Title
Higher Fitting Ideals of Iwasawa Modules

Author
Stone, Corey Dean

Publication Date
2016

Peer reviewed|Thesis/dissertation

UNIVERSITY OF CALIFORNIA - SAN DIEGO

Higher Fitting Ideals of Iwasawa Modules

A dissertation submitted in partial satisfaction of the requirements for the degree
Doctor of Philosophy

in

Mathematics

by

Corey Dean Stone

Committee in Charge:

Professor Cristian Popescu, Chair
Professor Ron Graham
Professor Kiran Kedlaya
Professor Shachar Lovett
Professor Claus Sorensen

2016

The Dissertation of Corey Dean Stone is approved, and it is acceptable in quality and form for publication on microfilm and electronically:

Chair

University of California, San Diego

2016

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

First, I would like to thank my advisor, Cristian Popescu, for his guidance, support and patience during my research on this dissertation.

I would like to thank all the other math graduate students that I spent time with at UCSD (although there are too many that I would want to name to name them all), for both providing stimulating discussions, and for making my time at UCSD an enjoyable one.

I would like to thank James, for all the support, encouragement, and joy he gave me during my time here in San Diego.

I would like to thank Zach, Adam, Jay, Ryan, and Nicki, for their friendship during my undergraduate degree, and for pushing me to challenge myself during those years.

I would like to thank Cory, for being a grounding presence during the last year, and especially during the writing process of this dissertation.

I would like to thank Dr. Holley, Dr. Radcliffe, and Dr. Walker, for the wonderful education and giving me the encouragement to reach this point.

Finally, I would like to thank my family, especially my parents Cathy and Brian, for the endless love and support they provided. Whenever I was grappling with self-doubt, it was comforting to know that they were always in my corner.

VITA

2011	Bachelor of Science , University of Nebraska - Lincoln
2011 - 2016	Teaching Assistant, University of California San Diego
2016	Doctor of Philosophy, University of California San Diego

FIELDS OF STUDY

Major Field: Mathematics (Number Theory)

Studies in Number Theory

Professor Cristian Popescu

ABSTRACT OF THE DISSERTATION

Higher Fitting Ideals of Iwasawa Modules

by

Corey Dean Stone

Doctor of Philosophy in Mathematics

University of California San Diego, 2016

Professor Cristian Popescu, Chair

The work of Iwasawa, beginning with a seminal paper in 1958 [7], provided a fruitful method of studying the structure of ideal class groups and other algebraic objects by viewing them inside of a p-adic tower of fields and then considering the corresponding object at the top of the tower as a module over a topological ring now called an Iwasawa algebra. One way to analyze the structure of these modules over the appropriate ring is to determine the Fitting ideals of the module; however, in the literature thus far only the initial Fitting ideal has been the object of close study. In this dissertation, we prove a conjecture by Kurihara about the higher Fitting ideals of Iwasawa modules of certain abelian number fields. This result shows that they are in essence generated by the special values of L-functions arising from a family of extensions of the number field.

Chapter 1

Introduction

The use of Fitting ideals in Iwasawa theory goes back to Mazur and Wiles' proof of the main conjecture in 1984, where they show that the initial Fitting ideal of the classical Iwasawa module associated to an abelian extension of $\mathbb{Q}$ is generated by a p-adic L-function. Most results that involve Fitting ideals of a particular module (such as an ideal class group, cohomology group, Selmer group, etc.) have had this main conjecture flavor, involving the initial Fitting ideal Fitt^0. For example, as $\mathrm{Fitt}^0_R(M)$ lies inside the annihilator $\mathrm{Ann}_R(M)$, giving generators of this Fitting ideal refines many conjectures that deal with the annihilation of a module, such as the Brumer-Stark conjecture or the Coates-Sinnott conjecture. However, studying the higher Fitting ideals can also be fruitful, as knowing all the Fitting ideals of a module can more completely determine the structure of the module, or can provide a method of attack for other central conjectures in number theory, such as the Iwasawa-Leopolt and Kummer-Vandiver conjectures.

This dissertation is concerned with a conjecture of Masato Kurihara formulated in 2003 in [8]. For a CM abelian field extension $\mathcal{F}$ over a totally real number field k, Kurihara studied the Fitting ideals of the ideal class group of $\mathcal{F}$, $Cl_{\mathcal{F}}$, over the ring $\mathbb{Z}[\mathrm{Gal}(\mathcal{F}/k)]$. This was done by studying the Fitting ideals of the p-primary part, $(Cl_{\mathcal{F}} \otimes \mathbb{Z}_p)$, of the ideal class group $Cl_{\mathcal{F}}$, for every prime p. As the prime 2 is problematic, he was primarily concerned with the case where p is an odd prime (and we will be as well). Moreover, as $\mathcal{F}$ is CM, $Cl_{\mathcal{F}} \otimes \mathbb{Z}_p$ has a decomposition as $Cl_{\mathcal{F}} \otimes \mathbb{Z}_p = (Cl_{\mathcal{F}} \otimes \mathbb{Z}_p)^+ \oplus (Cl_{\mathcal{F}} \otimes \mathbb{Z}_p)^-$, and Kurihara directed his attention to the minus part of this decomposition.

The strategy is to consider the cyclotomic $\mathbb{Z}_p$-extension of $\mathcal{F}$, denoted $\mathcal{F}_\infty$, and make use of the Iwasawa main conjecture for $\mathcal{F}_\infty$. Let $R = \mathbb{Z}_p[[\mathrm{Gal}(\mathcal{F}_\infty/k]]^-$, and consider the R-module $M = X^-_{F_\infty}$, which is the projective limit of the p-primary components of the ideal class groups, $(Cl_{\mathcal{F}_n} \otimes \mathbb{Z}_p)^-$, associated to the n-th level, $\mathcal{F}_n$ of the cyclotomic extension. In [8], Kurihara studies the Fitting ideals of the above module over the ring R for a special class of extensions $\mathcal{F}/k$, and determines $\mathrm{Fitt}^0_R(M)$ to essentially be generated by the special values of equivariant L-functions for abelian extensions of k contained in $\mathcal{F}$. In addition, for $k = \mathbb{Q}$, he also studies the higher Fitting ideals of M, and gives a conjecture as to what generates these ideals. While he only proves his conjecture for Fitt^1, he conjectures that the higher Fitting ideals, modulo a large power of p, are generated by the previous p-adic L-functions that generate $\mathrm{Fitt}^0_R(M)$, as well as additional elements that arise from equivariant p-adic L-functions of special abelian extensions of $\mathcal{F}$.

It is this conjecture that we turn our attention towards. The structure of the dissertation is the following. In chapter 2, we give the preliminary information needed for the rest of the paper; we briefly describe Fitting ideals and L-functions, and give a precise formulation of Kurihara's conjecture. In chapter 3, we discuss a Gross-type p-adic refinement of the Rubin-Stark conjecture, which is needed for chapter 4, and talk about how this conjecture can help us attack Kurihara's conjecture. Chapter 4 contains the main results of the paper: the second section gives the proof of Kurihara's conjecture, and the first section proves a technical theorem that is needed for the main theorem, but is of some interest in its own right. (It generalizes Theorem 3.1 in [14], suggesting that it can be used to relate the Gross-type conjecture to Euler systems, which we will do in a subsequent paper).

Chapter 2

Algebraic Preliminaries

2.1 Fitting Ideals

Let R be a commutative ring and M be a finitely generated R - module, with generators $v_1, \ldots, v_n$. We will also assume that M is finitely presented; i.e, there are finitely many relations among the above generators that generate all relations. Then we can write the following right exact sequence of R-modules:

$$R^m \xrightarrow{\phi} R^n \xrightarrow{f} M \to 0,$$

Let A be an $n \times m$ matrix associated to ϕ; the columns of the matrix A are the generating relations mentioned above.

Definition 2.1. *The i-th Fitting ideal of M, denoted $\mathrm{Fitt}_R^i(M)$, is the ideal generated by the determinants of all $(n-i) \times (n-i)$ minors of A.*

The cofactor expansion for determinants shows that the Fitting ideals form an ascending chain $\mathrm{Fitt}_R^0(M) \subseteq \mathrm{Fitt}_R^1(M) \ldots \subseteq \mathrm{Fitt}_R^n(M) = R$. Also, since the columns of A are relations for the v_i's, we have that $A^T \vec{v} = 0$. For any $n \times n$ minor

B of A^T, multiplying by its associated adjugate matrix gives $\det(B)\vec{v} = 0$; therefore, $\mathrm{Fitt}_R^0(M) \subseteq \mathrm{Ann}_R(M)$.

If M is not finitely presented, we can still define the Fitting ideals of M. In this case, we don't have an exact sequence as above. Instead, we directly form a matrix A, where the columns of A are relations for the generators of M. $\mathrm{Fitt}_R^i(M)$ is then defined to be generated by all $(n-i) \times (n-i)$ minors of A, for all matrices A whose columns are relations for the generators of M. However, since the modules that we consider in this dissertation are finitely presented, the results we state here will only be done for finitely presented M.

The definition above suggests that the Fitting ideals are dependent not only on M, but on the chosen presentation and choice of matrix A. The following proposition, in addition to recording a property of Fitting ideals that we will use later, will show that the Fitting ideals are only dependent on the module M (see [11]).

Proposition 2.2. *1. For all i, $\mathrm{Fitt}_R^i(M)$ is independent of the choice of presentation and matrix A.*

2. If M and N are two finitely generated, finitely presented R-modules such that $M \twoheadrightarrow N$, then for all i, $\mathrm{Fitt}_R^i(M) \subseteq \mathrm{Fitt}_R^i(N)$.

Proof. 2) It is easier here to use the general method of defining Fitting ideals outlined above. Denote the surjection of M onto N by ρ. Let $v_1, \ldots, v_n$ be generators for M; then $w_1, \ldots, w_n$ generate N, where $w_i = \rho(v_i)$. Then any relation of $v_1, \ldots, v_n$ is a relation of $w_1, \ldots, w_n$. Thus, any matrix A that would be appear in the definition of the Fitting ideals for M would also appear in that for N. Thus, $\mathrm{Fitt}_R^i(M) \subseteq \mathrm{Fitt}_R^i(N)$.

1) Consider two different sets of generators of M, $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$ with two different choices of generating relations; we will denote how we view M

with respect to these two choices by M_v and M_w. Then we have the obvious isomorphism i from M_v to M_w. Applying (1) to i and i^{-1} gives the result.

□

If R is a PID, the structure of all the Fitting ideals of a module over R can be used to determine the structure of the module itself. The structure theory of finitely generated modules over a PID yields that

$$M \cong R^n \oplus R/(a_1) \oplus \ldots \oplus R/(a_k)$$

with $(a_1) \subset (a_2) \subset \ldots \subset (a_k)$.

Calculating the Fitting ideals for M gives $\mathrm{Fitt}^i_R(M) = 0$ for $0 \leq i \leq n-1$ and $\mathrm{Fitt}^i_R(M) = (a_{i-n+1} \cdot \ldots \cdot a_k)$ for $n \leq i \leq n+k$, with the empty product being the whole ring R. Vice versa, if R is a PID and we know the Fitting ideals of an R-module M to have the form above, then one can easily determine that M has the structure above.

For more complicated rings R, knowing the Fitting ideals is not enough to completely determine the module. For the rings that we will consider, knowing the Fitting ideals determines the module up to quasi-isomorphism (a homomorphism with finite kernel and cokernel); however, the converse is not true.

For more information on Fitting ideals, see [11].

2.2 Augmentation Ideals

Consider a tower of field extensions $k \subseteq \mathcal{F} \subseteq \mathcal{L}$, with $\mathcal{L}/k$ a finite abelian extension. (A note: using projective limits, we can define augmentation ideals for infinite extensions as well; however, for purposes of this paper we only need the finite case). Then each field extension is Galois; we will let $\mathrm{Gal}(\mathcal{L}/k) = \mathcal{G}$, $\mathrm{Gal}(\mathcal{F}/k) = \Delta$, and $\mathrm{Gal}(\mathcal{L}/\mathcal{F}) = G$. Let R be a commutative ring.

Definition 2.3.

- *The augmentation ideal of the group ring $R[G]$, denoted by $I(G)$, is the kernel of the homomorphism aug : $R[G] \longrightarrow R$ which fixes every element of R and sends every element of G to 1.*
- *The G-relative augmentation ideal of the group ring $R[\mathcal{G}]$, denoted by I_G, is the kernel of the R-algebra homomorphism $\pi : R[\mathcal{G}] \longrightarrow R[\Delta]$ which is induced by Galois restriction from $\mathcal{G}$ to Δ.*

It is clear that $I(G)$ is generated as an $R[G]$-module by elements of the form $\sigma - 1$ for $\sigma \in G$; it is easy to see that I_G is also generated by elements of the form $\sigma - 1$ for $\sigma \in G$, but as an $R[\mathcal{G}]$-module.

We end this section with the following lemma, which occurs as a part of Lemma 5.2.3 in [13]:

Lemma 2.4. *Let r be a positive integer. Then we have a $R[\Delta]$-module isomorphism*

$$t : I(G)^r/I(G)^{r+1} \otimes_R R[\Delta] \cong I_G^r/I_G^{r+1},$$

given by $\hat{\gamma} \otimes \delta = \widehat{\tilde{\delta}\gamma}$.

2.3 L-functions

We first start by reviewing the definition of Artin L-functions. We follow the setup by Neukirch in [10]; however, we will restrict ourselves to the special case where the Galois group is abelian and the representation is one-dimensional. Let k be an algebraic number field, and F a finite abelian extension of k, with Galois group $\mathrm{Gal}(F/k) = G$. Let $\chi : G \to \mathbb{C}^\times$ be a group homomorphism, then we say that χ is a character of G. Recall that χ induces an action of G on V via $\sigma \cdot v = \chi(\sigma)v$, for $\sigma \in G$ and $v \in V$. Fix a prime ideal $\mathfrak{p}$ of k lying over a rational prime p, and let $\mathfrak{P}$ be a prime ideal of F lying over $\mathfrak{p}$. For a prime $\mathfrak{p}$ in k, we have its associated residue field $\kappa(\mathfrak{p})$; recall that $\kappa(\mathfrak{p})$ is $O_k/\mathfrak{p}$, the ring of integers of k modded out by $\mathfrak{p}$. If F is a Galois extension of k with prime ideal $\mathfrak{P}$ above $\mathfrak{p}$, then $\kappa(\mathfrak{P})$ is a Galois extension of $\kappa(\mathfrak{p})$.

In $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$, the automorphism $x \to x^{N\mathfrak{p}}$ generates the Galois group ($N\mathfrak{p}$ is $|O_k/\mathfrak{p}|$). This group is then canonically isomorphic to the quotient of the decomposition group $G_{\mathfrak{P}}$ by the inertia group $I_{\mathfrak{P}}$; the image of the above automorphism in $G_{\mathfrak{P}}/I_{\mathfrak{P}}$ is called the Frobenius automorphism associated to $\mathfrak{P}$, which we will denote $\Phi_{\mathfrak{P}}$.

Note that given two different primes that lie above $\mathfrak{p}$, their associated Frobenius automorphisms are Galois conjugates. We denote the conjugacy class of Frobenius automorphisms for primes lying above $\mathfrak{p}$ by $\mathrm{Frob}_{\mathfrak{p}}$; this conjugacy class is dependent only on $\mathfrak{p}$.

We now define the Artin L-function for $s \in \mathbb{C}$, denoted $L(\chi, s)$, to be

$$L(\chi, s) = \prod_{\mathfrak{p}} (1 - (\chi(\mathrm{Frob}_{\mathfrak{p}}) N(\mathfrak{p})^{-s})^{-1},$$

where the product runs over all primes of k such that $\chi|_{I_{\mathfrak{p}}}$ is trivial. If χ is not the trivial character, then $L(\chi, s)$ is uniformly and absolutely convergent on compact subsets of the half-plane $\mathrm{Re}(s) > 1$. This can then be uniquely extended to a holomorphic function on $\mathbb{C}$. If χ is the trivial character, then $L(\chi, s)$ can be uniquely extended to a function that is holomorphic on $\mathbb{C} \setminus \{1\}$, and has a simple pole at $s = 1$. We will refer to any particular term of this product as the Euler factor associated to $\mathfrak{p}$.

We now have many L-functions for any particular Galois field extension (one for each character χ of G), but we would like just one function associated to a particular field extension that still carries the same information the L-functions do. This is the equivariant L-function, and we define it as follows.

Let e_χ be the idempotent

$$e_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1},$$

which is an element of $\mathbb{C}[G]$. Let S be a finite set of primes in k, containing all of the ramified primes and all of the infinite primes. The S - modified Artin L-function, denoted $L_S(\chi, s)$, is simply

$$L_S(\chi, s) = \prod_{\mathfrak{p} \notin S} (1 - \chi(\mathrm{Frob}_\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1}.$$

With this in hand, we now have:

Definition 2.5. *The S-imprimitive G-equivariant L-function, which we denote $\theta_{F/k,S}(s)$, is a function from $\mathbb{C}$ to $\mathbb{C}[G]$, holomorphic outside of $s = 1$ with a simple pole at 1, given by*

$$\theta_{F/k,S}(s) := \sum_{\chi \in \hat{G}} L_S(\chi, s) e_\chi^{-1}.$$

Our focus in this paper will be the special value at $s = 0$, which is the value of the first non-vanishing derivative at 0. Throughout this paper, we will write $\theta_{F/k,S}$ for $\theta_{F/k,S}(0)$. From the definition above, we know that $\theta_{F/k,S} \in \mathbb{C}[G]$; however, a theorem of Klingen and Siegel (see [15]) tells us that, in fact, $\theta_{F/k,S} \in \mathbb{Q}[G]$.

We need one more tool in order to discuss the results in Kurihara's paper. Fix an odd rational prime p. Let F_∞ be the cyclotomic $\mathbb{Z}_p$-extension of F (the extension of F with Galois group over F isomorphic to $\mathbb{Z}_p$, obtained by adjoining all p-th power roots of unity to F, then taking the appropriate intermediate field.)

Write F_n for the intermediate field such that $[F_n : F] = p^n$, and $F = F_0$. For each of these finite levels, we have the equivariant L-value $\theta_{F_n,S}$. For any field extension L of k, we let S_L be the set finite primes in k that are ramified in L.

For any pair of non-negative integers m and n, $n < m$, let $r_{m,n} : \mathbb{Q}[\mathrm{Gal}(F_m/k)] \to \mathbb{Q}[\mathrm{Gal}(F_n/k)]$ be the natural map coming from viewing $\mathrm{Gal}(F_n/k)$ as a quotient of $\mathrm{Gal}(F_m/k)$. Then a result of Tate in [16] yields

$$r_{m,n}(\theta_{F_m,S}) = (\prod_{v \in S_{F_m} \setminus S_{F_n}} (1 - (\mathrm{Frob}_v^{-1}))\theta_{F_n,S}.$$

Since there are only finitely many ramified primes in F_∞, there is some positive integer N for which $S_{F_m} = S_{F_N}$ for all $m > N$. So for any $m, n > N$,

$$r_{m,n}(\theta_{F_m,S}) = \theta_{F_n,S}.$$

These maps form a projective system. Let T be a another finite set of primes in $\mathbb{Q}$ that is disjoint from S and such that there are no roots of unity in F congruent to 1 modulo every prime in T. Define the (S,T) - modified G-equivariant L-function, denoted $\theta_{F/k,S,T}(s)$ to be

$$\theta_{F/k,S,T}(s) = (\prod_{v \in T}(1 - \mathrm{Frob}_v^{-1} \cdot (Nv)^{1-s}))\theta_{F/k,S}(s).$$

The special value of this function at $s = 0$ has the same properties under the $r_{m,n}$ maps as that of $\theta_{F/k,S}$. Deligne and Ribet proved in [3] that there exists an element of $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$, which we will denote by $\theta_{F_\infty/k,S,T}$ that behaves as the projective limit. In particular, for every positive integer n, there exists a map

$$r_n : \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]] \to \mathbb{Z}_p[\mathrm{Gal}(F_n/k)]$$

such that $r_n(\theta_{F_\infty/k,S,T}) = \theta_{F_n/k,S,T}$. We will call this the equivariant p-adic L-function. However, for our purposes of proving Kurihara's conjecture, we do not want to consider the set T; we will discuss how to eliminate the presence of T in section 3.1.1.

2.4 Kurihara's paper

As the main result of this dissertation is proving a conjecture of Kurihara's, we will use this section to state the conjecture and to set notation which will be used in Chapters 3 and 4.

Fix an odd prime number p. We will let the base field $k = \mathbb{Q}$, and $\mathcal{F}$ is a cyclic CM extension of $\mathbb{Q}$, with $\Delta = \mathrm{Gal}(\mathcal{F}/\mathbb{Q})$ of order coprime to p. Since $\mathcal{F}$ is a CM field, Δ has a complex conjugation element, which we will denote $\mathfrak{j}$. For an odd character χ of Δ (meaning that $\chi(\mathfrak{j}) = -1$) that is injective on Δ, let $\Lambda^{\chi}_{\mathcal{F}_\infty} = \mathbb{Z}_p[\chi][[\Gamma]]$, where $\Gamma = \mathrm{Gal}(\mathcal{F}_\infty/\mathcal{F})$. For each finite level $\mathcal{F}_m$, we denote by $A_{\mathcal{F}_m}$ the p-primary component of the ideal class group of $\mathcal{F}_m$. $X_{\mathcal{F}_\infty}$ is then defined to be the projective limit of the $A_{\mathcal{F}_m}$'s with respect to the norm maps.

Also, for χ's as above which are different from the Teichmuller character, we define ω, $\theta^{\chi}_{\mathcal{F}_n/k,S} \coloneqq \chi(\theta_{\mathcal{F}_n/k,S}(0))$. This is an element of $\mathbb{Z}_p[\chi][\mathrm{Gal}(\mathcal{F}_n/\mathcal{F})]$, and therefore $\theta^{\chi}_{\mathcal{F}_\infty/k,S}$ is in $\Lambda^{\chi}_{\mathcal{F}_\infty}$.

The complex conjugation elements $\mathfrak{j}$ acts on any $\mathbb{Z}_p[\Delta]$ module M. This gives a decomposition of M into two parts, denoted M^+ and M^-, which are respectively the eigenspaces for $\mathfrak{j}$ corresponding to eigenvalues 1 and -1. In particular, each $A_{\mathcal{F}_m}$ has such a decomposition, and therefore $X_{\mathcal{F}_\infty}$ does too.

Kurihara's conjecture is concerned with determining generators of the Fitting ideals of $X^{\chi}_{\mathcal{F}_\infty}$, viewed as a $\Lambda^{\chi}_{\mathcal{F}_\infty}$ - module. We begin by stating the main conjecture of Iwasawa theory, proven by Mazur and Wiles in [9], that relates the p-adic L-function to the initial Fitting ideal.

Theorem 2.6. $\mathrm{Fitt}^0_{\Lambda_{\mathcal{F}_\infty}}(X^-_{\mathcal{F}_\infty}) = \langle \theta_{\mathcal{F}_\infty} \rangle$.

We now prove the following algebraic result, which we will use to show that some elements of $\Lambda^\chi_{\mathcal{F}_\infty}$ are in the appropriate Fitting ideals.

Proposition 2.7. *Let R be a commutative ring, G a finite abelian group, M a finitely generated, finitely presented R-module of rank n on which G acts trivially, and $F_i = \mathrm{Fitt}^i_R(M)$ for all $0 \leq i \leq n$. Define $s : R \longrightarrow R[G]$ via $s(r) = r \cdot 1_G$. Then*

$$\mathrm{Fitt}^0_{R[G]}(M) \subseteq s(F_0) + s(F_1)I_G + s(F_2)I_G^2 + \ldots + s(F_{n-1})I_G^{n-1} + I_G^n.$$

A remark on the notation of the proposition: to match the notation in Definition 2.3, we should technically be using $I(G)$ instead of I_G. However, for the application we have in mind for the proposition, R will itself be a group ring, and then I_G will actually function as a relative augmentation ideal.

In what follows (as well as in Chapter 4), for a positive integer n we will denote by $[n]$ the set $\{1, \ldots, n\}$. For a subset $Z \subseteq [n]$, we will denote its complement by Z^c.

Proof. First, we note that the map s forms a splitting for the exact sequence

$$1 \to I_G \to R[G] \xrightarrow{\pi} R \to 1,$$

and so $R[G] = s(R) \oplus I_G$.

Consider a free presentation of M as an R-module, given by

$$0 \to C \xrightarrow{V} R^n \xrightarrow{\alpha} M \to 0.$$

From this, we get the following presentation for M as an $R[G]$ - module:

$$R[G]^n \xrightarrow{W} R[G]^n \xrightarrow{\beta} M \to 0,$$

where β is the composition of α with the map from $R[G]^n$ to R^n that applies π to each coordinate.

Thus, by definition, $Fitt^0_{R[G]}(M)$ is generated by the determinant of the matrix corresponding to W, which by abuse of notation we will also refer to by W. We view W as the map that sends $R[G]^n$ to the kernel of β; since the kernel of α is C and G acts trivially on M, the kernel is $s(C) + \bigoplus_{i=1}^{n} I_G$. We conclude that the matrix of W has entries of the form $s(t_{ij}) + \gamma_{ij}$, for $t_{ij} \in C$, $\gamma_{ij} \in I_G$, and $1 \leq i, j \leq n$.

So we compute the determinant of W. By definition of the determinant, this is

$$\det(W) = \sum_{\tau \in S_n} \prod_{i=1}^{n} (-1)^{(i+\tau(i))} (s(t_{i,\tau(i)}) + \gamma_{i,\tau(i)}).$$

To expand the product, let $Z \subseteq [n]$ be the set of indices j for which we pick $\gamma_{j,\tau j}$. Then we have

$$\det(W) = \sum_{Z \subseteq [n]} \sum_{\tau \in S_n} \prod_{i \notin Z} (-1)^{(i+\tau(i))} s(t_{i,\tau(i)}) \prod_{j \in Z} (-1)^{(j+\tau(j))} \gamma_{j,\tau(j)}.$$

We now group the τ's by where they send the set Z. Doing so gives:

$$\sum_{Z \subseteq [n]} \sum_{g: Z \hookrightarrow [n]} \prod_{j \in Z} (-1)^{(j+g(j))} \gamma_{j,g(j)} \sum_{\substack{\tau \in S_n \\ \tau|_Z = g}} \prod_{i \notin Z} (-1)^{(i+\tau(i))} s(t_{i,\tau(i)}).$$

Denote by $V_{Z,g}$ the $n-k \times n-k$ minor of V, where $k = |Z|$ and where you delete the rows corresponding to the elements of Z, and the columns corresponding to the elements of $g(Z)$. Then we have

$$\sum_{Z\subseteq[n]}\sum_{g:Z\hookrightarrow[n]}\prod_{j\in Z}(-1)^{(j+g(j))}\gamma_{j,g(j)}\sum_{\substack{\tau\in S_n\\ \tau|_Z=g}} s(\det(V_{Z,g})).$$

But then $s(\det(V_{Z,g}))$ is an element of $s(F_k)$, and $\prod_{j\in Z}(-1)^{(j+g(j))}\gamma_{j,g(j)}$ is an element of I_G^k. So for any given Z, the corresponding summand is an element of $s(F_k)I_G^k$, which completes the proof. □

We apply this proposition in the special case where $R = \Lambda_{\mathcal{F}_\infty}$ and $G = \prod_{i=1}^{r}\mathbb{Z}/p^N$, and $M = (X^-_{\mathcal{L}_\infty})_G$, where $\mathcal{L}$ is an abelian extension of $\mathcal{F}$, linearly disjoint from $\mathcal{F}_\infty$, with no nontrivial subextensions that are unramified everywhere, such that $G = \mathrm{Gal}(\mathcal{L}/\mathcal{F})$. Then $R[G] = \Lambda_{\mathcal{L}_\infty}$. By Theorem 2.6, $\theta_{\mathcal{L}_\infty} \in \mathrm{Fitt}^0_{R[G]}(M)$, and so the proposition gives us that

$$\theta_{\mathcal{L}_\infty} \in s(F_0) + s(F_1)I_G + s(F_2)I_G^2 + \ldots + s(F_{n-1})I_G^{n-1} + I_G^n.$$

First, assume $r = 1$, and so G is cyclic, and let $x \in R[G]$. Then $\alpha_1 = x - s(\pi(x)) \in I_G$, and we have $x = x_1 + \alpha_1$, where $x_1 = s(\pi(x)) \in R$. Since G is cyclic, fix a generator σ of G. Then we have (non-canonical) isomorphisms

$$\phi_k : G \to I_G^k/I_G^{k+1},$$

given by

$$\sigma^j \to j(\sigma-1)^k.$$

In this manner, we can write $\alpha_i = x_{i+1}(\sigma-1)^i + \alpha_{i+1}$, where $\alpha_{i+1} \in I_G^{i+1}$ and $x_i \in R$. Since G has order p^N,

$$p^N(\sigma-1)^i = 0 \text{ in } I_G^k/I_G^{k+1},\ \forall\, i.$$

Therefore, each x_i, for $i \geq 2$, is well-defined in R/p^N.

For general G as above, view G as $G_1 \times \ldots \times G_r$, where each G_i is cyclic of order p^N with generator σ_i. We then set $R' = R[G_1 \times \ldots \times G_{r-1}]$. Applying the above initial case to $R'[G_r]$ yields

$$x = x_1 + x_2(\sigma_r - 1) + x_3(\sigma_r - 1)^2 + \ldots.$$

We then repeat this procedure for each x_i, with respect to G_{r-1}. Continuing by induction gives

$$x = \sum_{\vec{i}} x_{\vec{i}}(\sigma_1 - 1)^{i_1} \cdot \ldots \cdot (\sigma_r - 1)^{i_r},$$

where $\vec{i} = (i_1, \ldots, i_r) \in \mathbb{Z}^r$, and the $x_{\vec{i}}$'s are elements of R.

We do the above procedure for $\theta_{\mathcal{L}_\infty}$. The $x_{\vec{i}}$'s that we obtain we will denote $\delta_{i_1,\ldots,i_r}(\theta_{\mathcal{L}_\infty})$, where $i_1 + \ldots + i_r = i$. The above proposition gives us that, modulo p^N,

$$\delta_{1,1,\ldots,1}(\theta_{\mathcal{L}_\infty}) \in \mathrm{Fitt}^i_R(M_G).$$

Finally, since $\mathcal{L}$ has no unramified subextensions, the norm map yields a surjection from $(X^-_{\mathcal{L}_\infty})_G/p^N$ to $X^-_{\mathcal{F}_\infty}/p^N$; the surjectivity property of Fitting ideals gives us the following corollary:

Corollary 2.8. $\delta_{i_1,\ldots,i_r}(\theta_{\mathcal{L}_\infty}) \in \mathrm{Fitt}^i_{\Lambda^\chi_{\mathcal{F}_\infty}/p^N}(X^-_{\mathcal{F}_\infty}/p^N)$*, for* $i_1 + \ldots + i_r = i$.

Now we have all the tools necessary to state Kurihara's conjecture:

Conjecture 2.9. *For any* $i > 0$, $\mathrm{Fitt}^i_{\Lambda^\chi_{\mathcal{F}_\infty}/p^N}(X^\chi_{\mathcal{F}_\infty}/p^N)$ *is equal to the ideal* $\mathfrak{T}_i$ *generated by* $\theta^\chi_{\mathcal{F}_\infty/\mathbb{Q}}$ *and the* $\delta_{i_1,\ldots,i_r}(\theta_{\mathcal{L}_\infty})$*'s, where*

- $\mathcal{L}$ *ranges over all abelian extensions of* $\mathbb{Q}$ *such that* $\mathcal{L} \cap \mathcal{F}_\infty = \mathcal{F}$, $\mathrm{Gal}(\mathcal{L}/\mathbb{Q}) = \mathrm{Gal}(\mathcal{F}/\mathbb{Q}) \times \mathrm{Gal}(\mathcal{L}/\mathcal{F})$*, and* $\mathrm{Gal}(\mathcal{L}/\mathcal{F}) \cong \mathbb{Z}/p^{n_1} \times \ldots \times \mathbb{Z}/p^{n_r}$*, with each* $n_i \geq N$.

- $(i_1, \ldots, i_r)$ *ranges over all non-negative integers with* $i_1 + \ldots + i_r \leq i$.

Proposition 2.7 gives us that $\mathfrak{T}_i \subseteq \mathrm{Fitt}^i_{\Lambda^\chi_{\mathcal{F}_\infty}/p^N}(X^\chi_{\mathcal{F}_\infty}/p^N)$. The other inclusion is more difficult. In chapter 8 of [8], Kurihara proves his conjecture for the case $i = 1$. The basic method is to descend to a large enough finite level, concoct a useful free presentation for $A^\chi_{\mathcal{F}_m}$, then use the Euler system argument to prove the inclusion. For the general case that we prove later, we will appeal to a Gross-type conjecture and a Chebotarev density result to generalize the second step of Kurihara's proof. We will still need the presentation $A^\chi_{\mathcal{F}_m}$ (and, in fact, it is the lack of such a presentation for other Iwasawa modules that presents an obstacle in adapting our proof to those modules), so we will record the properties of this presentation as a lemma.

Lemma 2.10. *Assume that the* μ*-invariant of* $\mathcal{F}_\infty$ *is 0, and that Leopoldt's conjecture holds for the base field* k*, and let* χ *be an odd character of* Δ *such that the order of* χ *is coprime to* p*, and* $\chi|_{\Delta_p} \neq 1_{\Delta_p}$*, and* $\chi \neq \omega$*. Then we have a presentation*

$$0 \to (\Lambda_m)^n \xrightarrow{f} (\Lambda_m)^n \to A^\chi_{\mathcal{F}_n} \to 0,$$

such that the determinant of the matrix for f *is* $\theta^\chi_{\mathcal{F}_m}$.

A note: Leopoldt's conjecture does hold for abelian extensions of $\mathbb{Q}$, which is the situation we are in for this dissertation. The hypothesis $\mu = 0$ holds for abelian extensions of $\mathbb{Q}$ as well. However, for arbitrary base fields, these assumptions are needed.

Proof. The assumption that the μ-invariant of $\mathcal{F}_\infty$ is 0 gives us that $X_{\mathcal{F}_\infty}$ is finitely generated as a $\mathbb{Z}_p$ - module and that the $\mathrm{pd}_{\Lambda_\chi} X^\chi_{\mathcal{F}_\infty} = 1$. Let $w_1, \ldots, w_n$ be generators of $X^\chi_{\mathcal{F}_\infty}$. Then we have an exact sequence

$$0 \to (\Lambda_\chi)^n \xrightarrow{f} (\Lambda_\chi)^n \xrightarrow{g} X^\chi_{\mathcal{F}_\infty} \to 0.$$

Let $\mathcal{A}$ be the matrix of f, and choose bases so that $\det(\mathcal{A}) = \theta^{\chi}_{\mathcal{F}_\infty}$, which is possible due to Theorem 2.6. We fix a finite level $m > 0$, sufficiently large, and let $\Gamma_m = \mathrm{Gal}(\mathcal{F}_\infty/\mathcal{F}_m)$. We then take Γ_m-coinvariants of the above equation. By the snake lemma, we get

$$(X^{\chi}_{\mathcal{F}_\infty})^{\Gamma_m} \to (\Lambda_m)^n \xrightarrow{f} (\Lambda_m)^n \to (X^{\chi}_{\mathcal{F}_\infty})_{\Gamma_m} \to 0,$$

where $\Lambda_m = \mathbb{Z}_p[\chi][\mathrm{Gal}(\mathcal{F}_m/\mathcal{F})]$.

However, since $\chi(p) \neq 1$, a well-known result in Iwasawa theory gives us that $(X^{\chi}_{\mathcal{F}_\infty})_{\Gamma_m}$ is isomorphic to $A^{\chi}_{\mathcal{F}_m}$. Since this is a finite group, the above exact sequence implies that $(X^{\chi}_{\mathcal{F}_\infty})^{\Gamma_m}$ is finite. But $X_{\mathcal{F}_\infty}$ contains no finite $\Lambda_{\mathcal{F}_\infty}$ submodules (see Proposition 13.28, [17]), and so $(X^{\chi}_{\mathcal{F}_\infty})^{\Gamma_m} = 0$. Thus, we get the free presentation

$$0 \to (\Lambda_m)^n \xrightarrow{f} (\Lambda_m)^n \xrightarrow{g} A^{\chi}_{\mathcal{F}_m} \to 0$$

at the finite level.

By definition of the ideal class group, at each finite level m we have the exact sequence

$$(\mathcal{F}_m^{\times} \otimes \mathbb{Z}_p)^{\chi} \xrightarrow{div} (\mathrm{Div}_{\mathcal{F}_m} \otimes \mathbb{Z}_p)^{\chi} \to A^{\chi}_{\mathcal{F}_m} \to 0.$$

We project the generators $w_1, \ldots, w_n$ down to generators for $A^{\chi}_{\mathcal{F}_m}$, then use the Chebotarev density theorem to find primes $v_1, \ldots, v_n$ such that their images in $A^{\chi}_{\mathcal{F}_m}$ correspond to the classes of the projected generator, and that are split all the way down to $\mathbb{Q}$ (so that $v_1, \ldots, v_n$ generate a free Λ_m-module of rank n in $(\mathrm{Div}_{\mathcal{F}_m} \otimes \mathbb{Z}_p)^{\chi}$). Let M be this module. Then $M \cong \Lambda_m^n$, and the map $M \to A^{\chi}_{\mathcal{F}_m}$ is induced by the map g. Our free presentation for $A^{\chi}_{\mathcal{F}_m}$ above gives that the kernel of $M \to A^{\chi}_{\mathcal{F}_m}$, which we will denote M', is also a free Λ_m module of rank n.

Thus, we have the free presentation

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} A^{\chi}_{\mathcal{F}_m} \to 0,$$

where the matrix for f here has determinant $\theta^{\chi}_{\mathcal{F}_m}$. □

Let $\mathcal{D} = \{x \in (\mathcal{F}_m^{\times} \otimes \mathbb{Z}_p)^{\chi} \mid \mathrm{div}(x) \in M\}$. Then $\mathrm{div}(\mathcal{D}) = M'$. We will denote by $f_1, \ldots, f_n$ the elements of $\mathcal{F}^{\times}$ that map to the basis elements of M'. By definition, these f_i are linearly independent in $\mathcal{D}$. They are also linearly independent in $\mathcal{F}_m^{\times}/(\mathcal{F}_m^{\times})^{p^N}$, a fact which we will need later, and so we will prove it now.

Lemma 2.11. *The classes of $f_1, \ldots, f_n$ are Λ_m/p^m - linearly independent inside $\mathcal{F}_m^{\times}/(\mathcal{F}_m^{\times})^{p^N}$*

Proof. Suppose for contradiction that we have a dependence relation. Then there exist elements $\alpha_1, \ldots, \alpha_n \in \Lambda_m$ and $x \in \mathcal{F}_m^{\times}$ such that $f_1^{\alpha_1} \ldots f_n^{\alpha_n} = x^{p^N}$. Applying div to both sides gives that $p^N \mathrm{div}(x) \in M'$, and so is in M, since $M' \subseteq M$. Thus, there exist $\beta_1, \ldots, \beta_n \in \Lambda_m$ such that

$$p^N \mathrm{div}(x) = \beta_1 v_1 + \ldots + \beta_n v_n.$$

However, since the v_i's freely generate M, this implies that $\mathrm{div}(x) \in M$ and p^N divides β_i for all i. Thus, $x \in \mathcal{K}$, and so $x = f_1^{\gamma_1} \ldots f_n^{\gamma_n}$. From the linear independence of the f_i's in $\mathcal{K}$, we conclude that p^N divides α_i for all i, and so each α_i is 0 in Λ_m/p^N. □

Another consequence of $\chi(p) \neq 1$ is to guarantee that $\theta^{\chi}_{\mathcal{F}_m}$ is not a zero-divisor, which will be needed in Chapter 4. This is an easy consequence of the functional equation for $\theta_{\mathcal{F}_m}$, see [16].

Chapter 3

The Gross-type Conjecture

3.1 Statement of the Conjecture

In Kurihara's proof of his conjecture when $i = 1$, he makes use of the Kolyvagin's Euler system of Gauss sums (treated by Rubin in [14]).

It turns out that for $i > 1$, the Euler system argument breaks down. What is needed can be thought of as following from two conjectures: one of Rubin and Stark, and one of Gross. We will discuss the relevant conjectures here, following the treatment by Popescu in [13]. Later, we will discuss how to use the Gross-type conjecture to obtain the necessary results to prove Kurihara's conjecture.

Throughout this section, we will let k be a global field, and F a finite abelian extension of k with Galois group G. Let $\{\ell_1, \ldots, \ell_r\}$ be a set of r primes in k that split completely in F, and let $S_0 = \{\lambda_1, \ldots, \lambda_r\}$ be a set of primes in F with λ_i lying over ℓ_i for all i. We will take S to be a finite set of primes in k of size $\geq r+1$ that contains S_0; contains S_∞, the set of infinite primes; and contains $S_{\mathrm{ram}}(F/k)$, the set of all primes that ramify in F. Furthermore, we will take T to be another finite set of primes in k that is disjoint from S and such that there are no roots of unity in F congruent to 1 modulo every prime in T. (If $\mathrm{char}(k) = 0$, this is satisfied if T contains two primes whose residue fields have different characteristics, or one prime whose residue field has size larger than the number of roots of unity in K. If $\mathrm{char}(k) > 0$, then this is satisfied as long as T is non-empty). We will also let S_F and T_F be the set of primes in F that lie above S and T, respectively.

We denote by U_S to be the elements of $F^\times$ that are units at all the primes outside of S; i.e., $u \in U_S$ means that $u \in O_{F_v}^\times$ for all $v \notin S_F$. $U_{S,T}$ is the subset of U_S whose elements are congruent to 1 modulo every prime in T_F.

We consider the $\mathbb{Q}[G]$-module $\bigwedge\limits_{\mathbb{Q}[G]}^{r} \mathbb{Q}U_{S,T}$.

Definition 3.1. *The Rubin-Stark lattice, $\Lambda_{S,T}$, is the set of all $\varepsilon \in \bigwedge\limits_{\mathbb{Q}[G]}^{r} \mathbb{Q}U_{S,T}$ such that:*

- $e_\chi \varepsilon = 0$ *for all characters χ such that* $\mathrm{ord}_{s=0} L_{S,T}(\chi, s) > r$.
- *For every r-tuple $(\phi_1, \ldots, \phi_r) \in (\mathrm{Hom}_{\mathbb{Z}[G]}(U_{S,T}, \mathbb{Z}[G]))^r$,*

$$(\phi_1 \wedge \ldots \wedge \phi_r)(\varepsilon) \in \mathbb{Z}[G],$$

where $(\phi_1 \wedge \ldots \wedge \phi_r)(\varepsilon) = \det(\phi_i(\varepsilon_j), 1 \le i, j \le r)$ for $\varepsilon = \bigwedge\limits_{j=1}^{r} \varepsilon_j$, then extend this map $\mathbb{Z}[G]$ - linearly.

We also write $ev_\varepsilon(\phi_1 \wedge \ldots \wedge \phi_r)$ for $(\phi_1 \wedge \ldots \wedge \phi_r)(\varepsilon)$.

The Rubin-Stark conjecture then says the following:

Conjecture 3.2. *With the notation as before, there exists a unique element $\varepsilon_{S,T} \in \Lambda_{S,T}$ such that*

$$R_{\mathrm{Rubin-Stark}}(\varepsilon_{S,T}) = \frac{1}{r!}\theta^{(r)}_{F/k,S,T}(0),$$

where the definition of the regulator $R_{\mathrm{Rubin-Stark}}$ is given in [13].

The Rubin-Stark conjecture is known to follow from the Equivariant Tamigawa Number Conjecture (see [1]). In particular, the ETNC is known for $k = \mathbb{Q}$ (proven for $p > 2$ by Burns and Greither in [2], and for $p = 2$ by Flach in [4]), and so the above conjecture is true for $k = \mathbb{Q}$.

We remark that for a commutative ring R and maps

$$\phi_1, \ldots, \phi_r, \in \mathrm{Hom}_{\mathbb{Z}[G]}(U_{S,T}, R[G]),$$

$ev_{\varepsilon}(\phi_1 \wedge \ldots \wedge \phi_r)$ is well-defined in $R[G]$; the proof of this is given in [13].

We now turn to the statement of the Gross-type conjecture. Consider L, an abelian extension of k containing F that satisfies the following properties:

- $S_{\mathrm{ram}}(L/k) \subseteq S$.
- The set $L_T^\times$ of elements of $L^\times$ that are congruent to 1 modulo T has no $\mathbb{Z}$-torsion.

We let H be the Galois group of L/F, and $\mathcal{G}$ be the Galois group of L/k. For a given λ_i. we define

$$\phi_{\lambda_i} : F^\times \longrightarrow I(H)/I(H)^2 \otimes \mathbb{Z}[G]$$

$$\phi_{\lambda_i}(x) = \sum_{\sigma \in G} (\rho_{\lambda_i}(\widehat{x^{\sigma^{-1}}}) - 1) \otimes \sigma,$$

where ρ_{λ_i} is the local Artin map taking values in the decomposition group for λ_i in the extension L/F, which is a subgroup of H. Let $\psi_{\lambda_i} = t \circ \phi_{\lambda_i}$, where t is the isomorphism from Lemma 2.4.

Conjecture 3.3. *With the assumptions at the start of this section and above,*

- $\theta_{L/k,S,T}(0) \in I_G^r$

- *Assuming that the Rubin - Stark conjecture holds for the data $(F/k, S, T)$ and that the Rubin-Stark element is ε_F,*

$$\theta_{L/k,S,T}(0) = \mathrm{ev}_{\varepsilon_F}(\psi_{\lambda_1} \wedge \ldots \wedge \psi_{\lambda_r}) \text{ in } I_G^r/I_G^{r+1}.$$

We remark that the ψ's take values in $R[G]$; in [13], section 5.3, it is shown that $\mathrm{ev}_{\varepsilon_F}(\psi_{\lambda_1} \wedge \ldots \wedge \psi_{\lambda_r})$ does make sense in I_G^r/I_G^{r+1}.

This conjecture is known to be true for the same situations where the Rubin-Stark conjecture is known to be true, again as a consequence the ETNC. In particular, it is known when $k = \mathbb{Q}$.

3.1.1 Eliminating the set T

The presence of the set T is needed to ensure that $\theta_{F/k,S,T}(0) \in \mathbb{Z}[G]$ (this is true by a theorem of Deligne and Ribet, see [3]). However, in order to put this Gross-type conjecture in the context of Kurihara's conjecture, we will need a way to bypass the presence of the set T. To do this, we first prove the following lemma:

Lemma 3.4. *With the notation at the start of this section, for $\chi \neq \omega_p$,*

$$\chi(\prod_{v \in T}(1 - \sigma_v^{-1} Nv)) \in (\mathbb{Z}_p[G]^{\chi})^{\times}.$$

Proof. Let χ be a character of G different from the Teichmuller character ω_p. Also we will write $G = P \times \Delta$, where P is the p-primary part of G. Using this decomposition and one of the characterizations of θ in the L-functions section, we can write

$$\theta^{\chi} = \sum_{\tau \in P, \sigma \in \Delta} a_{\tau,\sigma} \chi(\sigma) \tau \in \mathbb{Z}_p(\chi)[P].$$

If we show that each term in the product is a unit, then we are done. To that end, let v be a prime in T, and consider $\chi(1-\sigma_v^{-1}Nv)$. We decompose σ_v as $\sigma_{P,v}\cdot\sigma_{\Delta,v}$; then

$$\chi(1-\sigma_v^{-1}Nv) = 1-\chi(\sigma_{\Delta,v}^{-1})\cdot Nv\cdot\sigma_{P,\Delta}^{-1}.$$

Let $\alpha=\chi(\sigma_{\Delta,v}^{-1})\cdot Nv$. We want to show that α is not 1 mod p in $\mathbb{Z}_P(\chi)$. Suppose otherwise. Note that the definition of ω_p is that for every $\zeta\in\mu_{p^\infty}(F)$, $\zeta^{\sigma_v}=\zeta^{\omega_p(\sigma_v)}$. But modulo v, $\zeta^{\sigma_v}\equiv\zeta^{Nv}$. Thus, $\omega_p(\sigma_v)\equiv Nv$ mod p. Therefore, under our assumption, $\omega_p(\sigma_{\Delta,v})^{-1}\equiv\chi(\sigma_{\Delta,v}^{-1})$. However, since $\chi\neq\omega_p$, there do exist primes where $\omega_p(\sigma_{\Delta,v})^{-1}$ is not congruent to $\chi(\sigma_{\Delta,v}^{-1})$ mod p.

Now, let $n=\mathrm{ord}(\sigma_{P,v})$, which is a power of p. Then we have

$$1-\alpha^n=(1-\alpha\sigma_{P,v})(1+\alpha\sigma_{P,v}+\ldots+(\alpha\sigma_{P,v})^{n-1}).$$

However, since α is not congruent to 1 modulo p, neither is α^n, since n is a p-th power. Therefore, $1-\alpha^n$ is not divisible by p, and is therefore a unit in $\mathbb{Z}_p(\chi)[\Delta]$. Thus, $\chi((1-\sigma_v^{-1}Nv))\in\mathbb{Z}_p[G]^\times$. $\square$

Now, in the full lattice, we define ε_S by

$$\varepsilon_{S,T}=\prod_{v\in T}(1-\sigma_v^{-1}Nv)\varepsilon_S;$$

note that $\prod_{v\in T}(1-\sigma_v^{-1}Nv)$ is a unit in $\mathbb{Q}[G]$. By the lemma, when we take χ-components, we get that $\varepsilon_S^\chi\in(\Lambda_{S,T}\otimes\mathbb{Z}_p)^\chi$. We make this definition because of the relation

$$\prod_{v\in T}(1-\sigma_v^{-1}Nv)\theta_{F/k,S}^\chi(0)=\theta_{F/k,S,T}^\chi(0).$$

Let χ be a character of G different from ω. Hitting both sides with the idempotent e_χ and then applying $\mathcal{R}_{\mathrm{Rubin-Stark}}$ to both sides yields

$$\mathcal{R}_{\mathrm{Rubin-Stark}}(\varepsilon_S^\chi) = \prod_{i=1}^{r} \log(Nv_i) \cdot (\theta_S^\chi(0)).$$

Also, we not only want to know that $\varepsilon_{S,T}$ exists, but we also want an explicit description of it. From the preceding discussion, we only need to describe ε_S. We start by recalling an theorem of Stickleberger.

Theorem 3.5. *For an abelian number field F, $\theta_{F/\mathbb{Q},S,T}$ annihilates the ideal class group of F.*

This theorem was proven in 1890 by Stickleberger. We can also deduce this fact using the main conjecture in Theorem 2.6 and the aforementioned result that the initial Fitting ideal of a module over a ring is contained in the annihilator of the module over the ring.

Now, for every i we define $g(\lambda_i)$ to be the element of $\mathcal{F}$ such that

$$\mathrm{div}(g(\lambda_i)) = \theta_{\mathcal{F},S}^\chi(0) \cdot \lambda_i,$$

this is possible due to Theorem 3.5. Denote $\tilde{\varepsilon} = g(\lambda_1) \wedge \ldots \wedge g(\lambda_r)$. Then

$$R_{\mathrm{Rubin-Stark}}(\tilde{\varepsilon}^\chi) = \prod_{i=1}^{r} \log(\mathbf{N}_{\ell_i}) \cdot (\theta_{S_{\mathrm{ram}}}^\chi(0))^r.$$

Since

$$\frac{1}{r!}(\theta_{F/k,S}^\chi)^{(r)}(0) = \prod_{i=1}^{r} \log(\mathbf{N}_{\ell_i}) \cdot (\theta_{S_{\mathrm{ram}}}^\chi(0)),$$

this shows that $(\theta_{S_{\mathrm{ram}}}^\chi(0))^r \varepsilon_S^\chi = (\theta_{S_{\mathrm{ram}}}^\chi(0))\tilde{\varepsilon}^\chi$.

3.2 Relating the two conjectures

The main goal of this section is to relate Gross's conjecture to the $\delta(\theta_L^\chi)$'s that appear in Kurihara's conjecture. Our set-up is as follows: let our base field be $k = \mathbb{Q}$. Let p be an odd prime, $\mathcal{F}$ an abelian extension of $\mathbb{Q}$ with Galois group Δ, where Δ has order co-prime to p. Given a prime $\ell \equiv 1 \bmod p^N$ that is unramified in $\mathcal{F}/\mathbb{Q}$, we let $\mathcal{K}_\ell$ be the unique subfield of $\mathbb{Q}(\mu_\ell)$ of degree p^N over $\mathbb{Q}$, and $\mathcal{L}_\ell = \mathcal{F}\mathcal{K}_\ell$, with Galois group G_ℓ. We consider a set of primes $\{\ell_1, \ldots, \ell_r\}$ as in the start of this section, unramified in $\mathcal{F}/\mathbb{Q}$, with the associated set $S_0 = \{\lambda_1, \ldots, \lambda_r\}$ of primes in $\mathcal{F}$, also as before. Then each G_{ℓ_i} is cyclic, and we will choose generators $\sigma_1, \ldots, \sigma_r$ such that $<\sigma_i>= G_{\ell_i}$.

Letting $n_i = \ell_1 \ldots \ell_i$ for i between 1 and r, we denote $\mathcal{L}_{n_r} = \mathcal{L}_{\ell_1}\mathcal{L}_{\ell_2}\ldots\mathcal{L}_{\ell_i}$. We denote the Galois group of $\mathcal{L}_i/\mathcal{F}$ by G_{n_i}. Finally, we let $S = S_0 \bigcup S_{\mathrm{ram}}(\mathcal{F}/\mathbb{Q})$.

Recall that $I_{G_{\ell_i}}$, the G_{ℓ_i}-augmentation ideal of $\mathbb{Z}[\mathrm{Gal}(\mathcal{L}_{n_r}/\mathbb{Q})]$, is the ideal in $\mathbb{Z}[\mathrm{Gal}(\mathcal{L}_{n_r}/\mathbb{Q})]$ generated by elements of the form $(\sigma - 1)$, for $\sigma \in G_{\ell_i}$. In fact, since G_{ℓ_i} is cyclic and generated by σ_i, $I_{G_{\ell_i}}$ is generated by $\sigma_i - 1$. We will denote by $\bar{I}_{G_{\ell_i}}$ the G_{ℓ_i}-augmentation ideal of $\mathbb{Z}[\mathrm{Gal}(\mathcal{L}_i/\mathbb{Q})]$. By lemma, we know that

$$\bar{I}_{G_{\ell_i}}/\bar{I}^2_{G_{\ell_i}} \cong \overline{I(G_{\ell_i})}/\overline{I(G_{\ell_i})}^2 \otimes \mathbb{Z}[\Delta] \cong (\mathbb{Z}/p^N\mathbb{Z})[\Delta],$$

since $\overline{I(G_{\ell_i})}/\overline{I(G_{\ell_i})}^2$ is isomorphic to G_{ℓ_i}, which is cyclic of order p^N. For each i, we denote this isomorphism by

$$\pi_i : \bar{I}_{G_{\ell_i}}/\bar{I}^2_{G_{\ell_i}} \xrightarrow{\sim} (\mathbb{Z}/p^N\mathbb{Z})[\Delta].$$

On the other hand, consider $I^r_{G_{n_r}}/I^{r+1}_{G_{n_r}}$, which is the object that appears in the Gross-type conjecture. Let α be an element of $I^{r+1}_{G_{n_r}}$. $I^{r+1}_{G_{n_r}}$ is generated by elements of the form $\tau - 1$, for $\tau \in G_{n_r}$; however, by the decomposition of G_{n_r} in the opening paragraph, we know that $I_{G_{n_r}}^{r+1}$ is generated by elements of the form $\sigma_i - 1$, for $1 \leq i \leq r$. Thus, we have that α can be written as a $\mathbb{Z}[\Delta]$-linear combination of elements of the form

$$\prod_{j=1}^{r+1}(\beta_j - 1),$$

where, for each j, $\beta_j = \sigma_i$ for some $1 \leq i \leq r$. By the pigeonhole principle, we must then have that there exists some i such that for at least two distinct j's, $\beta_j = \sigma_i$. We conclude that each of the above elements is in $I_{G_{\ell_i}}^2$ for some i, and so

$$\alpha \in (I_{G_{\ell_1}}^2 + \ldots + I_{G_{\ell_r}}^2).$$

Thus, $I_{G_{n_r}}^{r+1} \subseteq (I_{G_{\ell_1}}^2 + \ldots + I_{G_{\ell_r}}^2)$, and so we have a surjection

$$I_{G_{n_r}}^r / I_{G_{n_r}}^{r+1} \longrightarrow I_{G_{n_r}}^r / ((I_{G_{\ell_1}}^2 + \ldots + I_{G_{\ell_r}}^2) \cap I_{G_{n_r}}^r).$$

As before, we obtain the isomorphism

$$I_{G_{n_r}}^r / ((I_{G_{\ell_1}}^2 + \ldots + I_{G_{\ell_r}}^2) \cap I_{G_{n_r}}^r) \cong I(G_{n_r})^r / ((I(G_{\ell_1})^2 + \ldots + I(G_{\ell_r})^2) \cap I(G_{n_r})^r) \otimes \mathbb{Z}[\Delta].$$

However, the left entry of this tensor product is cyclic, generated by the class of $((\sigma_1 - 1) \cdot \ldots \cdot (\sigma_r - 1))$. Moreover, since each σ_i has order p^N in G_{ℓ_i}, we have that in $I_{G_{n_r}}$,

$$0 = \sigma_i^{p^N} - 1 = (\sigma_i - 1)(\sigma_i^{p^N - 1} + \ldots + \sigma_i + 1) = (\sigma_i - 1)((\sigma_i^{p^N - 1} - 1) + \ldots + (\sigma_i - 1) + p^N),$$

which means that $p^N(\sigma_i - 1) \in (I_{G_{\ell_1}}^2 + \ldots + I_{G_{\ell_r}}^2)$. Thus, $((\sigma_1 - 1) \ldots (\sigma_r - 1))$ has order divisible byp^N, and it is easy to show that the image of the surjection is also isomorphic to $(\mathbb{Z}/p^N\mathbb{Z})[\Delta]$. We will denote this map by

$$\pi : I^r_{G_{n_r}}/I^{r+1}_{G_{n_r}} \xrightarrow{\sim} (\mathbb{Z}/p^N\mathbb{Z})[\Delta].$$

Let $\theta = \theta_{(\mathcal{L}_{n_r}/k,S)}(0)$. Conjecture 3.3 states that $\theta \in I^r_{G_{n_r}}$ and that its class mod $I^{r+1}_{G_{n_r}}$ is equal to $\mathcal{R}_{\mathrm{Gross}}(\varepsilon_{\mathcal{F}})$, where $\varepsilon_{\mathcal{F}}$ is the Rubin-Stark element associated to the data $(\mathcal{F}/k, S, T)$ and the set of split primes $\{\ell_1, \ldots, \ell_r\} \subseteq S$. In particular, we have maps

$$\phi_{\lambda_i} : \mathcal{F}^\times \longrightarrow I(G_{n_r})/I(G_{n_r})^2 \otimes \mathbb{Z}[\Delta]$$

given by

$$\phi_{\lambda_i}(x) = \sum_{\sigma \in \Delta} (\rho_{\lambda_i}(\widehat{x^{\sigma^{-1}}}) - 1) \otimes \sigma,$$

where ρ_{λ_i} is the local Artin map taking values in G_{n_r}, and

$$\mathcal{R}_{\mathrm{Gross}}(\varepsilon_{\mathcal{F}}) = \mathrm{ev}_{\varepsilon_{\mathcal{F}}}(\phi_{\lambda_1} \wedge \ldots \wedge \phi_{\lambda_r}).$$

Similarly, we define

$$\bar{\phi}_{\lambda_i} : \mathcal{F}^\times \longrightarrow \bar{I}(G_{\ell_i})/\bar{I}(G_{\ell_i})^2 \otimes \mathbb{Z}[\Delta]$$

by

$$\bar{\phi}_{\lambda_i}(x) = \sum_{\sigma \in \Delta} (\bar{\rho}_{\lambda_i}(\widehat{x^{\sigma^{-1}}}) - 1) \otimes \sigma,$$

where $\bar{\rho}_{\lambda_i}$ is the local Artin map taking values in G_{ℓ_i}. We wish to prove the following:

Proposition 3.6. *Under all the hypotheses at the start of this subsection, we have*

$$\pi(\mathcal{R}_{\mathrm{Gross}}(\varepsilon_{\mathcal{F}})) = \mathrm{ev}_{\varepsilon_{\mathcal{F}}}((\pi_1 \circ \bar{\phi}_{\lambda_1}) \wedge \ldots \wedge (\pi_r \circ \bar{\phi}_{\lambda_r})),$$

where the maps π_i are defined at the beginning of this subsection.

Proof. We write $\varepsilon_{\mathcal{F}} = x_1 \wedge \ldots \wedge x_r$, where the x_i's are in $\mathcal{F}^\times$. (We know $\varepsilon_{\mathcal{F}}$ can be written in this manner, but we will not need the specific values of the x_i's for this proof). By definition,

$$\begin{aligned}\mathrm{ev}_{\varepsilon_{\mathcal{F}}}(\phi_{\lambda_1} \wedge \ldots \wedge \phi_{\lambda_r}) &= (\phi_{\lambda_1} \wedge \ldots \wedge \phi_{\lambda_r})(x_1 \wedge \ldots \wedge x_r) \\ &= \sum_{\tau \in S_r} \mathrm{sgn}(\tau) \prod_{i=1}^{r} \phi_{\lambda_i}(x_{\tau(i)})\end{aligned}$$

We analyze the above summation term by term. Without loss of generality, we take $\tau = \mathrm{id}$. Consider the term $\prod_{i=1}^{r} \phi_{\lambda_i}(x_i)$. For elements $\tau_1, \ldots, \tau_k \in G$, we have the general factorization

$$((\prod_{i=1}^{k} \tau_i) - 1) \ = \ \sum_{Z \subseteq [k]} \prod_{i \in Z} (\tau_i - 1).$$

Since $G = \prod_{i=1}^{r} G_{\ell_i}$, we combine the above general factorization with the definition of the ϕ_{λ_i} to get that in $I(G)^r/I(G)^{r+1} \otimes \mathbb{Z}[\Delta]$,

$$\phi_{\lambda_i}(x_i) = \sum_{\substack{Z \subseteq [r] \\ Z \neq \varnothing}} \prod_{j \in Z} (\phi_{\lambda_i}(x_i))_j,$$

where $(\phi_{\lambda_i}(x_i))_j$ is the component of $\phi_{\lambda_i}(x_i)$ in $I(G_{\ell_j})$. The above formula comes from applying the factorization formula above to $\rho_{\lambda_i}(x_i^\sigma)$ for each $\sigma \in \Delta$, then collecting terms based on the subsets of $[r]$.

When we take the product of all the ϕ_{λ_i}'s, we obtain

$$\prod_{i=1}^{r} \phi_{\lambda_i}(x_i) \ = \ \prod_{i=1}^{r} \sum_{\substack{Z \subseteq [r] \\ Z \neq \varnothing}} \prod_{j \in Z} (\phi_{\lambda_i}(x_i))_j.$$

However, when you expand the above equation, any term that has a Z that contains more than a single element will lie in $I(G)^{r+1}$, and so will be zero in $I(G)^r/I(G)^{r+1} \otimes \mathbb{Z}[\Delta]$. Thus, only terms where the subsets Z are single element sets appear, and so we can write

$$\prod_{i=1}^{r} \phi_{\lambda_i}(x_i) \;=\; \sum_{f} \prod_{i=1}^{r} (\phi_{\lambda_i}(x_i))_{f(i)},$$

where f ranges over all functions $f : [r] \to [r]$.

Since λ_{i+1} splits completely in $\mathcal{L}_{n_i}$, we have that $\rho_{\lambda_{i+1}}$ takes values in $G_{\ell_{i+1}} \times \ldots \times G_{\ell_r}$. This means that if the f above is not the identity function, then the corresponding term of the above sum is 0 when we project onto

$$I^r_{G_{n_r}}/((I^2_{G_{\ell_1}} + \ldots + I^2_{G_{\ell_r}}) \cap I^r_{G_{n_r}}).$$

To see this, observe that splitting condition lets us conclude that ρ_{λ_r} takes values in G_{ℓ_r}. $\rho_{\lambda_{r-1}}$ then takes values in $G_{\ell_{r-1}} \times G_{\ell_r}$; however, the portion in G_{ℓ_r} will be killed when we project, since it will give something in $I^2_{G_{\ell_r}}$. Continuing inductively gives us our claim. This lets us conclude that

$$\pi(\prod_{i=1}^{r} \phi_{\lambda_i}) = \prod_{i=1}^{r} (\pi_i \circ \mathrm{res})(\phi_{\lambda_i}),$$

where res is the extension of the Galois restriction map from G to G_{ℓ_i}.

From functorial properties of the local Artin map (see Proposition 5.8 in [10]), we have that $\mathrm{res} \circ \phi_{\lambda_i} = \bar{\phi}_{\lambda_i}$. Thus, we get that

$$\pi(\prod_{i=1}^{r} \phi_{\lambda_i}(x_i)) \;=\; \prod_{i=1}^{r} \pi_i(\mathrm{res} \circ \phi_{\lambda_i}(x_i)) \;=\; \prod_{i=1}^{r} \pi_i(\bar{\phi}_{\lambda_i}(x_i)).$$

Since this holds for every $\tau \in S_r$, this gives the result. $\square$

We think of $\pi(\mathcal{R}_{\mathrm{Gross}}(\varepsilon_{\mathcal{F}}))$ as the image of θ in $(\mathbb{Z}/p^N\mathbb{Z})[\Delta]$ obtained by using Conjecture 3.3, albeit with a loss of information that comes from the projection onto $I^r_{G_{n_i}}/((I^2_{G_{\ell_1}} + \ldots + I^2_{G_{\ell_r}}) \cap I^r_{G_{n_i}})$. We will denote this image by $\delta_{\vec{1}}(\theta_{\mathcal{L}_{n_r}})$. What the above lemma says is that $\delta_{\vec{1}}(\theta_{\mathcal{L}_{n_r}})$ can be computed from the extensions $\mathcal{L}_i$ for all i. $\delta_{\vec{1}}(\theta_{\mathcal{L}_{n_r}})$ is tied to the δ's as defined in Conjecture 2.8 in the following manner. Via the procedure outlined after Proposition 2.7, we have the decomposition

$$\theta_{\mathcal{L}_\infty} \;=\; \sum \delta_{i_1,\ldots,i_r}(\theta_{\mathcal{L}_\infty})(\sigma_1 - 1)^{i_1}\widehat{\cdot \ldots \cdot}(\sigma_r - 1)^{i_r},$$

where $\delta_{1,1,\ldots,1}(\theta_{\mathcal{L}_\infty})$ is an element of $\Lambda_{\mathcal{F}_\infty}$. Hitting this with the map r_N in section 2.3 gives

$$\theta_{\mathcal{L}_N} \;=\; \sum r_N[(\delta_{i_1,\ldots,i_r})](\theta_{\mathcal{L}_\infty})(\sigma_1 - \widehat{1)^{i_1}\cdot \ldots}\cdot(\sigma_r - 1)^{i_r},$$

with the map r_N as defined at the end of section 1.5. Moreover, the terms for which $i_1 + \ldots + i_r < r$ do not appear, by the first half of the Conjecture 3.3.

In fact, this gives the image of $\theta_{\mathcal{L}_N}$ in I^r_G. Applying π to this should then give $\delta_{\vec{1}}(\theta_{\mathcal{L}_{n_r}})$, so we conclude that $\delta_{\vec{1}}(\theta_{\mathcal{L}_{n_r}}) = (\pi \circ r_N)(\delta_{1,\ldots,1}(\theta_{\mathcal{L}_\infty}))$. Compare with Theorem 2.4 in [14].

Chapter 4

Proving Kurihara's Conjecture

4.1 A Chebotarev-Type Argument

In this section, we will prove a technical result that we need for the proof of Kurihara's conjecture. Our base field is still $\mathbb{Q}$. We fix an odd prime p and a sufficiently large positive integer N. Let $\mathcal{Q}$ be a CM abelian extension of $\mathbb{Q}$ with Galois group $G \cong P \times \Delta$, where P is a p-group and Δ has order co-prime to p, and contains a complex conjugation automorphism $\mathfrak{j}$. (The application will be when $\mathcal{Q}$ is some finite level of the cyclotomic $\mathbb{Z}_p$-extension of a CM field $\mathcal{F}$ whose Galois group over $\mathbb{Q}$ has order coprime to p). Given a prime $\ell \equiv 1 \bmod p^N$, we let $\mathcal{K}_\ell$ be the unique subfield of $\mathbb{Q}(\mu_\ell)$ of degree p^N over $\mathbb{Q}$, and $\mathcal{L}_\ell = \mathcal{Q}\mathcal{K}_\ell$. For a set of primes $\{\ell_1, \ldots, \ell_r\}$ that are distinct, unramified in the extension $\mathcal{Q}/\mathbb{Q}$, and congruent to 1 modulo p^N, we set $n_r = \ell_1 \ldots \ell_r$ and define $\mathcal{L}_{n_r}$ to be the compositum $\mathcal{L}_{\ell_1}\mathcal{L}_{\ell_2} \ldots \mathcal{L}_{\ell_r}$. We begin with two lemmas needed for the argument.

Lemma 4.1. *For a character χ of Δ, $\chi \neq \omega$ and an extension $\mathcal{L} = \mathcal{L}_{n_r}$ as above, the natural map*

$$(\mathcal{Q}^\times/(\mathcal{Q}^\times)^{p^N})^\chi \longrightarrow (\mathcal{L}(\mu_{p^N})^\times/((\mathcal{L}(\mu_{p^N})^\times)^{p^N})^\chi$$

is injective.

Proof. Assume it is not injective. Then there exists a nontrivial element $x \in (\mathcal{Q}^\times/(\mathcal{Q}^\times)^{p^N})^\chi$ such that $x = \xi^{p^N}$, for some $\xi \in \mathcal{L}(\mu_{p^N})^\times$. So, let $\sigma \in \mathrm{Gal}(\mathcal{L}(\mu_{p^N})/\mathcal{Q})$. Applying $\sigma - 1$ to the above equality gives $1 = (\xi^{\sigma-1})^{p^N}$, which implies that $\xi^{\sigma-1} \in \mu_{p^N}$. However, since $\chi \neq \omega$, $\mathcal{L}(\mu_{p^N})^\chi$ has no non-trivial roots of unity, and so $\xi^{\sigma-1} = 1$. Since this is true for all σ in the Galois group, we have $\xi = 1$, and so $x = 1$, a contradiction. □

Lemma 4.2. *The units of* $(\mathbb{Z}/p^N\mathbb{Z})(\chi)[P]$ *are precisely the elements* $\sum\limits_{\sigma \in P} a_\sigma \sigma$ *for which* p *does not divide* $\sum\limits_{\sigma \in P} a_\sigma$.

Proof. $(\mathbb{Z}/p^N\mathbb{Z})(\chi)[P]$ is a local ring (see [12], section 2) with maximal ideal $\mathfrak{m} = (p, I(P))$. Since everything not in the maximal ideal is a unit, it is enough to show that the elements of $\mathfrak{m}$ are precisely the set of elements of the form $\sum\limits_{\sigma \in P} a_\sigma \sigma$ for which p divides $\sum\limits_{\sigma \in P} a_\sigma$. Let $\mathcal{U}$ be this set; in fact, it is an ideal in $((\mathbb{Z}/p^N\mathbb{Z})(\chi)[P])$. By the definition of the augmentation ideal $I(P)$, the sum of the coefficients of any element of $I(P)$ is 0, and so it is clear that $\mathfrak{m} \subseteq \mathcal{U}$.

On the other hand, let $u = \sum\limits_{\sigma \in P} a_\sigma \sigma \in \mathcal{U}$, and $c = \sum\limits_{\sigma \in P} a_\sigma$. Define $v = \sum\limits_{\sigma \in P} (c - a_\sigma)(\sigma - 1)$. By definition, $v \in \mathfrak{m}$. Also, $u + v = (c \sum\limits_{\sigma \in P} \sigma) + (|P| - 1)c$, which is divisible by c, and therefore p. Thus, $u \in \mathfrak{m}$, and so $\mathfrak{m} = \mathcal{U}$, which completes the proof. □

We are now ready to prove the technical theorem that we need. We refer the reader to the paragraph preceding Lemma 2.11 for the definitions of the elements f_i that appear in the following theorem, and to the paragraph preceding Proposition 3.6 for the definition of the maps $\overline{\phi_{\lambda_j}}$. Compare the theorem with the conditions specified in [8], page 72, or in [14], Theorem 3.1.

Theorem 4.3. *Let $r \in \mathbb{N}$. Given an odd character χ of Δ, $\chi \neq \omega$, and classes $\hat{v}_1^{\chi}, \ldots, \hat{v}_r^{\chi}$ in $(Cl_{\mathcal{Q}} \otimes \mathbb{Z}_p)^{\chi}$, we can find rational primes $\ell_1, \ell_2, \ldots, \ell_r$ satisfying the following conditions:*

- *$\ell_j \equiv 1$ mod p^N and ℓ_j is completely split in the composite extension $\mathcal{L}_{n_{j-1}}$, for every $1 \leq j \leq r$, where $n_{j-1} = \ell_1 \ldots \ell_{j-1}$.*
- *For each $1 \leq j \leq r$, there exists a prime λ_j in $\mathcal{Q}$ lying over ℓ_j such that $\lambda_j \sim \hat{v}_j^{\chi}$*
- *For every $1 \leq i, j \leq r$, $\overline{\phi_{\lambda_j}}(f_i) \in ((\mathbb{Z}/p^N\mathbb{Z})(\chi)[P])^{\times}$ if $i = j$, and is 0 otherwise.*

Proof. We do this by induction on r. As the argument for the base case is essentially the same as the inductive step, we will prove the inductive step first. Assume that the theorem holds up to $r-1$; we will show it holds for r. The first condition is satisfied if ℓ_r splits in $\mathcal{E}_{r-1}/\mathbb{Q}$, where $\mathcal{E}_{r-1} = \mathcal{L}_{n_{r-1}}(\mu_{p^N})$.

For the second condition, let H_χ be the subextension of the Hilbert class field of $\mathcal{Q}$ whose Galois group over $\mathcal{Q}$ is isomorphic to $(Cl_{\mathcal{Q}} \otimes \mathbb{Z}_p)^{-}$. We know that $\mathfrak{j}$ acts via lift and conjugation on both $\mathrm{Gal}(H_\chi/\mathcal{Q})$ and $\mathrm{Gal}(\mathcal{E}_{r-1}/\mathcal{Q})$. Since $\mathcal{E}_{r-1}/\mathbb{Q}$ is an abelian extension, $\mathrm{Gal}(\mathcal{E}_{r-1}/\mathcal{Q})$ is abelian and therefore $\mathfrak{j}$ acts trivially on it. On the other hand, $\mathfrak{j}$ acts as (-1) on $\mathrm{Gal}(H_\chi/\mathcal{Q})$. Combining this with the previous fact gives us that $H_\chi/\mathcal{Q}$ and $\mathcal{E}_{r-1}/\mathcal{Q}$ are linearly disjoint.

The third condition requires the most work. Define X to be the subgroup $\langle f_1, \ldots, f_r \rangle \subseteq (\mathcal{Q}^{\times}/(\mathcal{Q}^{\times})^{p^N})^{\chi}$. Recall that as a $((\mathbb{Z}/p^N\mathbb{Z})(\chi)[P])^{\times}$ - module, this is free of rank n. Thus, the elements of the set

$$\mathfrak{F} \coloneqq \{f_i^{\sigma} | 1 \leq i \leq r, \sigma \in P\}$$

are $\mathbb{Z}/p^N\mathbb{Z}$-linearly independent. From Lemma 4.1, we conclude that the elements of $\mathfrak{F}$ are $\mathbb{Z}/p^N\mathbb{Z}$-linearly independent in $(\mathcal{E}_{r-1}^\times/(\mathcal{E}_{r-1}^\times)^{p^N})^\chi$.

Let us consider the family of extensions $\mathcal{E}_{r-1}(x^{1/p^N})$, for $x \in \mathfrak{F}$. From the preceding paragraph, we know that each of these extensions are linearly disjoint from the compositum of the rest. From Kummer theory, we have an isomorphism

$$X \cong \operatorname{Hom}_{\mathbb{Z}/p^N}(\operatorname{Gal}(\mathcal{E}_{r-1}(x^{1/p^N})/\mathcal{E}_{r-1}), \mu_{p^N}).$$

The right hand side of this equation is acted upon by $\delta \in \Delta$ as

$$\delta * \phi(y) = \delta(\phi(\delta^{-1}y),$$

and the isomorphism respects the action of Δ on both sides. However, Δ acts on μ_{p^N} via ω and on X via χ. Thus, Δ must act on $\operatorname{Gal}(\mathcal{E}_{r-1}(x^{1/p^N})/\mathcal{E}_{r-1})$ via $\chi\omega^{-1}$. Therefore, $\mathfrak{j}$ acts as 1 on $\operatorname{Gal}(\mathcal{E}_{r-1}(x^{1/p^N})/\mathcal{E}_{r-1})$. From this, we conclude that each of these extensions is linearly disjoint from $\mathcal{E}_{r-1}H_\chi$.

Recall that

$$\overline{\phi_{\lambda_r}}(f_j) = \sum_{\sigma \in P} (\bar{\rho}_{\lambda_r}(\widehat{f_j^{\sigma^{-1}}}) - 1) \otimes \sigma.$$

From our characterization on the units of $(\mathbb{Z}/p^N\mathbb{Z})(\chi)[P]$, we can ensure that the third condition holds for $r = j$ if

$$\bar{\rho}_{\lambda_r}\widehat{(f_r) -} 1 \in (\mathbb{Z}/p^N\mathbb{Z})^\times \text{ and } \bar{\rho}_{\lambda_r}(\widehat{f_r^{\sigma^{-1}}}) - 1 \in (p\mathbb{Z}/p^N\mathbb{Z})\, \forall\, \sigma \neq \text{ id}.$$

From our identification of $I(G_{\ell_r})/I(G_{\ell_r})^2$ with $\mathbb{Z}/p^N\mathbb{Z}$, this is equivalent to saying that

$$\bar{\rho}_{\lambda_r}\widehat{(f_r) -} 1 \in G_{\ell_r}^\times \text{ and } \bar{\rho}_{\lambda_r}(\widehat{f_r^{\sigma^{-1}}}) - 1 \in G_{\ell_r}^p$$

To obtain conditions that we can use the Chebotarev theorem on, let us consider what happens if we were to localize at ℓ_r. The localization of both $\mathbb{Q}$ and $\mathcal{Q}$ at ℓ_r is $\mathbb{Q}_{\ell_r}$, since $\ell_r \equiv 1 \bmod p^N$. The localization of $\mathcal{L}_r$ at ℓ_r is the subextension of $\mathbb{Q}_{\ell_r}(\mu_{\ell_r})$ that has degree p^N over $\mathbb{Q}_{\ell_r}$, we will denote this subextension by $\mathbb{Q}_{\ell_r}(\mu_{\ell_r})^*$. From local class field theory,

$$\mathrm{Gal}(\mathbb{Q}_{\ell_r}(\mu_{\ell_r})/\mathbb{Q}_{\ell_r}) \;=\; \mathbb{Z}_{\ell_r}^{\times}/(1+\ell_r\mathbb{Z}_{\ell_r}),$$

and so, since $\ell_r \neq p$, we have

$$\mathrm{Gal}(\mathbb{Q}_{\ell_r}(\mu_{\ell_r})^*/\mathbb{Q}_{\ell_r}) \cong \mathbb{Z}_{\ell_r}^{\times}/(1+\ell_r\mathbb{Z}_{\ell_r})(\mathbb{Z}_{\ell_r}^{\times})^{p^N} \cong G_{\ell_r}.$$

Thus, we have that:

- $\bar{\rho}_{\lambda_r}(f_r)$ needs to generate G_{ℓ_r}, which occurs if and only if $\rho_{\lambda_r}(f_r) \notin (\mathbb{Z}_{\ell_r}^{\times})^p$.
- $\bar{\rho}_{\lambda_r}(f_r^{\sigma^{-1}}) \in G_{\ell_r}^p$ for $\sigma \neq \mathrm{id}$, which occurs if and only if $\rho_{\lambda_r}(f_r)^{\sigma^{-1}} \in (\mathbb{Z}_{\ell_r}^{\times})^p$.
- When $r \neq j$, we obtain that $\overline{\phi_{\lambda_r}}(f_j) = 0$ when $\bar{\rho}_{\lambda_r}(f_j) = 1$ for all σ, which occurs if and only if $\rho_{\lambda_r}(f_j)^{\sigma^{-1}} \in (\mathbb{Z}_{\ell_r}^{\times})^{p^N}$.

To finish the argument, consider the field extension $\mathcal{C}$ of $\mathcal{E}_{r-1}$ which is the composite of $\mathcal{E}_{r-1}H_\chi$ and all of the extensions $\mathcal{E}_{r-1}(x^{1/p^N})$, for $x \in \{f_i^\sigma | 1 \leq i \leq n, \sigma \in P\}$. Since we proved that these extensions are linearly disjoint from one another, the Galois group of $\mathcal{C}/\mathcal{E}_{r-1}$ is the product of the Galois groups of each of the component extensions over $\mathcal{E}_{r-1}$. Consider the element Ω in the Galois group of $\mathcal{C}$ which satisfies the following conditions:

- The coordinate for $\mathrm{Gal}(\mathcal{E}_{r-1}H_\chi/\mathcal{E}_{r-1})$ is $\hat{v}_r^\chi$ via the global Artin map.
- The coordinate for $\mathrm{Gal}(\mathcal{E}_{r-1}(f_r^{1/p^N})/\mathcal{E}_{r-1})$ has order p^N.

- For every $\sigma \in \Delta$, $\sigma \neq \mathrm{id}$, the coordinate for $\mathrm{Gal}(\mathcal{E}_{r-1}((f_r^\sigma)^{1/p^N})/\mathcal{E}_{r-1}$ is 1.
- For every $j < r$ and $\sigma \in \Delta$, the coordinate for $\mathrm{Gal}(\mathcal{E}_{r-1}((f_j^\sigma)^{1/p^N})/\mathcal{E}_{r-1})$ is a p-th power.

We note that $\mathcal{C}/\mathbb{Q}$, $\mathcal{C}/\mathcal{E}_{r-1}$, and $\mathcal{E}_{r-1}/\mathbb{Q}$ are all Galois extensions. Let H be the group $\mathrm{Gal}(\mathcal{C}/\mathbb{Q})$, and K be the group $\mathrm{Gal}(\mathcal{C}/\mathcal{E}_{r-1})$. Then we can view K as a subgroup of H. We use the Chebotarev density theorem on the extension $\mathcal{C}/\mathbb{Q}$. This gives us infinitely many primes whose associated Frobenius automorphism lies in the conjugacy class of Ω; let $\lambda_{\mathcal{C}}$ be one of them. Let λ_r be a prime in $\mathcal{Q}$ that lies below $\lambda_{\mathcal{C}}$, and ℓ_r be a rational prime that lies below it. By the above construction of Ω, λ_r satisfies the second and third conditions of the theorem. However, since Ω fixes $\mathcal{E}_{r-1}$, $\mathrm{Frob}_{\lambda_{\mathcal{E}_{r-1}}} = 1$, for $\lambda_{\mathcal{E}_{r-1}}$ a prime in $\mathcal{E}_{r-1}$ lying above λ_r and below $\lambda_{\mathcal{C}}$. Thus, ℓ_r splits completely in $\mathcal{E}_{r-1}/\mathbb{Q}$, and so the first condition of the theorem is satisfied.

For the base case of $r = 1$, only the first condition changes; as such, the argument for the base case is almost identical to the general argument above. The first condition is satisfied as long as ℓ_1 splits in $\mathcal{E}_0/\mathbb{Q}$, where $\mathcal{E}_0 := \mathcal{Q}(\mu_{p^N})$. The argument for the case of $r = 1$ is then identical to that of the inductive step, except for replacing $\mathcal{E}_{r-1}$ with $\mathcal{E}_0$. By induction, the proof is now complete. $\square$

4.2 The proof

4.2.1 A preliminary lemma and setup

We start with a pair of linear algebra lemmas.

Lemma 4.4. *Let M be an $n \times n$ block matrix over the commutative ring R of the* *form* $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$*, where A is a k* $\times$ *k matrix and D is a (n - k)* $\times$ *(n - k) matrix, and write the adjugate matrix of* M*, which we will denote as* $M^\dagger$*, as* $\begin{bmatrix} X & W \\ Y & Z \end{bmatrix}$*, with the block sizes the same as that of* M*. Then*

$$det(X) = det(M)^{k-1} \cdot det(D).$$

Proof. Let $\mathcal{R}$ be the polynomial ring $\mathbb{Z}[x_{ij} : 1 \leq i, j \leq n]$, and let $\mathcal{M}$ be the matrix $[x_{ij}]$, with block decomposition $\begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{C} & \mathcal{D} \end{bmatrix}$, where $\mathcal{A}$ and $\mathcal{D}$ have the same sizes as A and D respectively. We also write $\mathcal{M}^\dagger$ as $\begin{bmatrix} \mathcal{X} & \mathcal{W} \\ \mathcal{Y} & \mathcal{Z} \end{bmatrix}$; note that this matrix still has entries in $\mathcal{R}$. Then

$$\mathcal{M}^\dagger \cdot \mathcal{M} \; = \; \det(\mathcal{M}) I_n.$$

In particular, we have equations

$$\mathcal{A}\mathcal{X} + \mathcal{B}\mathcal{Y} = \det(\mathcal{M}) I_k$$

and

$$\mathcal{C}\mathcal{X} + \mathcal{D}\mathcal{Y} = 0.$$

Attempting to solve for $\mathcal{X}$ yields

$$\mathcal{X}\mathcal{M}_{\mathcal{D}} = \det(\mathcal{D})\det(\mathcal{M}) I_k,$$

where

$$\mathcal{M}_{\mathcal{D}} = \det(\mathcal{D})\mathcal{A} - \mathcal{B}\mathcal{D}^\dagger\mathcal{C}.$$

Taking determinants yields

$$\det(\mathcal{X})\det(\mathcal{M}_{\mathcal{D}}) = (\det(\mathcal{D})\det(\mathcal{M}))^k.$$

On the other hand, using the matrix identity

$$\begin{bmatrix} I_k & \mathcal{B}\mathcal{D}^\dagger \\ 0 & I_{n-k} \end{bmatrix} \begin{bmatrix} \mathcal{M}_{\mathcal{D}} & 0 \\ 0 & I_{n-k} \end{bmatrix} \begin{bmatrix} I_k & 0 \\ \mathcal{C} & \mathcal{D} \end{bmatrix} = \begin{bmatrix} \det(\mathcal{D})\mathcal{A} & \det(\mathcal{D})\mathcal{B} \\ \mathcal{C} & \mathcal{D} \end{bmatrix}$$

and then taking determinants, we get

$$\det(\mathcal{D})\det(\mathcal{M}_D) = \det(\mathcal{D})^k\det(\mathcal{M}).$$

From the previous two equations, we get

$$\det(\mathcal{D})^k\det(\mathcal{M})(\det(\mathcal{X}) - \det(\mathcal{D})\det(\mathcal{M})^{k-1}) = 0.$$

In the integral domain $\mathcal{R}$, $\det(\mathcal{D})$ and $\det(\mathcal{M})$ are non-zero divisors, so we conclude that

$$(\det(\mathcal{X}) - \det(\mathcal{D})\det(\mathcal{M})^{k-1}) = 0.$$

Applying the ring homomorphism $\phi : \mathcal{R} \longrightarrow \mathrm{R}$, which sends the variable x_{ij} to the ij-th entry of M then gives the result. □

Lemma 4.5. *Let R be a commutative ring and M an $n \times n$ matrix with entries in R whose determinant is not a zero divisor. Suppose N is another $n \times n$ matrix with entries in R such that*

$$MN = det(M)I_n. \tag{*}$$

Then $N = M^\dagger$, where $M^\dagger$ is the adjugate matrix of M.

Proof. Left-multiplying both sides of (*) by $M^\dagger$ gives

$$\det(M)N = \det(M)M^\dagger.$$

Since $\det(M)$ is a not a zero divisor, we can cancel it from both sides, giving the result. $\square$

We now set some notation. Let $\mathcal{F}$ and $X^\chi_{\mathcal{F}_\infty}$ be as before. Recall from Lemma 2.10 that we have a presentation

$$0 \to (\Lambda^\chi)^n \xrightarrow{f} (\Lambda^\chi)^n \to X^\chi_{\mathcal{F}_\infty} \to 0.$$

This descends to a presentation

$$0 \to (\Lambda^\chi_{\mathcal{F}_m})^n \to (\Lambda^\chi_{\mathcal{F}_m})^n \to A^\chi_{\mathcal{F}_m} \to 0.$$

We picked generators of $X^\chi_{\mathcal{F}_\infty}$, which descend to generators of $A^\chi_{\mathcal{F}_m}$, and we select primes $v_1, \ldots, v_m$ which split all the way down to $\mathbb{Q}$ and which are representatives for the classes that form the chosen set of generators. Then we have a presentation:

$$0 \to \tilde{M} \xrightarrow{\tilde{f}} M \to A^\chi_{\mathcal{F}_m} \to 0,$$

where $M \cong \bigoplus_{i=1}^{n} \mathbb{Z}_p(\chi)[P]v_i$ and the matrix $\mathcal{A}$ corresponding to the map $\tilde{f}$ has

$$\det(\mathcal{A}) = \theta^\chi,$$

where $\theta^\chi = \theta^\chi_{\mathcal{F}_m/\mathbb{Q}}(0)$. We define $\mathcal{D}$ as we did at the end of Lemma 2.10, and choose a basis $f_1, \ldots, f_n$ of $\mathcal{D}$ in the same manner. We note that by Theorem 3.5, for every

$1 \leq i \leq n$, we can write

$$\theta^\chi \cdot v_i = \mathrm{div}(g_i)$$

for some $g_i \in \mathcal{D}$. Then we have the decomposition

$$g_i = \prod_{s=1}^{n} f_s^{a_{s,j}}$$

where $a_{s,j} \in \mathbb{Z}_p(\chi)[P]$ for all $1 \leq s, j \leq n$.

4.2.2 The main result

We now prove the following:

Theorem 4.6. *Fix a sufficiently large power of p, denoted p^m. Define sets*

$$\mathfrak{S}_j = \{t \in \mathbb{N} \mid t \textit{ is the product of } j \textit{ distinct primes all congruent to 1} \bmod p^m\},$$

and

$$\mathfrak{E}_j = \{\mathcal{L}_{n_j} \mid n_j \in \mathfrak{S}_j\}.$$

Assume that θ is not a zero-divisor. Then

$$\mathrm{Fitt}^i_{\Lambda^\chi_{\mathcal{F}_m}/p^N}(A^\chi_{\mathcal{F}_m}/p^N) = \mathfrak{T}_i,$$

where $\mathfrak{T}_i$ is the ideal generated by θ^χ and $\delta_{\vec{1}}(\theta^\chi_{\mathcal{L}_{n_r}})$, for $\mathcal{L}_{n_r} \in \mathfrak{E}_r$ and $1 \leq r \leq i$.

Proof. We already proved that $\mathrm{Fitt}^i_{\Lambda^\chi_{\mathcal{F}_m}/p^N}(A^\chi_{\mathcal{F}_m}/p^N) \supseteq \mathfrak{T}_i$ in Proposition 2.7, so all that is left is the other inclusion.

To prove the other inclusion, we proceed by induction. The base case of $i = 0$ is the main conjecture.

So suppose the inclusion is true for all the Fitting ideals up to $i-1$. Let $\mathcal{B}$ be an $(n-i)\times(n-i)$ minor of $\mathcal{A}$. We perform a series of row and column switches to obtain a matrix $\tilde{\mathcal{A}}$ for which $\mathcal{B}$ appears in the bottom right corner of $\tilde{\mathcal{A}}$. Reordering the rows corresponds to reordering the basis $f_1,\ldots,f_n$, while reordering the columns corresponds to reordering the basis $v_1,\ldots,v_n$; by abuse of notation, we will continue to refer to these bases as before.

Using the Chebotarev argument in chapter 3, we find rational primes $\ell_1,\ldots,\ell_n$ and associated primes $\lambda_1,\ldots,\lambda_n$ in $\mathcal{F}_m$ satisfying the three conditions in the theorem. In particular, note that due to the first condition in the theorem, the choices of both sets of primes is dependent on the reordering we did. Let

$$S = S_{\mathrm{ram}}(\mathcal{F}_m/\mathbb{Q})\bigcup\{\ell_1,\ldots,\ell_n\}.$$

By Theorem 3.5, for $1\le s\le n$, we denote by $g(\lambda_s)$ the element of $\mathcal{F}_m$ such that

$$\mathrm{div}(g(\lambda_s)) = \theta^{\chi}_{\mathcal{F}_m}\cdot\lambda_s.$$

We also let ε be the Rubin-Stark element associated to the data $(\mathcal{F}_m/\mathbb{Q},S)$ and the set of split primes $\{\ell_1,\ldots,\ell_i\}$. Recall that

$$\mathcal{R}_{\text{Rubin-Stark}}(\varepsilon^{\chi}) = (\theta^{\chi}_{\mathcal{F}_m/\mathbb{Q}})^{(i)}(0).$$

From the definition of the $g(\lambda_s)$'s and the uniqueness of ε, we have that

$$(\theta^{\chi})^n\varepsilon = \theta^{\chi}(g(\lambda_1)\wedge\ldots\wedge g(\lambda_i)).$$

Let X be the $n\times i$ matrix whose (s,j)-th entry is $\alpha_{s,j}$. Then, from the properties of the g_s's, we have that

$$\tilde{\mathcal{A}}X = \theta^{\chi} \cdot I_i.$$

Since θ^{χ} is not a zero-divisor, by Lemmas 4.5 and 4.4, this means that

$$(\theta^{\chi})^{i-1} \cdot \det(\mathcal{B}) = \det(\tilde{X}),$$

where $\tilde{X}$ is the upper left $i \times i$ minor of X.

Since $\operatorname{div}(g(\lambda_s)) = \theta^{\chi} \cdot \lambda_s$ and $\lambda_s \sim v_s$, we have that in $\mathcal{F}_m^{\times}$,

$$g(\lambda_s) = g_s \xi_s^{\theta^{\chi}} \text{ for some } \xi_s \in \mathcal{F}_m^{\times}.$$

This means that in $\bigwedge\limits_{\mathbb{Z}[P]}^{i} \mathcal{F}_m^{\times}$, we have

$$\bigwedge_{s=1}^{i} g(\lambda_s) = \sum_{\vec{y} \in \{0,1\}^i} \bigwedge_{s=1}^{i} (\theta^{\chi})^{\|\vec{y}\|_1} (g_s^{1-y_s} \xi_s^{y_s}), \text{ where } \|\vec{y}\|_1 = y_1 \, + \ldots + \, y_i. \tag{4.1}$$

We can write the g_s's in terms of our basis $f_1, \ldots, f_n$, and so we can use this and properties of wedge products to write the above equation in terms of the f_s's. Let $\vec{y} \in \{0,1\}^i$ with $\|\vec{y}\|_1 = k$. Define

$$\mathcal{Z}_k \coloneqq \{Z \colon Z \subseteq [n], |Z| = k, k \leq i\}.$$

For $Z \in \mathcal{Z}_k$ and $\vec{y} \in \{0,1\}^i$ with $\|\vec{y}\|_1 = k$, define $X_{Z,\vec{y}}$ to be the $(i-k) \times (i-k)$ minor of X obtained by deleting the rows in Z and deleting the columns for which corresponding entry of $\vec{y}$ is 1. Also, for the elements $z_1 < z_2 < \ldots < z_k$ of Z, we write

$$\vec{f}_Z = f_{z_1} \wedge \ldots \wedge f_{z_k}.$$

Then

$$\bigwedge_{s=1}^{i} (\theta^\chi)^{\|\vec{y}\|_1} (g_s^{1-y_s} \xi_s^{y_s}) = (\theta^\chi)^{\|\vec{y}\|_1} \sum_{Z \subseteq \mathcal{Z}} \det(X_{Z,\vec{y}})(\vec{f}_Z \wedge \vec{\xi}_{\vec{y}}),$$

where $\vec{\xi}_{\vec{y}}$ is just the wedge product of the present ξ_s terms in order of increasing index.

Let $\tilde{\mathcal{A}}_{Z,\vec{y}}$ denote the $(n-i+k) \times (n-i+k)$ minor of $\tilde{\mathcal{A}}$ obtained by deleting the rows corresponding to Z^c and the columns corresponding to the zero entries of $\vec{y}$. We combine the above paragraph with equation (4.1), and then apply Lemma 4.4 to obtain

$$\bigwedge_{s=1}^{i} g(\lambda_s) = (\theta^\chi)^{i-1} \det(\mathcal{B})(f_1 \wedge \ldots \wedge f_i) + \sum_{k=0}^{i} \sum_{\substack{\vec{y} \in \{0,1\}^i \\ \|\vec{y}\|_1 = k}} (\theta^\chi)^k \sum_{\substack{Z \subset \mathcal{Z}_k \\ Z \neq [i]}} \det(X_{Z,\vec{y}})(\vec{f}_Z \wedge \vec{\xi}_{\vec{y}})$$

$$= (\theta^\chi)^{i-1} \det(\mathcal{B})(f_1 \wedge \ldots \wedge f_i) + (\theta^\chi)^{i-1} \sum_{k=1}^{i} \sum_{\substack{\vec{y} \in \{0,1\}^i \\ \|\vec{y}\|_1 = k}} \sum_{\substack{Z \subset \mathcal{Z}_k \\ Z \neq [i]}} \det(\tilde{\mathcal{A}}_{Z,\vec{y}})(\vec{f}_Z \wedge \vec{\xi}_{\vec{y}})) + \theta^i(\vec{\xi}_{\vec{1}})$$

(Here, $\vec{1}$ is the all 1's element of $\{0,1\}$.) Now, since

$$(\theta^\chi)^i \varepsilon = \theta^\chi(g(\lambda_1) \wedge \ldots \wedge g(\lambda_i)),$$

we view the above equalities in $(\mathbb{Q} \bigwedge_{\mathbb{Z}[P]}^{i} \mathcal{F}_m^\times)^\chi$ and apply θ^χ to both sides of the first equation. As θ^χ is by assumption not a zero divisor, we may cancel $(\theta^\chi)^i$ and obtain:

$$\varepsilon^\chi = \det(\mathcal{B})(f_1 \wedge \ldots \wedge f_i) + (\sum_{k=1}^{i} \sum_{\substack{\vec{y}\in\{0,1\}^i \\ \|\vec{y}\|_1 = k}} \sum_{\substack{Z\subset\mathcal{Z}_k \\ Z\neq[i]}} \det(\tilde{\mathcal{A}}_{Z,\vec{y}})(\vec{f_Z} \wedge \vec{\xi_{\vec{y}}})) + \theta^\chi \vec{\xi_{\vec{1}}} \qquad (4.2)$$

We now apply Gross's regulator to the tower of extensions $\mathcal{L}_{n_i}/\mathcal{F}_m/\mathbb{Q}$ to (4.3); note that the Gross regulator in this setting is $\phi_1 \wedge \ldots \wedge \phi_i$. We then project onto $I^i_{G_{n_i}}/(I^2_{G_{\ell_1}} + \ldots + I^2_{G_{\ell_i}}) \cap I^i_{G_{n_i}})$. We observe the following:

- From the results in the section on Gross's conjecture, $\mathcal{R}_{Gross}(\varepsilon^\chi) = \delta_{\vec{1}}(\theta^\chi_{\mathcal{L}_{n_i}})$, which is in $\mathfrak{T}_i$.

- By the third condition in the Chebotarev argument, $(\overline{\phi_1} \wedge \ldots \wedge \overline{\phi_i})(f_1 \wedge \ldots \wedge f_i)$ is the determinant of the matrix whose j-th diagonal entry is $\overline{\phi_j}(f_j)$ (which is are units in $\Lambda^\chi_{\mathcal{F}_m}$), and has 0's outside of the diagonal. Thus, the determinant is also a unit in $\Lambda^\chi_{\mathcal{F}_m}$.

- By the Chebotarev construction, $\overline{\phi}_{\lambda_s}(f_j) = 0$ when $s \neq j$. So if $Z \neq [i]$ but is in $\mathcal{Z}_i$ (and so has size i), then there is some f_j that appears in $\vec{f_Z}$ with index $j > i$. From this, we see that when we calculate $(\overline{\phi_1} \wedge \ldots \wedge \overline{\phi_i})(\vec{f_Z})$, the column corresponding to f_j has entries of the form $\overline{\phi}_{\lambda_s}(f_j)$ for $1 \leq s \leq i < j$; therefore this column is 0, and so the determinant is 0. Thus, all of the other terms corresponding subsets $Z \subseteq \mathcal{Z}_k$ with $k = i$ and $Z \neq [i]$ are 0.

- For $1 \leq k < i$, $\det(\tilde{\mathcal{A}}_{Z,\vec{y}})$ is some $(n-i+k) \times (n-i+k)$ minor of $\tilde{\mathcal{A}}$ (and therefore of $\mathcal{A}$). This is an element of $\mathrm{Fitt}^{i-k}_{\Lambda^\chi_{\mathcal{F}_m}/p^N}(A^\chi_{\mathcal{F}_m}/p^N)$. By induction, this means they are contained in $\mathfrak{T}_{i-k}$, which is contained in $\mathfrak{T}_i$.

We conclude that $\det(\mathcal{B})$ times a unit in $\Lambda^\chi_{\mathcal{F}_m}$ is a sum of elements in $\mathfrak{T}_i$. Since $\mathcal{B}$ was an arbitrary $i \times i$ minor of $\mathcal{A}$, this completes the proof. $\square$

Since this is true for each finite level, taking projective limits with respect to the maps $r_{k+1,k}$ for $k \geq m$ gives the following:

Corollary 4.7. *For any* $i > 0$, $\mathrm{Fitt}^i_{\Lambda^\chi_{\mathcal{F}_\infty}/p^N}(X^\chi_{\mathcal{F}_\infty}/p^N)$ *is equal to the ideal* $\mathfrak{T}$ *generated by* $\theta^\chi_{\mathcal{F}_\infty/\mathbb{Q}}$ *and the* $\delta_{i_1,\ldots,i_r}(\theta^\chi_{\mathcal{L}_\infty})$*'s, where*

- $\mathcal{L}$ *ranges over all abelian extensions of* $\mathbb{Q}$ *such that* $\mathcal{L} \cap \mathcal{F}_\infty = \mathcal{F}$, $\mathrm{Gal}(\mathcal{L}/\mathbb{Q}) = \mathrm{Gal}(\mathcal{F}/\mathbb{Q}) \times \mathrm{Gal}(\mathcal{L}/\mathcal{F})$, *and* $\mathrm{Gal}(\mathcal{L}/\mathcal{F}) \cong \mathbb{Z}/p^N \times \ldots \times \mathbb{Z}/p^N$.

- $i_1 + \ldots + i_r \leq i$.

This settles Conjecture 2.9 for all $i \geq 0$.

Chapter 5

Future Work

The techniques developed in this dissertation can be extended in several directions. One direction is to try and extend the result to cases where the base field is not $\mathbb{Q}$, but a general totally real field k. The main difficulty here is in proving the result in Theorem 4.3, as base fields other than $\mathbb{Q}$ may not provide enough of the $\mathcal{L}_{n_i}$'s to make sure that $\overline{\phi_{\lambda_j}}(f_i) \in ((\mathbb{Z}/p^N\mathbb{Z})(\chi)[P])^\times$ (and 0 otherwise). However, under some restrictive conditions on k, one can construct enough extensions to ensure the above.

Part of this project was to get a Kurihara-like result for other Iwasawa modules, in particular the Tate module of 1-motives constructed by Popescu and Greither in [6]. Most of the techniques developed in this dissertation here still apply to those modules; in particular, the Chebotarev argument will still work for base field $\mathbb{Q}$. The main difficulty here is in getting a suitable free presentation for these modules. However, once that is obtained we will have a Theorem 4.6-like result for these modules.

Another direction would be to attempt to prove a sort of Kurihara's conjecture for global fields of positive characteristic and for various Iwasawa modules. In particular, the Tate module of 1-motives was also defined by Greither and Popescu (see [5]) in that setting.

Bibliography

[1] D. Burns. Congruences between derivatives of abelian L-functions at s = 0. *Invent. Math.*, 169 (3):459 – 499, 2007.

[2] D. Burns and C. Greither. On the Equivariant Tamigawa Number Conjecture for Tate Motives. *Invent. Math.*, 153 (2):303 – 359, 2003.

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

[4] M. Flach. The Equivariant Tamigawa Number Conjecture: a survey. In David Burns, Jonathan Sands, and David Solomon, editors, *Stark's Conjectures: Recent Work and New Directions*, volume 358 of *Contemporary Mathematics*. American Mathematics Society, 2004.

[5] C. Greither and C. Popescu. The Galois module structure of l-adic realizations of Picard 1-motives and applications. *Intl. Math. Res. Notices*, 5:986–1036, 2012.

[6] C. Greither and C. Popescu. An Equivariant Main Conjecture in Iwasawa Theory and Applications. *Journal of Algebraic Geometry*, 24:629–692, 2015.

[7] K. Iwasawa. On some invariants of cyclotomic fields. *American Journal of Mathematics*, 80:773–783, 1958.

[8] M. Kurihara. Iwasawa Theory and Fitting Ideals. *Journal fur die reine und angewandte Mathematik*, 561:39 – 86, 2003.

[9] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathbb{Q}$. *Invent. Math.*, 76:986–1036, 1984.

[10] J. Neukirch. *Algebraic Number Theory*. Springer, 1999.

[11] D. G. Northcott. *Finite Free Resolutions*. Cambridge University Press, 1976.

[12] C. Popescu. On the Coates-Sinnott Conjecture. *Mathematische Nachrichten*, 282:13701390, 2009.

[13] C. Popescu. Integral and p-adic refinements of the abelian stark conjecture. *Arithmetic of L–Functions, The IAS/Park City Mathematics Series*, 18:45–102, 2011.

[14] K. Rubin. Kolyvagin's System of Gauss Sums. In G. van der Geer, F. Oort, and J. Steenbrink, editors, *Arithmetic Algebraic Geometry*, volume 89 of *Progress in Mathematics*. Birkhauser, 1991.

[15] C.L. Siegel. *Über die Fourierschen Koeffizienten von Modulformen*. Nachrichten der Akademie der Wissenschaften in Göttingen. Vanderhoeck & Ruprecht, 1970.

[16] J. Tate. *Les conjectures de Stark sur les Fonctions L d'Artin en s = 0*, volume 47 of *Progress in Mathematics*. Birkhauser, 1984.

[17] L. Washington. *Introduction to Cyclotomic Fields*. Springer-Verlag, 1982.