While $\operatorname{red}_{E'/E}(\tilde{z}_{E'})$ depends on the lift chosen (even its image in R_E depends on this choice), it is easy to check that $e_E \operatorname{red}_{E'/E}(\tilde{z}_{E'})P(E'/E)$ is independent of this choice, so the definition is well-formed.

With this definition, Proposition 7 states that $(e_E y_E)_{E \subset K}$ is a norm compatible family.

Definition 9. Suppose we are given a norm compatible set of elements $(z_E)_{E \subset K}$, with $z_E \in R_E$. Let K'/F be a CM abelian extension such that $K' \supset K$. We say that the family $(z_E)_{E \subset K}$ *can be extended to K'* if there exists a norm compatible family $(z'_E)_{E \subset K'}$ with $z'_E \in R_E$ such that $z'_E = z_E$ for $E \subset K$.

In the language of [3], the result below describes the "scarcity of Euler systems."

Proposition 10. *Suppose we are given a norm compatible set of elements $(z_E)_{E \subset K}$, with $z_E \in R_E$. Suppose that for each CM abelian extension K'/F such that*

$$K' \supset K \quad and \quad \Sigma(K') = \Sigma(K),$$

the family $(z_E)_{E \subset K}$ can be extended to a norm compatible family $(z'_E)_{E \subset K'}$ with $z'_E \in R_E$. Then there exists a lift $\tilde{z}_K$ of z_K to $\mathbf{Z}_p[G_K]_-$ such that

$$e_E \operatorname{red}_{K/E}(\tilde{z}_K) = z_E \text{ in } R_E$$

for all $E \subset K$.

Proposition 10 is proven in §3.2. In Proposition 17 of §3.1, we will show that the norm compatible family $(e_E y_E)_{E \subset K}$ can indeed be lifted to an arbitrary CM abelian extension K'/F containing K, and we also prove Proposition 7. These statements together yield the desired result that Theorem 4 implies Theorem 5.

2 Definitions and Functorial Properties

In this section we fix notation by recalling the definitions of the modules $V_{S'}^{\Sigma'}$, $B_{S'}$, and the map $f_\Sigma^{\Sigma'}$. We then establish some (well-known) elementary properties.

2.1 Ritter–Weiss modules

In this section we let K/F denote an arbitrary Galois extension of number fields, with $G = \mathrm{Gal}(K/F)$. Let Σ and Σ' denote finite disjoint sets of places of F. We impose the condition that K contains no nontrivial roots of unity congruent to 1 modulo all the primes above those in Σ'. We assume in this paper that $\Sigma \supset S_\infty$ and that $\Sigma \cup \Sigma' \supset S_{\mathrm{ram}}(K/F)$, though there is a more general construction that holds in the absence of these conditions (see [8]). We will recall the definition of the Ritter–Weiss module $\nabla_\Sigma^{\Sigma'}(K)$, referring the reader to [6, Appendix A] or of course the original paper of Ritter–Weiss [17] for details.

Let S' be a set of places of F satisfying the following properties:

- $S' \supset \Sigma$ and $S' \cap \Sigma' = \emptyset$.

- $\mathrm{Cl}_{S'}^{\Sigma'}(K) = 1$.

- $\cup_{w \in S'_K} G_w = G$, where $G_w \subset G$ is the decomposition group at w.

Here S'_K denotes the set of places of K above those in S'.

For each place v of F, we fix a place w of K above v. Ritter and Weiss define a $\mathbf{Z}[G_w]$-module V_w sitting in an exact sequence:

$$0 \longrightarrow K_w^* \longrightarrow V_w \longrightarrow \Delta G_w \longrightarrow 0, \tag{9}$$

where $\Delta G_w \subset \mathbf{Z}[G_w]$ denotes the augmentation ideal (see [17] or [6, Equation (133)]). For w finite, they define a $\mathbf{Z}[G_w]$-module W_w sitting in an exact sequence (see [17, §3]):

$$0 \longrightarrow \mathcal{O}_w^* \longrightarrow V_w \longrightarrow W_w \longrightarrow 0. \tag{10}$$

We have

$$W_w \cong \{(r,s) \in \Delta G_w \times \mathbf{Z}[G_w/I_w] : \overline{r} = (1 - \sigma_w^{-1})s\}, \tag{11}$$

where $\sigma_w \in G_w/I_w$ denotes an arithmetic Frobenius. Note that if w is unramified then projection on to the second coordinate yields an isomorphism $W_w \cong \mathbf{Z}[G_w]$.

Remark 11. Here and throughout this paper, we follow Kurihara's conventions [12] using the choice of $1 - \sigma^{-1}$, rather than $\sigma - 1$ as in our previous paper [6], which followed Ritter–Weiss [17]. These differ only by unit multiples, which had no effect in [6] because we were working with ideals; here, we are proving exact equalities, and Kurihara's conventions yield cleaner formulas.

We adopt the following notation of [10] and [6]: for a collection of G_w-modules M_w, we define

$$\overset{\sim}{\prod_v} M_w := \prod_v \operatorname{Ind}_{G_w}^G M_w.$$

Let $U_w^1 \subset \mathcal{O}_w^*$ denote the group of 1-units. Define

$$\tilde{V}_{S'}^{\Sigma'}(K) = \overset{\sim}{\prod_{v \notin S' \cup \Sigma'}} \mathcal{O}_w^* \overset{\sim}{\prod_{v \in S'}} V_w \overset{\sim}{\prod_{v \in \Sigma'}} U_w^1.$$

Now, there is a canonical extension (see pg. 148 of [17])

$$0 \longrightarrow C_H = \mathbf{A}_H^*/H^* \longrightarrow \mathfrak{O} \longrightarrow \Delta G \longrightarrow 0 \tag{12}$$

associated to the global fundamental class in $H^2(G, C_H)$, and a canonical surjective map

$$\theta_V \colon \tilde{V}_{S'}^{\Sigma'}(K) \longrightarrow \mathfrak{O}.$$

We define

$$V_{S'}^{\Sigma'}(K) = \ker(\theta_V).$$

Next we let

$$\tilde{B}_{S'}(K) = \prod_{v \in S'} \mathbf{Z}[G_K].$$

We define a map

$$\theta_B \colon \tilde{B}_{S'}(K) \longrightarrow \mathbf{Z}[G_K]$$

componentwise as follows.

- If $v \in \Sigma$, the component of θ_B at v is the identity.

- If $v \in S' \setminus \Sigma$, the component of θ_B at v is multiplication by $1 - \sigma_v^{-1}$, where σ_v is the arithmetic Frobenius (note that by our assumptions, $v \in S' \setminus \Sigma$ implies that K/F is unramified at v).

We then define

$$B_{S'}(K) = \ker(\theta_B).$$

To proceed, we must choose a splitting of the map θ_B. We do this once and for all by picking an infinite place ∞ of F, since the component of θ_B at ∞ is the identity. This yields an isomorphism

$$B_{S'}(K) \cong \prod_{v \in S' \setminus \{\infty\}} \mathbf{Z}[G_K]. \tag{13}$$

Next we define

$$\tilde{f}_\Sigma^{\Sigma'}(K) \colon \tilde{V}_{S'}^{\Sigma'}(K) \longrightarrow \tilde{B}_{S'}(K)$$

componentwise.

8

- If $v \in \Sigma$, the component of $\tilde{f}_\Sigma^{\Sigma'}(K)$ at v is induced by the composition of the map $V_w \to \Delta G_w$ with the canonical injection $\Delta G_w \subset \mathbf{Z}[G_w]$.

- If $v \in S' \setminus \Sigma$, component of $\tilde{f}_\Sigma^{\Sigma'}(K)$ at v is induced by the composition of $V_w \to W_w$ with the isomorphism $W_w \cong \mathbf{Z}[G_w]$ given by projection on to the second coordinate, which as noted above is an isomorphism since v is unramified.

It can be shown that $\tilde{f}_\Sigma^{\Sigma'}(K)$ restricts to a map

$$f_\Sigma^{\Sigma'}(K) \colon V_{S'}^{\Sigma'}(K) \longrightarrow B_{S'}(K).$$

The module $\nabla_\Sigma^{\Sigma'}(K)$ is defined to be the cokernel of $f_\Sigma^{\Sigma'}(K)$.

2.2 Functorial Properties

We now recall some properties of the map $f_\Sigma^{\Sigma'}$ described above. Let E/F denote any CM extension contained in K. Fix a prime p. We prove in [6] that if the sets of primes Σ, Σ' satisfy certain conditions, then the modules $V_{S'}^{\Sigma'}(E)_p$ and $B_{S'}^{\Sigma'}(E)_p$ are free $\mathbf{Z}_p[G_K]$-modules of rank $(\#S' - 1)$. After choosing bases, it therefore makes sense to consider the determinant of the map

$$f_\Sigma^{\Sigma'}(E)_p \colon V_{S'}^{\Sigma'}(E)_p \longrightarrow B_{S'}^{\Sigma'}(E)_p.$$

We now consider three specific cases, each of which satisfies the necessary conditions:

1. $f_\Sigma^{\Sigma'}(E)_p$, where $\Sigma = \Sigma(K), \Sigma' = \Sigma'(K)$ are defined in (2).

2. $f_{\Sigma - \{v\}}^{\Sigma'}(E)_p$, where $v \in \Sigma$ is unramified in E/F.

3. $f_\Sigma^{\Sigma' \cup \{v\}}(E)_p$, where $v \notin S' \cup \Sigma'$.

We use the same auxiliary set S' in all three cases.

Using the isomorphism (13), it is clear that a choice of basis for $B_{S'}(K)$ induces a basis for $B_{S'}(E)$ by taking $\mathrm{Gal}(K/E)$-coinvariants; in fact the isomorphism yields a canonical basis.

Similarly, a choice of basis for each of $V_{S'}^{\Sigma'}(K)_p$ and $V_{S'}^{\Sigma' \cup \{v\}}(K)_p$ induces bases for $V_{S'}^{\Sigma'}(E)_p$ and $V_{S'}^{\Sigma' \cup \{v\}}(E)_p$ by taking co-invariants. This follows from the following.

Lemma 12. *The map $f_\Sigma^{\Sigma'}(E)$ equals the $\mathrm{Gal}(K/E)$ co-invariants of the map $f_\Sigma^{\Sigma'}(K)$.*

Proof. See [6, Appendix B]. $\qquad\square$

Proposition 13. *We have:*

1. $\det(f_\Sigma^{\Sigma'}(E)_p) = \mathrm{red}_{K/E}(\det(f_\Sigma^{\Sigma'}(K)_p))$

2. $\det(f_\Sigma^{\Sigma'}(E)_p) = (1 - \sigma_v^{-1})\det(f_{\Sigma - \{v\}}^{\Sigma'}(E)_p)$

3. Suppose $v \notin S'$. Then

$$\det(f_\Sigma^{\Sigma' \cup \{v\}}(E)_p) = \mathrm{red}_{K/E}(x_K)(1 - \sigma_v^{-1}\mathrm{N}v)\det(f_\Sigma^{\Sigma'}(E)_p)$$

for some $x_K \in \mathbf{Z}_p[G_K]^*$ that does not depend on E.

Proof. (1) This follows immediately from Lemma 12.

(2) Consider the map of complexes:

$$
\begin{array}{ccc}
V_{S'}^{\Sigma'}(E)_p & \xrightarrow{\;f_\Sigma^{\Sigma'}(E)_p\;} & B_{S'}(E)_p \\
\downarrow & & \downarrow \\
V_{S'}^{\Sigma'}(E)_p & \xrightarrow{\;f_{\Sigma-\{v\}}^{\Sigma'}(E)_p\;} & B_{S'}(E)_p.
\end{array}
$$

The first vertical arrow is an equality, while the second vertical arrow is equal to

$$(\mathrm{id}, 1 - \sigma_v^{-1})\colon N \oplus \mathbf{Z}_p[G_E] \longrightarrow N \oplus \mathbf{Z}_p[G_E],$$

where N is a free $\mathbf{Z}_p[G_E]$-module. This has determinant $(1 - \sigma_v^{-1})$, and so we conclude that $\det(f_\Sigma^{\Sigma'}(E)_p) = (1 - \sigma_v^{-1})\det(f_{\Sigma-\{v\}}^{\Sigma'}(E)_p)$.

(3) Consider the map of complexes

$$
\begin{array}{ccc}
V_{S'}^{\Sigma' \cup \{v\}}(E)_p & \xrightarrow{\;f_\Sigma^{\Sigma' \cup \{v\}}(E)_p\;} & B_{S'}(E)_p \\
\downarrow & & \downarrow \\
V_{S'}^{\Sigma'}(E)_p & \xrightarrow{\;f_\Sigma^{\Sigma'}(E)_p\;} & B_{S'}(E)_p.
\end{array}
$$

This map of complexes is injective, with cokernel

$$\mathrm{Ind}_{\mathbf{Z}[G_{E_w}]}^{\mathbf{Z}[G_E]}(\mathbf{F}_w^*)_p \longrightarrow 0,$$

where w is a place of E over v and $\mathbf{F}_w$ is its residue field. This uses the fact that the auxiliary set S' used to define $V_{S'}^{\Sigma'}(E)$ does not include v.

Since the domain and codomain of

$$h_E\colon V_{S'}^{\Sigma' \cup \{v\}}(E)_p \longrightarrow V_{S'}^{\Sigma'}(E)_p$$

are projective, h_E is a quadratic presentation of $\mathrm{Ind}_{\mathbf{Z}[G_{E_w}]}^{\mathbf{Z}[G_E]}(\mathbf{F}_w^*) \otimes \mathbf{Z}_p[G_E]$. The Fitting ideal of $\mathrm{Ind}_{\mathbf{Z}[G_{E_w}]}^{\mathbf{Z}[G_E]}(\mathbf{F}_w^*) \otimes \mathbf{Z}_p[G_E]$ as a $\mathbf{Z}_p[G_E]$-module is $(1 - \sigma_v^{-1}\mathrm{N}v)$. Hence, for any choice of basis for the domain and codomain of h_E, we have $\det(h_E) = x_E(1 - \sigma_v^{-1}\mathrm{N}v)$ for some $x_E \in \mathbf{Z}_p[G_E]^*$.

Note that h_E equals the $\mathrm{Gal}(K/E)$ co-invariants of the map h_K. Thus if we use bases for the domain and codomain of h_E induced from a choice of bases for h_K, then we may take $x_E = \mathrm{red}_{K/E}(x_K)$. We conclude that

$$\det(f_\Sigma^{\Sigma' \cup \{v\}}(E)_p) = \mathrm{red}_{K/E}(x_K)(1 - \sigma_v^{-1}\mathrm{N}v)\det(f_\Sigma^{\Sigma'}(E)).$$

$\square$

Consider the maps $f_K = f_{\Sigma(K)}^{\Sigma'(K)}(K)_p$ and $f_E = f_{\Sigma(E)}^{\Sigma'(K)}(E)_p$ from the introduction. From parts 1 and 2 of Proposition 13, we obtain:

Corollary 14.

$$\det(f_E) = P(K/E)\,\mathrm{red}_{K/E}(\det(f_K)). \tag{14}$$

Consider a finite abelian CM extension K'/F containing K such that $\Sigma(K') = \Sigma(K)$, with maps $g_{E'} := f_{\Sigma(E')}^{\Sigma'(K')}(E')$ for any CM field $E' \subset K'$ containing F. Define

$$Q(K'/K) = \prod_{v \in \Sigma'(K') - \Sigma'(K)} (1 - \sigma_v^{-1}\mathrm{N}v). \tag{15}$$

Note that the map $g_{K'}$ may require a larger auxiliary set S' than f_K did. To deal with this, we use the following lemma:

Lemma 15. *Let $S_1' \subset S_2'$ be two auxiliary sets for (K, Σ, Σ'), with maps denoted $f_\Sigma^{\Sigma'}(K)_1$ and $f_\Sigma^{\Sigma'}(K)_2$. A choice of bases for the domain and codomain of $f_\Sigma^{\Sigma'}(K)_1$ naturally determines bases for the domain and codomain of $f_\Sigma^{\Sigma'}(K)_2$, and with these bases, $\det(f_\Sigma^{\Sigma'}(K)_1) = \det(f_\Sigma^{\Sigma'}(K)_2)$.*

Proof. By induction, we add one prime at a time, and consider $S_1' = S'$, $S_2' = S' \cup \{v\}$. The injective map of complexes

$$
\begin{array}{ccc}
V_{S'}^{\Sigma'}(K)_p & \xrightarrow{\ f_\Sigma^{\Sigma'}(K)_1\ } & B_{S'}(K)_p \\
\downarrow & & \downarrow \\
V_{S' \cup \{v\}}^{\Sigma'}(K)_p & \xrightarrow{\ f_\Sigma^{\Sigma'}(K)_2\ } & B_{S' \cup \{v\}}(K)_p
\end{array}
$$

has cokernel

$$\mathbf{Z}_p[G_K] \xrightarrow{\ \cong\ } \mathbf{Z}_p[G_K].$$

Given a basis of $V_{S'}^{\Sigma'}(K)_p$ and any choice of splitting of the surjection

$$V_{S' \cup \{v\}}^{\Sigma'}(K) \longrightarrow \mathbf{Z}_p[G_K],$$

we obtain a basis of $V_{S' \cup \{v\}}^{\Sigma'}(K)$. The comparison of determinants is then clear. $\square$

Corollary 16. *There exists a unit $x_K \in \mathbf{Z}_p[G_K]^*$ such that, for any CM field $E \subset K$ containing F,*

$$\det(g_E) = \mathrm{red}_{K/E}(x_K) Q(K'/K) \det(f_E).$$

Proof. Since $g_E = f_{\Sigma(E)}^{\Sigma'(K')}(E)$ and $f_E = f_{\Sigma(E)}^{\Sigma'(K)}(E)$ with the same auxiliary set S' by Lemma 15, we apply Proposition 13 (3) to the primes $v \in \Sigma'(K') - \Sigma'(K)$. $\square$

3   Norm compatible families

Recall that we have defined units $y_E \in (\mathbf{Z}_p[G_E]_-)^*$ such that

$$\det(f_{E,-}) = y_E \Theta_{\Sigma(E),\Sigma'(K)}(E/F).$$

In this section we first prove Proposition 7, which states that the units $(e_E y_E)_{E \subset K}$ are a norm compatible family. Next we prove that this norm compatible family extends over CM abelian extensions K'/F containing K. Finally, we prove Proposition 10 on the scarcity of norm compatible families that enjoy this extension property.

3.1   Construction and extension of a norm compatible family

Proof of Proposition 7. From the definitions of the Stickelberger elements, we have

$$\mathrm{red}_{E'/E}(\Theta_{\Sigma(E'),\Sigma'(K)}(E'/F)) = \Theta_{\Sigma(E),\Sigma'(K)}(E/F) P(E'/E) \tag{16}$$

in $\mathbf{Z}_p[G_E]_-$. Combining (5), (14) and (16), we find

$$(\mathrm{red}_{E'/E}(y_{E'}) - y_E)\Theta_{\Sigma(E),\Sigma'(K)}(E/F) P(E'/E) = 0. \tag{17}$$

We project to the quotient R_E of $\mathbf{Z}_p[G_E]_-$, on which $\Theta_{\Sigma(K),\Sigma'(E)}(E/F)$ is a non-zerodivisor and can be canceled. This yields

$$(e_E \, \mathrm{red}_{E'/E}(y_{E'}) - e_E y_E) P(E'/E) = 0$$

in R_E as desired. $\square$

Proposition 17. *Let K'/F be a finite abelian CM extension such that*

$$K' \supset K \text{ and } \Sigma(K') = \Sigma(K).$$

The norm compatible family $(e_E y_E)_{E \subset K}$ extends to a norm compatible family $(e_E y_E)_{E \subset K'}$.

Proof. Using Theorem 4 we define units $w_{E'} \in (\mathbf{Z}_p[G_{E'}]_-)^*$ such that

$$\det(g_{E'}) = w_{E'} \Theta_{\Sigma(E'),\Sigma'(K')}(E'/F). \tag{18}$$

Applying Proposition 7 to K'/F, we have the norm compatibility

$$e_E(\mathrm{red}_{E'/E}(w_{E'}) - w_E)P(E'/E) = 0 \text{ in } R_E$$

for any $F \subset E \subset E' \subset K'$. Now we have

$$\det(g_E) = w_E \Theta_{\Sigma(E),\Sigma'(K')}(E/F) = w_E \Theta_{\Sigma(E),\Sigma'(K)}(E/F)\overline{Q(K'/K)}, \qquad (19)$$

while Corollary 16 implies that

$$\begin{aligned}\det(g_E) &= \mathrm{red}_{K/E}(x_K)(\det f_E)\overline{Q(K'/K)} \\ &= \mathrm{red}_{K/E}(x_K)y_E\Theta_{\Sigma(E),\Sigma'(K)}(E/F)\overline{Q(K'/K)}. \end{aligned} \qquad (20)$$

Comparing (19) and (20) and canceling the expression $\Theta_{\Sigma(E),\Sigma'(K)}(E/F)\overline{Q(K'/K)}$, which is a non-zerodivisor on R_E, we obtain

$$e_E y_E \, \mathrm{red}_{K/E}(x_K) = e_E w_E \text{ in } R_E$$

for each $E \subset K$.

We may therefore choose an arbitrary element $x_{K'} \in \mathbf{Z}_p[G_{K'}]_-$ lifting x_K, and we obtain that $(e_{E'}w_{E'} \, \mathrm{red}_{K'/E'}(x_{K'})^{-1})_{E' \subset K'}$ is a norm compatible family that is equal to $(e_E y_E)$ for $E \subset K$. □

3.2   Scarcity of Norm Compatible Familes

In this section, we prove Proposition 10.

Lemma 18. *Let E/F be a finite abelian CM extension, let $v \mid p$ with $v \notin \Sigma(E)$, and let m be a positive integer. There exists a CM abelian extension E'/F containing E such that:*

- $\Sigma(E') = \Sigma(E)$,

- $\#G_{E,w} = \#G_{E',w}$ *for all $w \in \Sigma(E)$,*

- *the Frobenius σ_v in $G_{E'}$ has order divisible by p^m.*

Proof. We use [14, Theorem 9.2.7] to construct an extension F' of F with prescribed decomposition of primes above p. Using the notation in *loc. cit.* we take S to be the set of all finite places of F, the set T_0 to be the set of primes in F above p and T to be the empty set. Then by [14, Theorem 9.2.7] the canonical homomorphism

$$H^1(F, \mathbf{Z}/p^r\mathbf{Z}) \longrightarrow \oplus_{\mathfrak{p}|p} H^1(F_\mathfrak{p}, \mathbf{Z}/p^r\mathbf{Z})$$

has cokernel of order 1 or 2 (the latter can occur only if $p = 2$). Therefore there exists a totally real cyclic extension F' of F such that

(i) each prime $v' \in \Sigma(E)$ has trivial decomposition subgroup.

(ii) all primes above p not in $\Sigma(E)$ are unramified in F'.

(iii) The decomposition subgroup of v in $\mathrm{Gal}(F'/F)$ has order at least p^{r-1}.

Taking $r = m + 1$ and $E' = EF'$ gives the required extension.

$\square$

The proof of Proposition 10 will proceed by induction. We are given a norm compatible set of elements $(z_E)_{E \subset K}$, with $z_E \in R_E$. Write

$$\Sigma(K) = \{v_1, v_2, \ldots, v_m\}. \tag{21}$$

For $i = 0, \ldots, m$, define

$$P_i(E'/E) = \prod_{\substack{j > i \\ v_j \in \Sigma(E') - \Sigma(E)}} (1 - \sigma_{v_j}^{-1}) \in \mathbf{Z}_p[G_E]_-.$$

So in particular $P_0(E'/E) = P(E'/E)$ as defined earlier, and $P_m(E'/E) = 1$. We will prove the following statement by induction on i:

There exists $\tilde{z}_K \in \mathbf{Z}_p[G_K]_-$ lifting $z_K \in R_K$ such that

$$(e_E \, \mathrm{red}_{K/E}(\tilde{z}_K) - z_E) P_i(K/E) = 0 \tag{22}$$

in R_E for all $E \subset K$.

Note that we will induct on this statement for all fields $K' \supset F$ satisfying (21) with associated norm compatible system $(z_E)_{E \subset K'}$, not just the K that we start with. The base case $i = 0$ is automatic, as it is the definition of norm compatible system; any lift $\tilde{z}_K$ will do. So let $i \geq 1$ and suppose the statement holds for $i - 1$; we want to prove it for i.

Lemma 19. *In order to deduce (22), it suffices to prove that for each positive integer k, there exists $\tilde{z}_{K,k} \in \mathbf{Z}_p[G_K]_-$ lifting $z_K \in R_K$ such that*

$$(e_E \, \mathrm{red}_{K/E}(\tilde{z}_{K,k}) - z_E) P_i(K/E) \equiv 0 \ \text{in} \ R_E/p^k \tag{23}$$

for all $E \subset K$.

Proof. Let J denote the intersection of the kernels of the compositions

$$\mathbf{Z}_p[G_K]_- \longrightarrow \mathbf{Z}_p[G_E]_- \longrightarrow R_E$$

for all E, and for each positive integer k let $J_k \supset J$ denote the intersections of the kernels of the compositions

$$\mathbf{Z}_p[G_K]_- \longrightarrow \mathbf{Z}_p[G_E]_- \longrightarrow R_E \longrightarrow R_E/p^k.$$

14

The defining equation (23) of the $\tilde{z}_{K,k}$ specifies its value uniquely modulo J_k. We therefore have $\tilde{z}_{K,k+1} \equiv \tilde{z}_{K,k} \pmod{J_k}$. Hence the $\{\tilde{z}_{K,k}\}$ specify a unique element of

$$\varprojlim_k \mathbf{Z}_p[G_K]_- / J_k = \mathbf{Z}_p[G_K]_- / \bigcap_{k=1}^{\infty} J_k = \mathbf{Z}_p[G_K]_- / J.$$

Letting $\tilde{z}_K$ be any lift of this element to $\mathbf{Z}_p[G_K]_-$ gives the desired result. $\qquad\square$

Fix a positive integer k. Let E be a CM field with $F \subset E \subset K$ such that v_i is unramified in E (i.e. $v_i \notin \Sigma(E)$). Let p^r denote the power of p dividing $\prod_{v \in \Sigma(E)} \#G_{E,v}$, and let p^s be the power of p dividing the order of σ_v in G_E. Let $k' = k + r + s$. Let E' be as in Lemma 18 for $m = k'$.

Let K' be the compositum of K with all fields E' defined in this way (there is one such E' for each CM subfield $E \subset K$ containing F, so K'/F is a finite abelian CM extension). We consider a norm compatible family $(z_L)_{L \subset K'}$ extending the given family. Using the induction hypothesis, we find a lift $\tilde{z}_{K'} \in \mathbf{Z}_p[G_{K'}]_-$ such that

$$(e_L \, \mathrm{red}_{K'/L}(\tilde{z}_{K'}) - z_L) P_{i-1}(K'/L) = 0 \tag{24}$$

for all $L \subset K'$.

We define

$$\tilde{z}_K = \mathrm{red}_{K'/K}(\tilde{z}_{K'}) \in \mathbf{Z}_p[G_K]_-.$$

This is a lift of $z_K \in R_K$ by the norm compatibility relation since $\Sigma(K') = \Sigma(K)$.

If $L \subset K$ is a CM field containing F such that $v_i \in \Sigma(L)$, then $P_i(K/L) = P_{i-1}(K/L)$, and the statement (24) can be written

$$(e_L \, \mathrm{red}_{K/L}(\tilde{z}_K) - z_L) P_i(K/L) = 0.$$

This is exactly the statement (22) that we are trying to prove for the field L. It remains to consider the more salient case of the fields E such that $v_i \notin \Sigma(E)$ which were used in the construction of K'. For $L = E'$ with E' as above, (24) reads

$$(e_{E'} \, \mathrm{red}_{K'/E'}(\tilde{z}_{K'}) - z_{E'}) P_i(K'/E')(1 - \sigma_{v_i}^{-1}) = 0. \tag{25}$$

By the definition of $e_{E'}$ given in (6), and the second property of the extension E' given in Lemma 18, we see that $p^r e_{E'} \in \mathbf{Z}_p[G_{E'}]$. Hence, $p^r z \in \mathbf{Z}_p[G_{E'}]_-$ for any $z \in R_{E'} \subset \mathbf{Q}_p[G_{E'}]_-$. From (25) we therefore have

$$(p^r e_{E'} \, \mathrm{red}_{K'/E'}(\tilde{z}_{K'}) - p^r z_{E'}) P_i(K'/E')(1 - \sigma_{v_i}^{-1}) = 0 \text{ in } \mathbf{Z}_p[G_{E'}]_-.$$

The kernel of multiplication by $(1 - \sigma_{v_i}^{-1})$ in $\mathbf{Z}_p[G_{E'}]_-$ is the ideal generated by

$$1 + \sigma_{v_i} + \cdots + \sigma_{v_i}^{n'-1}$$

where n' is the order of σ_{v_i} in $G_{E'}$. We can therefore write

$$(p^r e_{E'} \operatorname{red}_{K'/E'}(\tilde{z}_{K'}) - p^r z_{E'}) P_i(K'/E') \in (1 + \sigma_v + \cdots + \sigma_v^{n'-1}) \text{ in } \mathbf{Z}_p[G_{E'}]_-.$$

Reducing to $\mathbf{Z}_p[G_E]_-$, we find

$$\left[p^r e_E \operatorname{red}_{K'/E}(\tilde{z}_{K'}) - \operatorname{red}_{E'/E}(p^r z_{E'}) \right] P_i(K/E) \tag{26}$$
$$\in (n'/n)(1 + \sigma_{v_i} + \cdots + \sigma_{v_i}^{n-1}) \subset (p^{k'-s}) \text{ in } \mathbf{Z}_p[G_E]_-,$$

where n is the order of σ_v in G_E. Note that $\operatorname{red}_{E'/E}(p^r z_{E'}) = p^r z_E$ by the norm compatibility relation, since $\Sigma(E') = \Sigma(E)$. Therefore, projecting (26) to R_E and canceling p^r we obtain

$$(e_E \operatorname{red}_{K'/E}(\tilde{z}_{K'}) - z_E) P_i(K/E) \in (p^{k'-s-r}) = (p^k) \text{ in } R_E. \tag{27}$$

From (27) we obtain

$$(e_E \operatorname{red}_{K/E}(\tilde{z}_K) - z_E) P_i(K/E) \equiv 0 \text{ in } R_E/p^k.$$

This is (23), so by Lemma 19 we obtain the desired inductive statement (22). The result for $i = m$ is exactly the statement of Proposition 10, since $P_m(K/E) = 1$. This concludes the proof of Proposition 10.

A   Reductions

In this appendix we prove Lemmas 2 and 6, which together show that Theorem 5 implies Theorem 1. The proof of Lemma 6 has the same flavor as the computations of §2.2, but is significantly more complicated because of the changing set S'.

Lemma 2 is standard.

Proof of Lemma 2. Theorem 3 for all primes p yields an element $y_K \in (\hat{\mathbf{Z}}[G_K]_-)^*$ such that (1) holds. We need to show that $y_K \in (\mathbf{Z}[G_K]_-)^*$. Let χ be an odd character of G and let $E \subset K$ denote the fixed field of the kernel of χ. Applying χ to (1), we obtain

$$\chi(\det(f_{S(E)}^T)) = \chi(y_K) L_{S(E),T}(\chi^{-1}, 0).$$

Since $\chi(v) \neq 1$ for $v \in S(E)$, it follows that $\chi(\det(f_{S(E)}^T))$ and $L_{S(E),T}(\chi^{-1}, 0)$ are non-zero algebraic numbers, and therefore the same is true for $\chi(y_K)$. Therefore $y_K \in \overline{\mathbf{Q}}[G_K]_-$. The desired result follows since

$$\overline{\mathbf{Q}}[G_K]_- \cap (\hat{\mathbf{Z}}[G_K]_-)^* = (\mathbf{Z}[G_K]_-)^*.$$

$\square$

The proof of Lemma 6 is more subtle. We should mention that such an "independence of (S, T) sets" result was proved by Atsuta and Kataoka in [2, Proposition 3.1(iii)].

We begin with an important purely local computation regarding local Ritter–Weiss modules. Let L/K be an abelian extension of ℓ-adic local fields (i.e. finite extensions of $\mathbf{Q}_\ell$). Write $G = \mathrm{Gal}(L/K)$. Let V denote the local Ritter–Weiss G-module associated to L as in (9). Let $U \subset \mathcal{O}_L^*$ denote the subgroup of 1-units. We then obtain a short exact sequence

$$1 \longrightarrow L^*/U \longrightarrow V/U \longrightarrow \Delta G \longrightarrow 1. \tag{28}$$

We will work over $\mathbf{Z}_p$ where $p \neq \ell$ is another prime. For any G-module M, we write M_p for the $\mathbf{Z}_p[G]$-module $M \otimes_{\mathbf{Z}} \mathbf{Z}_p$. Let $I \subset G$ be the inertia group. Let $e = \#I$ be the size of I, write $\mathrm{N}I = \sum_{g \in I} g$, and let $\sigma \in G$ be a representative of the Frobenius coset in G/I.

Lemma 20. *With notation as above, there exist an element $\tilde{x} \in V$ that maps to*

$$x = e - \sigma^{-1}\mathrm{N}I \in \Delta G$$

under (28) and satisfies the following. If $M = V/(U, \tilde{x})$, then

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]}(M_p) = (y), \qquad y = e - \sigma^{-1}\mathrm{N}I \cdot q, \tag{29}$$

where q is the size of the residue field of K.

Remark 21. It can be shown that if $\tilde{x} \in V$ is *any* element mapping to x in ΔG, then

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]}(M_p) = (y) \text{ for some } y \equiv e - \sigma^{-1}\mathrm{N}I \cdot q \pmod{\mathrm{N}G}. \tag{30}$$

This does not affect the proof of Lemma 6 that follows, since $\Theta_{S,T}(K/F) \cdot \mathrm{N}G_v = 0$ for any $v \in S$. The statement (30) requires a little extra computation and is not necessary for our proof of Lemma 6.

Proof. We begin with a reduction that will greatly simplify the notation. Namely, we show that it suffices to prove the result in the case that the inertia group I is pro-p (hence tame, hence cyclic). We can uniquely decompose $G = G_p \times G'$ where G_p is the p-Sylow subgroup of G and G' is the subgroup of prime-to-p order elements. We have a corresponding decomposition $I = I_p \times I'$. The group ring $\mathbf{Z}_p[G]$ decomposes as a product

$$\mathbf{Z}_p[G] = \prod_{(\chi)} R_\chi, \qquad R_\chi = e_{(\chi)}\mathbf{Z}_p[G],$$

as (χ) ranges over the $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-conjugacy classes of characters of G'. Here

$$e_{(\chi)} = \sum_{\chi \in (\chi)} e_\chi$$

17

is the usual idempotent. It suffices to prove the result on each component R_χ.

If $\chi(I') \neq 1$, the result is easy to see from (28). Indeed, in this case we have

$$(L^*/U)_{(\chi)} := (L^*/U)_p \otimes_{\mathbf{Z}_p[G]} R_\chi = 0.$$

This follows from the short exact sequence

$$1 \longrightarrow k_L^* \longrightarrow L^*/U \longrightarrow \mathbf{Z} \longrightarrow 1.$$

Since I' acts trivially on k_L^* and $\mathbf{Z}$, the assumption $\chi(I') \neq 1$ implies that $e_{(\chi)}$ annihilates these modules, whence it annihilates L^*/U. Therefore

$$(V/U)_{(\chi)} \cong (\Delta G)_{(\chi)} \cong R_\chi,$$

hence

$$\mathrm{Fitt}_{R_\chi}(V/(U, \tilde{x}))_{(\chi)} = \mathrm{Fitt}_{R_\chi}(R_\chi/x) = (x)$$

for any $\tilde{x} \in V$ mapping to $x \in \Delta G$. The desired result then follows since $e_{(\chi)}x = e_{(\chi)}y$, as $\mathrm{N}I = \mathrm{N}I_p \cdot \mathrm{N}I'$, and $e_{(\chi)}\mathrm{N}I' = 0$ because $\chi(I') \neq 1$.

It therefore remains to consider the components R_χ such that $\chi(I') = 1$. Let $L' = L^{I'}$ be the subfield fixed by I'. It is elementary to check that

$$(V/U)_{(\chi)} \cong (V(L')/U(L'))_{(\chi)},$$

for example, by connecting the (χ)-components of the sequences (28) for L and L' and using the five lemma. Therefore, on these components we can replace L by L', which satisfies the property that the inertia subgroup of $\mathrm{Gal}(L'/K)$ is a p-group.

We therefore start the proof afresh with the assumption that I is cyclic of order prime to ℓ. Let τ be a generator of I. We define $\mathbf{Z}_p[G]$-module generators of $(V/U)_p$ using the definition of V given in [6, Equation (133)]. Let $\tilde{\sigma}, \tilde{\tau} \in \mathrm{W}(L^{\mathrm{ab}}/K)$ be lifts of σ, τ, respectively. Specifically, we let $\tilde{\tau}$ be a lift to the tame inertia subgroup of $\mathrm{W}(L^{\mathrm{ab}}/K)$, and let σ be a representative of the Frobenius coset. Let $g_{\tilde{\sigma}}, g_{\tilde{\tau}} \in V/U$ be the images of $1 - \tilde{\sigma}^{-1}$ and $\tilde{\tau} - 1$ respectively. We claim that these elements are generators of $(V/U)_p$, and that there is a single relation between them.

To prove this, we employ the short exact sequence

$$1 \longrightarrow k_L^* \longrightarrow V/U \longrightarrow W \longrightarrow 1 \tag{31}$$

obtained from (10). The elements $g_{\tilde{\sigma}}, g_{\tilde{\tau}}$ map to

$$g_\sigma = (1 - \sigma^{-1}, 1) \text{ and } g_\tau = (\tau - 1, 0) \text{ in } W,$$

respectively, using the model of W given in (11). The relations among g_σ, g_τ in W are generated by

$$(\tau - 1)g_\sigma - (1 - \sigma^{-1})g_\tau = 0, \tag{32}$$

$$\mathrm{N}I \cdot g_\tau = 0. \tag{33}$$

18

The element $\mathrm{N}I \cdot g_{\tilde{\tau}} = \tilde{\tau}^e - 1$ maps to $\mathrm{N}I \cdot g_{\tau} = 0$ in W, and hence under the exact sequence (31) corresponds to an element of k_L^*. We claim that this element is a multiplicative generator of the cyclic group k_L^*. To see this note that we can consider a finite Galois extension $\tilde{L}/K$ containing L whose inertia $\tilde{I}$ is tame and sits in a short exact sequence

$$1 \longrightarrow k_L^* \longrightarrow \tilde{I} \longrightarrow I \longrightarrow 1.$$

For example, the abelian extension of L corresponding to $\hat{L}^*/\overline{(U, \pi_K)}$ under class field theory, where π_K is a uniformizer of K, is such an extension. But $\tilde{I}$ is the tame inertia of a finite Galois extension of K and hence cyclic. Therefore, any lift $\tilde{\tau}$ of the generator τ of I is a generator of $\tilde{I}$. This implies that $\tilde{\tau}^e$ is a generator of k_L^*.

These considerations imply our claim that $g_{\tilde{\sigma}}$ and $g_{\tilde{\tau}}$ generate $(V/U)_p$ as a $\mathbf{Z}_p[G]$-module. To compute the relations among these generators, we lift the relations (32) and (33). For (33), we have already observed that $\mathrm{N}I \cdot g_{\tilde{\tau}}$ is a generator of k_L^*. The annihilator of k_L^* is generated by $1 - \sigma^{-1}q$ and $\tau - 1$. Now $\tau - 1$ annihilates $\mathrm{N}I$, so this leads to the trivial relation. We therefore obtain only one relation in $(V/U)_p$ from the relation (33) in W, namely

$$(1 - \sigma^{-1}q)\mathrm{N}I \cdot g_{\tilde{\tau}} = 0. \tag{34}$$

For (32) we note that

$$\begin{aligned}
(\tau - 1)g_{\tilde{\sigma}} - (\sigma - 1)g_{\tilde{\tau}} &= \tau\sigma^{-1}(\tilde{\sigma}\tilde{\tau}^{-1}\tilde{\sigma}^{-1}\tilde{\tau} - 1) \\
&= \tau\sigma^{-1}(\tilde{\tau}^{1-q} - 1) \\
&= \sigma^{-1}\left(\frac{1-q}{e}\right)\mathrm{N}I \cdot g_{\tilde{\tau}}.
\end{aligned}$$

We therefore obtain the relation

$$(\tau - 1)g_{\tilde{\sigma}} - \left(1 - \sigma^{-1} + \sigma^{-1}\left(\frac{1-q}{e}\right)\mathrm{N}I\right)g_{\tilde{\tau}} = 0. \tag{35}$$

Now, it is easy to see that (34) can be obtained from (35) by multiplying by $\mathrm{N}I$. We have therefore proven our claim that $(V/U)_p$ has a presentation with two generators $g_{\tilde{\sigma}}, g_{\tilde{\tau}}$, and the one relation (35).

To conclude the proof, we note that the element

$$\tilde{x} = -e \cdot g_{\tilde{\sigma}} - z \cdot g_{\tilde{\tau}}, \tag{36}$$

where

$$z = \sigma^{-1}((e-1) + (e-2)\tau + (e-3)\tau^2 + \cdots + \tau^{e-2})$$

(with the understanding $z = 0$ if $e = 1$) maps to

$$e(1 - \sigma^{-1}) - z \cdot (\tau - 1) = x$$

19

in ΔG. We have that $\mathrm{Fitt}_{\mathbf{Z}_p[G]}((V/(U, \tilde{x}))_p)$ is generated by

$$\det \begin{pmatrix} \tau - 1 & \sigma^{-1} - 1 - \sigma^{-1}\left(\frac{1-q}{e}\right)\mathrm{N}I \\ -e & -z \end{pmatrix} = e - \sigma^{-1}q \cdot \mathrm{N}I.$$

This equality is a direct calculation, and completes the proof. $\qquad\square$

We can now prove Lemma 6, which states that the (Σ, Σ') version of the ETNC over $\mathbf{Z}_p$ implies the (S, T) version over $\mathbf{Z}_p$.

Proof. The main difficulty in relating the (Σ, Σ') and (S, T) versions of the ETNC is the fact that different sets S' must be taken by the assumptions on this set. Write

$$J = S \setminus \Sigma = \Sigma' \setminus T = \{v \in S_{\mathrm{ram}}(H/F) : v \nmid p\}.$$

When working with (Σ, Σ'), we start with a set S' that is necessarily disjoint from J. Let us fix this choice of S'. When we work with (S, T), the set that plays the role of S' must contain J, so we use $S' \cup J$. From the definitions[1] one finds that there is a short exact sequence

$$0 \longrightarrow V_{S'}^{\Sigma'}(K) \overset{\iota}{\longrightarrow} V_{S' \cup J}^{T}(K) \longrightarrow \overset{\sim}{\prod_{v \in J}} V_w/U_w^1 \longrightarrow 0.$$

Here w denotes the place of K above the place v of F used in the definition of the V modules. Meanwhile, the isomorphism (13) yields

$$B_{S' \cup J}(K)_p \cong \prod_{v \in S' \cup J \setminus \infty} \mathbf{Z}_p[G_K] \cong B_{S'}(K)_p \oplus \prod_{v \in J} \mathbf{Z}_p[G_K].$$

This identification yields natural bases for $B_{S'}(K)$ and $B_{S' \cup J}(K)$. For each $v \in J$, let $(x_v, \tilde{x}_v)$ be the pair $(x, \tilde{x})$ for the local extension K_w/F_v given in Lemma 20. We consider the following commutative diagram of free $\mathbf{Z}_p[G_K]$-modules of rank $\#(S' \cup J) - 1$:

$$
\begin{array}{ccc}
V_{S'}^{\Sigma'}(K)_p \oplus \prod_{v \in J} \mathbf{Z}_p[G_K] & \overset{(f_{\Sigma}^{\Sigma'}(K)_p, 1)}{\longrightarrow} & B_{S'}(K)_p \oplus \prod_{v \in J} \mathbf{Z}_p[G_K] \\
\downarrow{\scriptstyle (\iota, \tilde{x}_v)} & & \downarrow{\scriptstyle (1, x_v)} \\
V_{S' \cup J}^{T}(K)_p & \overset{f_S^T(K)_p}{\longrightarrow} & B_{S' \cup J}(K)_p.
\end{array}
\tag{37}
$$

By Theorem 5, we can choose a basis of $V_{S'}^{\Sigma'}(K)_p$ such that the top arrow of (37) has determinant $\Theta_{\Sigma, \Sigma'}(K/F)$. The cokernel of the left arrow of (37) is

$$\overset{\sim}{\prod_{v \in J}}(V_w/(U_w^1, \tilde{x}_v))_p,$$

---

[1]The snake lemma must also be used, since the module $V_{S'}^T$ is the kernel of θ_V.

which by Lemma 20 has Fitting ideal generated by $\prod_{v \in J} y_v$, where y_v is the element (29). We can therefore choose a basis for $V_{S' \cup J}^T(K)_p$ such that the determinant of the left arrow of (37) is exactly $\prod_{v \in J} y_v$. The commutative diagram (37) therefore yields

$$\det(f_S^T(K)_p) \prod_{v \in J} y_v = \Theta_{\Sigma, \Sigma'}(K/F) \prod_{v \in J} x_v.$$

Since the elements y_v are non-zerodivisors, we may divide, and we obtain

$$\det(f_S^T(K)_p) = \Theta_{\Sigma, \Sigma'}(K/F) \prod_{v \in J}(x_v/y_v) = \Theta_{S,T}(K/F)$$

as desired. The same analysis holds for any CM subfield $E \subset K$ containing F. Take $\mathrm{Gal}(K/E)$-coinvariants of each term in (37). Replace the horizontal arrows by $(f_{\Sigma(E)}^{\Sigma'}(E)_p, 1)$ and $f_{S(E)}^T(E)_p$. Leave the left vertical arrow the same, but to maintain commutativity of the diagram, replace x_v by $e_v = \#I_v$ on the right at the places $v \in J$ such that $v \notin S(E)$. The explanation for this is the definition of the local component $V_w \longrightarrow \mathbf{Z}[G_w]$ when w is unramified given in §2.1. This map sends the element $\tilde{x}_v$ defined in (36) to e_v.

Now, the elements x_v and y_v for K have images in $\mathbf{Z}_p[G_E]$ equal to the analogous constants for E/F scaled by the ramification index at v of K/E. These extra scaling factors cancel, and we obtain

$$\det(f_{S(E)}^T(E)) = \Theta_{\Sigma(E), \Sigma'}(K/F) \prod_{v \in S(E) - \Sigma(E)} (x_v/y_v) \prod_{v \in J, \ v \notin S(E)} (e_v/y_v)$$
$$= \Theta_{S(E), T}(E/F).$$

This completes the proof. □

B   Consequences

The fact that the ETNC in its various formulations implies the consequences stated in §1.1 is well-known. In this appendix we indicate how Theorem 1 combined with the refinements of [8] at the prime $p = 2$ can be used to prove these consequences with an improved power of 2. Here we adapt the beautiful argument of Burns, Kurihara, and Sano, who proved that their LTC implies all of these results [4] (without the improved power of 2). Since our argument is essentially identical to theirs, we provide a sketch and discuss only the Brumer–Stark conjecture, focusing on the issues related to projecting to the minus side and the improved power of 2.

We consider our setup as above, with a CM abelian extension K of a totally real field F. We let $S = S_\infty \cup S_{\mathrm{ram}}(K/F)$. Let $\mathfrak{p} \notin S$ denote a prime of F that splits completely in K, and suppose that the auxiliary set S' contains $\mathfrak{p}$. Let us fix one element $v_0 \in S \subset S'$ as

21

follows. If K/F is ramified at some finite place, we let v_0 be such a place; otherwise, we let v_0 be a real place of F. Then as in (13) we have

$$B_{S'}(K)_- \cong \prod_{v \in S' \setminus \{v_0\}} \mathbf{Z}[G_K]_-, \qquad (38)$$

and we fix the basis of $B_{S'}(K)_-$ associated to this isomorphism.

Theorem 1 implies that we may choose a basis for $V_{S'}^T(K)_-$ such that if A is the matrix for $f_S^T(K)_-$ with respect to these bases, then

$$\det(A) = \Theta_{S,T}(K/F) \quad \text{in } \mathbf{Z}[G_K]_-.$$

Note that A is a square matrix of dimension $\#S' - 1$ and coefficients in $\mathbf{Z}[G_K]_-$. As indicated in (38), the columns of A are indexed by the elements $v \in S' \setminus \{v_0\}$.

Now let A_V be the matrix A modified so that in the column indexed by $\mathfrak{p}$, the element in each row is replaced by the basis vector in $V_{S'}^T(K)_-$ indexing that row. So the matrix A_V has all its coefficients in $\mathbf{Z}[G_K]_-$ except one column, which has coefficients in $V_{S'}^T(K)_-$. It makes sense to consider $\det(A_V) \in V_{S'}^T(K)_-$ using the Leibniz rule.

Write $n = [F : \mathbf{Q}]$ and let

$$t = \begin{cases} n & \text{if } S_{\mathrm{ram}}(K/F) \text{ is nonempty,} \\ n-1 & \text{if } S_{\mathrm{ram}}(K/F) \text{ is empty.} \end{cases}$$

Then $S' \setminus \{v_0\}$ contains t real places. The trick observed in [8] is that all the columns of A indexed by these real places are divisible by 2 (they are divisible by $1 - c$ since this element generates the ideal ΔG_w, and $1 - c = 2$ in $\mathbf{Z}[G_K]_-$). Hence we can divide each of these columns by 2 and obtain $\det(A_V)/2^t \in V_{S'}^T(K)_-$. We then define

$$u = (1 - c)\det(A_V)/2^t \in V_{S'}^T(K),$$

which is a well-defined element of $V_{S'}^T(K)$. This is the key point at which we have lifted from $\mathbf{Z}[G_K]_-$ to $\mathbf{Z}[G_K]$.

Lemma 22. *Let $S_{\mathfrak{p}} = S \cup \mathfrak{p}$. The element u lies in the kernel of $f_{S_{\mathfrak{p}}}^T \colon V_{S'}^T(K) \longrightarrow B_{S'}^T(K)$.*

Proof. For any place $v \in S' \setminus \{v_0\}$, the component of $f_{S_{\mathfrak{p}}}^T(u)$ at v is $(1 - c)/2^t$ times the determinant of the matrix A_v obtained from A_V by replacing the column at $\mathfrak{p}$ with its image under the component of $f_{S_{\mathfrak{p}}}^T$ at v. If $v \neq \mathfrak{p}$, this is precisely the column of A_V at v. Hence the matrix A_v has two identical columns, namely the columns indexed by $\mathfrak{p}$ and v. It follows that $\det(A_v) = 0$. If $v = \mathfrak{p}$, the component of $f_{S_{\mathfrak{p}}}^T(u)$ at $\mathfrak{p}$ lies in $\Delta G_{\mathfrak{p}}$, which vanishes since $\mathfrak{p}$ splits completely in K. Therefore $A_{\mathfrak{p}}$ has a column of 0's and hence $\det(A_{\mathfrak{p}}) = 0$. This proves the lemma. $\square$

Now we can view u as an element of $\mathcal{O}_{K,S_{\mathfrak{p}},T}^*$, since this is the kernel of $f_{S_{\mathfrak{p}}}^T$ (see [6, Eqn. (146)]).

Lemma 23. *We have $|u|_w = 1$ for all places $w \nmid \mathfrak{p}$, finite or infinite.*

Proof. For $w \in S_K$ finite, this is the argument of [7, Lemma 4.8], which we briefly sketch. Let $v \in S$ denote the place of F below w. In view of the exact sequence (10), we need to show that the image of u in $\operatorname{Ind}_{G_w}^G W_w(K_w)$ vanishes. This image is evaluated by taking $(1 - c)/2^t$ times the determinant of the matrix $A_{W,v}$ obtained from A_V by replacing the column indexed by $\mathfrak{p}$ by its image in $\operatorname{Ind}_{G_w}^G W_w(K_w)$. But using the definition of $W_w(K_w)$, one can show that the 2×2 minors arising from the columns of $A_{W,v}$ indexed by $\mathfrak{p}$ and v vanish. It follows that $\det(A_{W,v}) = 0$.

For w complex, the result is immediate; by definition, u satisfies $c(u) = u^{-1}$. $\qquad\square$

Recall that defining $V_{S'}^T(K)$ involved choosing a place of K above each place of F. Let $\mathfrak{P}$ denote the place above $\mathfrak{p}$ chosen in this definition. Define

$$\operatorname{ord}_G \colon K^* \longrightarrow \mathbf{Z}[G_K], \qquad x \mapsto \sum_{\sigma \in G} \operatorname{ord}_{\mathfrak{P}}(\sigma(x))\sigma^{-1}.$$

The following is the Brumer–Stark conjecture, with the usual appearance of $\Theta_{S,T}$ improved to $\Theta_{S,T}/2^{t-1}$.

Theorem 24. *We have*

$$\operatorname{ord}_G(u) = \frac{\Theta_{S,T}(K/F)}{2^{t-1}}.$$

Proof. The proof of [7, Lemma 4.9] applies essentially without change. We recall the argument. Consider the map

$$f_{\mathfrak{p}} \colon \operatorname{Ind}_{G_{\mathfrak{P}}}^G V_{\mathfrak{P}}(K_{\mathfrak{P}}) \longrightarrow \mathbf{Z}[G_K]$$

induced by

$$V_{\mathfrak{P}}(K_{\mathfrak{P}}) \longrightarrow W_{\mathfrak{P}}(K_{\mathfrak{P}}) \cong \mathbf{Z}[G_{\mathfrak{P}}] = \mathbf{Z}.$$

Note that if we start with A_V and replace the column indexed by $\mathfrak{p}$ with its image under $f_{\mathfrak{p}}$, then we obtain precisely the matrix A, since the component of f_S^T at $\mathfrak{p}$ is by definition $f_{\mathfrak{p}}$.

Now, the composition of $f_{\mathfrak{p}}$ with

$$K^* \longrightarrow \operatorname{Ind}_{G_{\mathfrak{P}}}^G V_{\mathfrak{P}}(K_{\mathfrak{P}})$$

is precisely the map ord_G. It follows that

$$\operatorname{ord}_G(u) = \frac{(1 - c)}{2^t} \det(A) = \frac{\Theta_{S,T}(K/F)}{2^{t-1}}.$$

$\qquad\square$

The other consequences of Theorem 1 stated in §1.1, with $\Theta_{S,T}$ improved to $\Theta_{S,T}/2^{t-1}$, follow similarly by mildly adapting the arguments of [4].

References

[1] Mahiro Atsuta. Iwasawa theory for class groups of CM fields with $p = 2$. *J. Number Theory* 204:624–660, 2019.

[2] M. Atsuta and T. Kataoka. On the minus component of the equivariant Tamagawa number conjecture for $\mathbb{G}_m$, preprint.

[3] D. Bullach, D. Burns, A. Daoud, and S. Seo. Dirichlet L-series at $s = 0$ and the scarcity of Euler systems, preprint.

[4] David Burns, Masato Kurihara, and Takamichi Sano. On zeta elements for $\mathbb{G}_m$. *Doc. Math.* 21:555–626, 2016.

[5] D. Burns and M. Flach. Tamagawa numbers for motives with (non-commutative) coefficients. *Doc. Math.* 6:501–570, 2001.

[6] Samit Dasgupta and Mahesh Kakde. On the Brumer-Stark conjecture. *Ann. of Math. (2)* 197 (1):289–388, 2023.

[7] ———. Brumer-Stark units and Explicit Class Field Theory. *Duke Math. J.* To appear.

[8] Samit Dasgupta, Mahesh Kakde, Jesse Silliman, and Jiuya Wang. The Brumer-Stark conjecture over **Z**. Preprint.

[9] Leslie Jane Federer. A note on Iwasawa invariants and the main conjecture. *J. Number Theory* 24 (1):107–113, 1986.

[10] Cornelius Greither. Determining Fitting ideals of minus class groups via the equivariant Tamagawa number conjecture. *Compos. Math.* 143 (6):1399–1426, 2007.

[11] Benedict H. Gross. On the values of abelian L-functions at $s = 0$. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 35 (1):177–197, 1988.

[12] Masato Kurihara. Notes on the dual of the ideal class groups of CM-fields. *J. Théor. Nombres Bordeaux* 33 (3):971–996, 2021.

[13] Barry Mazur and Karl Rubin. Refined class number formulas for $\mathbb{G}_m$. *J. Théor. Nombres Bordeaux* 28 (1):185–211, 2016.

[14] 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.

[15] Cristian D. Popescu. 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.

[16] Karl Rubin. A Stark conjecture "over **Z**" for abelian L-functions with multiple zeros. *Ann. Inst. Fourier (Grenoble)* 46 (1):33–62, 1996.

[17] Jürgen Ritter and Alfred Weiss. A Tate sequence for global units. *Compositio Math.* 102 (2):147–178, 1996.

[18] T. Sano. Refined abelian Stark conjectures and the equivariant leading term conjecture of Burns. *Compos. Math.* 150 (11):1809–1835, 2014.