An Introduction to Iwasawa Theory

Notes by Jim L. Brown

Contents

Chapter 1

Introduction

These notes are the course notes from a topics course in Iwasawa theory taught at the Ohio State University autumn term of 2006. They are an amalgamation of results found elsewhere with the main two sources being [Wash] and [Skinner]. The early chapters are taken virtually directly from [Wash] with my contribution being the choice of ordering as well as adding details to some arguments. Any mistakes in the notes are mine. There are undoubtably type-o's (and possibly mathematical errors), please send any corrections to jimlb@math.ohio-state.edu. As these are course notes, several proofs are omitted and left for the reader to read on his/her own time. The goal of the course was to give the students a feel for the arithmetic side of Iwasawa theory as much as possible with the clear goal of discussing the main conjecture. To this end, analytic arguments are generally omitted entirely. The students were assumed to be familiar with basic algebraic number theory and have been exposed to class field theory previously. Background material is presented, though in more of a fact gathering framework.

Classically Iwasawa theory was concerned with the study of sizes of class groups of cyclotomic fields and other related fields. More recent results are phrased in terms of "main conjectures" of Iwasawa theory. These main conjectures relate the sizes of class groups, or more generally Selmer groups, to p-adic L-functions. In these notes we will focus on the classical theory with the ultimate goals of proving Iwasawa's theorem about the sizes of class groups in $\mathbb{Z}_p$-extensions and stating the main conjecture of Iwasawa theory for totally real fields and outlining Wiles' proof. We now give a brief overview of the two main goals.

Let $K_n = \mathbb{Q}(\zeta_{p^n})$ for $n \geq 1$ and $K_\infty = \mathbb{Q}(\zeta_{p^\infty}) = \bigcup K_n$. Observe that $\mathrm{Gal}(K_\infty/\mathbb{Q}) \cong \mathbb{Z}_p^\times$ via the map $\sigma \mapsto a_\sigma \in \mathbb{Z}_p^\times$ where a_σ is determined by the equation $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{a_\sigma}$. Recall that one has an isomorphism

$$\mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p.$$

Set $\mathbb{Q}_\infty = K_\infty^{(\mathbb{Z}/p\mathbb{Z})^\times}$ so that

$$\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p.$$

The extension $\mathbb{Q}_\infty/\mathbb{Q}$ is what is called a $\mathbb{Z}_p$*-extension*. Let $\gamma \in \mathrm{Gal}(K_\infty/\mathbb{Q})$ be such that $\gamma \mapsto 1 + p \in \mathbb{Z}_p^\times$ in the above isomorphism. The image of γ in $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ is a topological generator and we still denote it as γ.

Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$ be a primitive Dirichlet character. We view χ as a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ via

$$\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times.$$

Let $\mathbb{Q}^\chi = \overline{\mathbb{Q}}^{\ker\chi}$ be the splitting field of χ. Observe this means that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^\chi) \cong \ker\chi$ and so χ can be viewed as a character of $\mathrm{Gal}(\mathbb{Q}^\chi/\mathbb{Q})$. One should note that often one will see $\mathbb{Q}^\chi$ written as $\mathbb{Q}_\chi$. We use the superscript notation to remind the reader this is the fixed field of $\ker\chi$ as well as to ease notation as we will often be dealing with the subscripts that arise in dealing with $\mathbb{Z}_p$-extensions as well.

Assume now that $\mathbb{Q}^\chi \cap \mathbb{Q}_\infty = \mathbb{Q}$. Set $F_\infty = \mathbb{Q}^\chi\mathbb{Q}_\infty$. We have $\mathrm{Gal}(F_\infty/\mathbb{Q}) \cong \Gamma \times \Delta$ where

$$\Delta = \mathrm{Gal}(F_\infty/\mathbb{Q}_\infty) \cong \mathrm{Gal}(\mathbb{Q}^\chi/\mathbb{Q})$$

so χ can be viewed as a character of Δ and

$$\Gamma = \mathrm{Gal}(F_\infty/\mathbb{Q}_\infty) \cong \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$$

so we view γ as an element of Γ.

There are fields $F_n \subset F_\infty$ that correspond to the subgroups Γ^{p^n} of Γ (and $\mathbb{Q}_n$ corresponding to the subgroups $p^n\mathbb{Z}_p$ of $\mathbb{Z}_p$) such that $\mathrm{Gal}(F_n/\mathbb{Q}^\chi) \cong \Gamma/\Gamma^{p^n} \cong \mathbb{Z}/p^n\mathbb{Z}$. Let L_n be the maximal unramified abelian p-extension of F_n. The group $X_n = \mathrm{Gal}(L_n/F_n)$ is isomorphic to A_n, the p-Sylow subgroup of the class group of F_n. Set $X = \mathrm{Gal}(L_\infty/F_\infty)$ so we have the following diagram of fields:

$$\begin{tikzcd}
& L_\infty \arrow[d, dash, "X"] & \\
& F_\infty \arrow[dl, dash, "\Gamma"'] \arrow[dr, dash, "\Delta"] & \\
\mathbb{Q}^\chi \arrow[dr, dash] & & \mathbb{Q}_\infty \arrow[dl, dash, "\mathbb{Z}_p"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Thus, X is a $\Delta \times \Gamma$-module. In fact, X is a $\mathbb{Z}_p[\![\Gamma]\!]$-module. One can show that $\mathbb{Z}_p[\![\Gamma]\!] \cong \Lambda := \mathbb{Z}_p[\![T]\!]$. Thus, X is a Λ-module. In fact, X is a finitely generated torsion Λ-module so has that there exists a Λ-module homormophism

$$X \to \left(\bigoplus_{i=1}^{r} \Lambda/p^{\mu_i}\right) \oplus \left(\bigoplus_{j=1}^{s} \Lambda/f_j(T)^{m_j}\right)$$

where the kernel and cokernel are Λ-modules of finite order, $\mu_i, m_j \geq 0$, and the $f_j(T)$ are irreducible monic polynomials in $\mathbb{Z}_p[T]$. The terms μ_i and the polynomial $f_X(T) = \prod f_j(T)^{m_j}$ are uniquely determined by X. The following theorem tells us exactly how the size of the p-part of the class group grows in a $\mathbb{Z}_p$-extension.

Theorem 1.1. *(Iwasawa's Theorem) Let p^{e_n} be the exact power of p dividing the class group of F_n. There exists integers $\lambda \geq 0$, $\mu \geq 0$, and ν all independent of n and $n_0 \in \mathbb{N}$ such that for $n \geq n_0$ one has*

$$e_n = \lambda n + \mu p^n + \nu.$$

Set $V = X \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p$. This is a finite dimensional vector space since $V \cong \overline{\mathbb{Q}}_p(T)/f_X(T)$. Set

$$V^\chi = \{v \in V : \sigma v = \chi(\sigma)v \ \ \forall \ \sigma \in \Delta\}.$$

This is the χ-isotypical piece of V. Let $f_\chi(T)$ be the characteristic polynomial of $\gamma - 1$ acting on V_χ. Note that $f_X(T)$ is the characteristic polynomial of $\gamma - 1$ acting on V so $f_\chi(T) \mid f_X(T)$. If instead of tensoring with $\overline{\mathbb{Q}}_p$ we tensored with $\mathcal{O}_\chi := \mathbb{Z}_p[\chi]$ we would also obtain a μ_χ term corresponding to the power of ϖ occurring where ϖ is a uniformizer of $\mathcal{O}_\chi$.

The main conjecture relates the characteristic polynomial $f_\chi(T)$ and μ_χ to a p-adic L-function and an analytic μ factor. Let ψ be any primitive Dirichlet character. Set

$$H_\psi(T) = \left\{ \begin{array}{cc} \psi(1+p)(1+T) - 1 & \psi = 1 \text{ or has conductor a power of } p \\ 1 & \text{otherwise.} \end{array} \right.$$

There exists $G_\psi(T) \in \mathcal{O}_\psi[\![T]\!]$ such that

$$\mathcal{L}_p(1-s, \psi) = G_\psi((1+p)^s - 1)/H_\psi((1+p)^s - 1) \qquad (s \in \mathbb{Z}_p)$$

such that

$$\mathcal{L}_p(1-n, \psi) = (1 - \psi\omega^{-n}(p)p^{n-1})L(1-n, \psi\omega^{-n}) \qquad (n \geq 1).$$

This is the "p-adic L-function" which we will discuss in more detail later. The Weierstrass preparation theorem states that we can write

$$G_\psi(T) = \varpi^{\mu_\psi^{\mathrm{an}}} g_\psi(T) u_\psi(T)$$

where $\mu_\psi^{\mathrm{an}} \geq 0$, $g_\psi(T)$ is a monic polynomial in $\mathcal{O}_\psi[T]$, and $u_\psi(T)$ is a unit in $\mathcal{O}_\psi[\![T]\!]$.

Theorem 1.2. *(Main Conjecture of Iwasawa Theory) Let χ be odd of order prime to p and assume $\mathbb{Q}^\chi \cap \mathbb{Q}_\infty = \mathbb{Q}$. Then*

$$f_\chi(T) = g_{\chi^{-1}\omega}((1+p)(1+T)^{-1} - 1)$$

and

$$\mu_\chi = \mu^{\mathrm{an}}_{\chi^{-1}\omega}.$$

We connect the main conjecture back to results on sizes of class groups by proving the following theorem.

Theorem 1.3. *Let p be an odd prime and let F be an abelian imaginary extension of $\mathbb{Q}$ of degree prime to p. Let $\chi : \mathrm{Gal}(F/\mathbb{Q}) \to \overline{\mathbb{Q}}_p^\times$ be an odd character. Suppose $\chi \neq \omega$, then*

$$|A_F^\chi| = |\mathcal{O}_\chi/(\mathcal{L}_p(0, \chi^{-1}\omega))|$$

where A_F^χ is the χ-isotypical piece of the p-part of the class group of F.

Chapter 2

Background Material

This chapter will contain a very brief review of some of the background material necessary to understand the material in this course. It is assumed that you have seen this material before and may need a quick refresher. If you are unfamiliar with any of the results you should consult [CF], [Milne1], or [Milne2].

2.1 Algebraic Number Theory

Let L/K be a finite extension of number fields with ring of integers $\mathcal{O}_L$ and $\mathcal{O}_K$ respectively.

Theorem 2.1. *Every non-zero proper ideal $\mathfrak{a} \subset \mathcal{O}_K$ admits a unique factorization*

$$\mathfrak{a} = \wp_1^{e_1} \cdots \wp_r^{e_r}$$

with $e_i > 0$ and the $\wp_i$ prime ideals.

Given a prime ideal $\wp \subset \mathcal{O}_K$, we can consider the ideal $\wp\mathcal{O}_L$ in $\mathcal{O}_L$. The previous theorem allows us to factor this ideal into a product of prime ideals:

$$\wp\mathcal{O}_L = \wp_1^{e_1} \cdots \wp_r^{e_r} \tag{2.1}$$

where the $\wp_i$ are prime ideals of $\mathcal{O}_L$. We make the following definition.

Definition 2.2. Given a factorization as in Equation 2.1, we call e_i the *ramification index of $\wp$ at $\wp_i$*. We denote the ramification index by $e(\wp_i/\wp)$. The prime $\wp$ is said to *ramify* in L if some $e_i > 1$. The *residue class degree of $\wp$ at $\wp_i$* is the dimension of the vector space $\mathcal{O}_L/\wp_i$ over $\mathcal{O}_K/\wp$. We denote the residue class degree by $f(\wp_i/\wp)$.

Proposition 2.3. *A prime $\wp$ in $\mathcal{O}_K$ ramifies in $\mathcal{O}_L$ if and only if $\wp | \operatorname{disc}(\mathcal{O}_L/\mathcal{O}_K)$.*

One has the following important theorem.

Theorem 2.4. *With the set-up as above,*

$$\sum_{i=1}^{r} e(\wp_i/\wp)f(\wp_i/\wp) = [L : K].$$

In these notes we will only be interested in the case where L/K is a Galois extension. This assumption allows us to simplify Theorem 2.4 considerably.

Corollary 2.5. *Suppose L/K is Galois and $0 \neq \wp \subset \mathcal{O}_K$ is a prime ideal. Then $e(\wp_i/\wp) = e(\wp_j/\wp)$ and $f(\wp_i/\wp) = f(\wp_j/\wp)$ for all i, j as in Equation 2.1. In particular, we have $[L : K] = ref$.*

This corollary follows immediately from the following proposition.

Proposition 2.6. *The Galois group $\mathrm{Gal}(L/K)$ acts transitively on the set of prime ideals $\wp_i$ of $\mathcal{O}_L$ lying over $\wp$.*

Proof. Suppose that $\sigma(\wp_i) \neq \wp_j$ for all $\sigma \in \mathrm{Gal}(L/K)$. The Chinese remainder theorem says that there exists $x \in \mathcal{O}_L$ such that $x \equiv 0(\operatorname{mod} \wp_i)$ and $x \equiv 1(\operatorname{mod} \sigma(\wp_j))$ for all $\sigma \in \mathrm{Gal}(L/K)$. Observe that the norm

$$\mathrm{N}_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$$

is in $\mathcal{O}_K \cap \wp_i = \wp$ since $\wp_i$ is a prime ideal and by definition the norm lands in $\mathcal{O}_K$. However, $x \notin \sigma(\wp_i)$ for any $\sigma \in \mathrm{Gal}(L/K)$, hence $\sigma(x) \notin \wp_j$ for any $\sigma \in \mathrm{Gal}(L/K)$. Thus, $\prod \sigma(x) \notin \mathcal{O}_K \cap \wp_j = \wp$, a contradiction. □

Definition 2.7. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_L$. The subgroup $D_\mathfrak{p} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{p}) = \mathfrak{p}\}$ is called the *decomposition group of $\mathfrak{p}$ over K.*

Proposition 2.6 gives the following Corollary.

Corollary 2.8. *For L/K as above we have:*
(a) $[\mathrm{Gal}(L/K) : D_\mathfrak{p}] = r$ *for any* $\mathfrak{p}|\wp$
(b) $D_\mathfrak{p} = 1$ *if and only if* $\wp\mathcal{O}_L$ *is totally split*
(c) $D_\mathfrak{p} = \mathrm{Gal}(L/K)$ *if and only if* $\wp\mathcal{O}_L = \mathfrak{p}^n$ *for* $n = [L : K]$
(d) $\#D_\mathfrak{p} = ef$

It is not difficult to see that one has a natural map $D_\mathfrak{p} \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{p})/(\mathcal{O}_K/\wp))$. It turns out that this map is also surjective ([Lang1], Proposition 14). This leads to the following definition.

Definition 2.9. The kernel $I_\mathfrak{p} \subseteq D_\mathfrak{p}$ of the homomorphism $D_\mathfrak{p} \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{p})/(\mathcal{O}_K/\wp))$ is called the *inertia group of $\mathfrak{p}$ over K.*

It is then clear from Corollary 2.8 that we have:

Corollary 2.10. *For L/K as above we have that $\#I_\mathfrak{p} = e$.*

Let $q = \#\mathcal{O}_K/\wp$. The theory of finite fields gives that for $\mathfrak{p}|\wp$ there is an automorphism $\overline{\sigma}_{\mathfrak{p}}$ of $\mathcal{O}_L/\mathfrak{p}$ fixing $\mathcal{O}_K/\wp$ given by $\overline{\sigma}_{\mathfrak{p}}(x) = x^q$. This is often referred to as the Frobenius automorphism. The isomorphism

$$D_{\mathfrak{p}}/I_{\mathfrak{p}} \cong \mathrm{Gal}((\mathcal{O}_L/\mathfrak{p})/(\mathcal{O}_K/\wp))$$

shows that we have a coset $\sigma_{\mathfrak{p}} I_{\mathfrak{p}}$ that corresponds to the Frobenius automorphism. Any element of this coset is called a *Frobenius automorphism of* $\mathfrak{p}$ and will be denoted $\mathrm{Frob}_{\mathfrak{p}}$. If $I_{\mathfrak{p}}$ is trivial, i.e., $\wp$ is unramified, then there is a well defined element $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$. It is of course important to be able to relate $\mathrm{Frob}_{\mathfrak{p}_1}$ to $\mathrm{Frob}_{\mathfrak{p}_2}$ for different primes $\mathfrak{p}_i|\wp$. We know that there exists $\tau \in \mathrm{Gal}(L/K)$ so that $\tau\mathfrak{p}_1 = \mathfrak{p}_2$. It is then easy to see that $D_{\mathfrak{p}_2} = \tau D_{\mathfrak{p}_1}\tau^{-1}$ and $\mathrm{Frob}_{\mathfrak{p}_2} = \tau \,\mathrm{Frob}_{\mathfrak{p}_1} \tau^{-1}$. If $\mathrm{Gal}(L/K)$ is abelian and $\wp$ unramified in L, we are able to associate a unique element in $\mathrm{Gal}(L/K)$ lying in $D_{\mathfrak{p}}$ for all $\mathfrak{p}|\wp$. We then call this element $\mathrm{Frob}_{\wp}$.

It will also be necessary to use the following fact on decomposition groups.

Proposition 2.11. *Let L/K be a finite Galois extension with $\wp$ a prime of K and $\mathfrak{p}$ a prime of L with $\mathfrak{p}|\wp$. There is an isomorphism $D_{\mathfrak{p}} \cong \mathrm{Gal}(L_{\mathfrak{p}}/K_{\wp})$ where $L_{\mathfrak{p}}$ and $K_{\wp}$ denote the completions.*

2.2 Cyclotomic Fields

In this section we recall some basic facts about cyclotomic fields. These number fields will be the primary focus of classical Iwasawa theory, so we give some of the relevant details in this section.

Definition 2.12. A *primitive n^{th} root of unity* is a number $\zeta_n \in \mathbb{C}$ such that $\zeta_n^n = 1$ but $\zeta_n^m \neq 1$ for every $0 < m < n$. The field $\mathbb{Q}(\zeta_n)$ is called the n^{th} *cyclotomic field.*

Exercise 2.13. *Show that ζ_n^m is a primitive n^{th} root of unity if and only if* $\gcd(m,n) = 1$.

Define the n^{th} cyclotomic polynomial $\Phi_n(x)$ by

$$\Phi_n(x) = \prod_{\substack{0<m<n\\(m,n)=1}} (x - \zeta_n^m).$$

Note that the roots of this polynomial are precisely the primitive n^{th} roots of unity. It is clear that we have $\deg(\Phi_n) = \varphi(n)$. It is also true that $\Phi_n(x) \in \mathbb{Q}[x]$. This can be seen by using the fact that

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{2.2}$$

and induction on n. Observe that $\Phi_n(\zeta_n) = 0$, so $\deg(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \leq \varphi(n)$. We also have that $\mathbb{Q}(\zeta_n)$ is Galois over $\mathbb{Q}$ since $\Phi_n(x)$ splits over $\mathbb{Q}(\zeta_n)$.

Applying Möbius inversion to Equation 2.2 we obtain

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}.$$

In particular, for $n = p^r$, one has

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1}.$$

Exercise 2.14. *Prove the following are equivalent:*
1. Φ *is irreducible over* $\mathbb{Q}$.
2. $\mathrm{Gal}(K/\mathbb{Q})$ *acts transitively on the roots of* Φ_n.
3. $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ *by* ($\sigma \mapsto m$ *such that* $\sigma(\zeta_n) = \zeta_n^m$).
4. $\#\,\mathrm{Gal}(K/\mathbb{Q}) = \varphi(n)$.

Lemma 2.15. *Suppose* $n = p^r$ *with* p *a prime. Then*
1. $\deg(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}) = \varphi(p^r) = p^r - p^{r-1}$.
2. $p\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = (1 - \zeta_{p^r})^{\varphi(p^r)}$ *and* $(1 - \zeta_{p^r})$ *is a prime of* $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$.
3. $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathbb{Z}[\zeta_{p^r}]$
4. $\Delta_{\mathbb{Q}(\zeta_{p^r})} = \pm p^{p^{r-1}(pr-r-1)}$.

Proof. First observe that clearly we have $\mathbb{Z}[\zeta_{p^r}] \subset \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$.
If ζ'_{p^r} is another $p^{r\,\mathrm{th}}$ root of unity, then there exists $s, t \in \mathbb{Z}$ such that $p \nmid st$ and $\zeta_{p^r} = (\zeta'_{p^r})^t$, $\zeta'_{p^r} = \zeta_{p^r}^s$. Thus $\mathbb{Q}(\zeta_{p^r}) = \mathbb{Q}(\zeta'_{p^r})$ and $\mathbb{Z}[\zeta_{p^r}] = \mathbb{Z}[\zeta'_{p^r}]$. Moreover,

$$\frac{1 - \zeta'_{p^r}}{1 - \zeta_{p^r}} = 1 + \zeta_{p^r} + \cdots + \zeta_{p^r}^{s-1} \in \mathbb{Z}[\zeta_{p^r}]$$

and similarly, $\dfrac{1 - \zeta_{p^r}}{1 - \zeta'_{p^r}} \in \mathbb{Z}[\zeta_{p^r}]$. Thus $\dfrac{1 - \zeta'_{p^r}}{1 - \zeta_{p^r}}$ is a unit in $\mathbb{Z}[\zeta_{p^r}]$, and hence is a unit in $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$.
Note

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = \frac{t^p - 1}{t - 1} = 1 + t + \cdots + t^{p-1}, \quad t = x^{p^{r-1}},$$

i.e., $\Phi_{p^r}(1) = p$.
Using the definitions we see that

$$\begin{aligned} \Phi_{p^r}(1) &= \prod (1 - \zeta'_{p^r}) \\ &= \prod \frac{1 - \zeta'_{p^r}}{1 - \zeta_{p^r}}(1 - \zeta_{p^r}) \\ &= u \cdot (1 - \zeta_{p^r})^{\varphi(p^r)} \end{aligned}$$

with u a unit in $\mathbb{Z}[\zeta_{p^r}]$. Therefore we have an equality of ideals in $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ given by $p\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = (1-\zeta_{p^r})^{\varphi(p^r)}$. Thus $p\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ has at least $\varphi(p^r)$ prime factors in $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$. Therefore we have $\deg(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}) \geq \varphi(p^r)$. But we already had that $\deg(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}) \leq \varphi(p^r)$, therefore we have that

$$\deg(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}) = \varphi(p^r) = p^r - p^{r-1}.$$

Observe that we also have that $(1-\zeta_{p^r})$ must generate a prime ideal for otherwise we would have too many prime factors of $p\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$. This gives us part 2.
Now we compute (up to sign) $\mathrm{disc}(\mathbb{Z}[\zeta_{p^r}]/\mathbb{Z})$. We have the formula (see for example [Milne1], Prop. 2.33)

$$\mathrm{disc}(\mathbb{Z}[\zeta_{p^r}]/\mathbb{Z}) = \pm\, \mathrm{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\Phi'_{p^r}(\zeta_{p^r})).$$

To get $\Phi'_{p^r}(\zeta_{p^r})$, we differentiate $(x^{p^{r-1}}-1)\Phi_{p^r}(x) = x^{p^r}-1$ and substitute $x=\zeta_{p^r}$ to get $\Phi'_{p^r}(\zeta_{p^r}) = \dfrac{p^r\zeta_{p^r}^{p^r-1}}{\zeta_{p^r}^{p^{r-1}}-1}$. Clearly we have that

$$\mathrm{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}) = \pm 1$$

and

$$\mathrm{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(p^r) = (p^r)^{\varphi(p^r)} = p^{r\varphi(p^r)}.$$

Claim: $\mathrm{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_{p^r}^{p^s}) = p^{p^s}, \quad 0 \leq s < r.$

Pf: The minimal polynomial of $1-\zeta_{p^r}$ is $\Phi_{p^r}(1-x)$, which has a constant term of $\Phi_{p^r}(1) = p$, so $\mathrm{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_{p^r}) = \pm p$. Now let $s<r$, $\zeta_{p^r}^{p^s}$ is a primitive $p^{(r-s)\mathrm{th}}$ root of unity, so the computation we just did with r replaced by $r-s$ gives $\mathrm{N}_{\mathbb{Q}(\zeta_{p^r}^{p^s})/\mathbb{Q}}(1-\zeta_{p^r}^{p^s}) = \pm p$. Now using that $\mathrm{N}_{M/K} = \mathrm{N}_{L/K}\circ \mathrm{N}_{M/L}$ for fields $K \subset L \subset M$ and the fact that $\mathrm{N}_{M/L}(\alpha) = \alpha^{[M:L]}$ if $\alpha \in L$, we obtain

$$\mathrm{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_{p^r}^{p^s}) = p^a$$

where

$$a = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}(\zeta_{p^r}^{p^s})] = \varphi(p^r)/\varphi(p^{r-s}) = p^s. \qquad \square$$

Thus we have $\mathrm{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\Phi'_{p^r}(\zeta_{p^r})) = \pm p^c$ where $c = p^{r-1}(pr-r-1)$. So we have that $\mathrm{disc}(\mathbb{Z}[\zeta_{p^r}]/\mathbb{Z})$ is a power of p. Hence $\mathrm{disc}(\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}/\mathbb{Z})$ is a power of p using the formula $\mathrm{disc}(\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}/\mathbb{Z})[\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} : \mathbb{Z}[\zeta_{p^r}]]^2 = \mathrm{disc}(\mathbb{Z}[\zeta_{p^r}]/\mathbb{Z})$ ([Milne1], Remark 2.24)

We also have that $[\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} : \mathbb{Z}[\zeta_{p^r}]]$ is a power of p, and hence $p^M(\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}/\mathbb{Z}[\zeta_{p^r}]) = 0$ for some M, i.e., $p^M\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} \subseteq \mathbb{Z}[\zeta_{p^r}]$. Now we use that for $\mathfrak{p} = (1-\zeta_{p^r})$ we have $f(\mathfrak{p}/p) = 1$ to get that the map

$$\mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}/(1-\zeta_{p^r})$$

is an isomorphism. Thus $\mathbb{Z} + (1-\zeta_{p^r})\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ and so

$$\mathbb{Z}[\zeta_{p^r}] + (1-\zeta_{p^r})\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}. \tag{2.3}$$

This gives

$$(1-\zeta_{p^r})\mathbb{Z}[\zeta_{p^r}] + (1-\zeta_{p^r})^2\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = (1-\zeta_{p^r})\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}. \tag{2.4}$$

Now let $\alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$. Then Equation 2.3 gives that $\alpha = \alpha' + \gamma$ with $\alpha' \in (1-\zeta_{p^r})\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ and $\gamma \in \mathbb{Z}[\zeta_{p^r}]$, and Equation 2.4 gives $\alpha' = \alpha'' + \gamma'$ with $\alpha'' \in (1-\zeta_{p^r})^2\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ and $\gamma' \in \mathbb{Z}[\zeta_{p^r}]$. Thus $\alpha = (\gamma + \gamma') + \alpha''$. So we get

$$\mathbb{Z}[\zeta_{p^r}] + (1-\zeta_{p^r})^2\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}.$$

We can iterate this to get $\mathbb{Z}[\zeta_{p^r}] + (1-\zeta_{p^r})^m\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ for $m \in \mathbb{N}$. Since $(1-\zeta_{p^r})^{\varphi(p^r)} = p \cdot \text{unit}$, we have $\mathbb{Z}[\zeta_{p^r}] + p^m\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ for all $m \in \mathbb{N}$. However, for large enough m, $p^m\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} \subseteq \mathbb{Z}[\zeta_{p^r}]$. Thus $\mathbb{Z}[\zeta_{p^r}] = \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$, i.e., part 3 holds. Combining this with the above computation of $\operatorname{disc}(\mathbb{Z}[\zeta_{p^r}]/\mathbb{Z})$ gives part 4 as well. □

We now generalize to the case of general n.

Proposition 2.16. *Let ζ_n be a primitive n^{th} root of unity and let $K = \mathbb{Q}(\zeta_n)$. Then we have:*
1. $\deg(K/\mathbb{Q}) = \varphi(n)$
2. $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$
3. The prime p ramifies in K if and only if $p \mid n$ (unless $n = 2 \cdot odd$ and $p = 2$); in particular, if $n = p^r m$ with $\gcd(p, m) = 1$*, then*

$$p\mathcal{O}_K = (\mathfrak{p}_1 \dots \mathfrak{p}_s)^{\varphi(p^r)}$$

in K with the $\mathfrak{p}_i$ distinct primes in K.

Proof. We proceed by induction on the number of primes dividing n. Consider the fields:

$$\begin{tikzcd}
 & K = \mathbb{Q}(\zeta_n) \arrow[dl, no head] \arrow[dr, no head] & \\
E = \mathbb{Q}(\zeta_{p^r}) \arrow[dr, no head] & & F = \mathbb{Q}(\zeta_m) \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}$$

We look at how p factors in E and F:
$p\mathcal{O}_E = \mathfrak{p}^{\varphi(p^r)}$ is totally ramified as given in the previous theorem.
$p\mathcal{O}_F = \mathfrak{p}_1 \dots \mathfrak{p}_r$ is unramified since p is relatively prime to the discriminant.

Now we can consider the factorization of p in $\mathcal{O}_K$ by going up the tower in two different ways. This shows that we must have $\deg(K/F) = \varphi(p^r)$ and that

$$p\mathcal{O}_K = (\prod \mathfrak{q}_i)^{\varphi(p^r)}$$

where

$$\mathfrak{p}_i\mathcal{O}_K = \mathfrak{q}_i^{\varphi(p^r)}$$

and

$$\mathfrak{p}\mathcal{O}_K = \prod \mathfrak{q}_i.$$

Therefore we have that $\deg(K/\mathbb{Q}) = \varphi(p^r)\varphi(m) = \varphi(n)$ and we have part 1. To finish the proof, we note the following lemma. □

Lemma 2.17. *([Milne1], Lemma 6.5) Let K and L be finite extensions of $\mathbb{Q}$ such that*

$$[KL : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}],$$

and let $d = \gcd(\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}), \mathrm{disc}(\mathcal{O}_L/\mathbb{Z}))$. Then

$$\mathcal{O}_{KL} \subset d^{-1}\mathcal{O}_K\mathcal{O}_L.$$

Remark 2.18. Note that since $\varphi(p^r) = p^{r-1}(p-1)$, if $n = 2\cdot$(odd number)and $p = 2$ then it will happen that 2 divides n but does not ramify. One should also note that $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$ if n in this case.

Remark 2.19. Let $K = \mathbb{Q}(\zeta_p)$. The only roots of unity in K are those ζ_p^s for $1 \leq s \leq p-1$. This follows immediately from the fact that $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ if $\gcd(m, n) = 1$.

We can say a little more about how a prime p splits in $\mathbb{Q}(\zeta_n)$ if $p \nmid n$. First we need the following lemma.

Lemma 2.20. *Let p be a prime so that $p \nmid n$. Let $\mathfrak{p}$ be a prime of $\mathbb{Q}(\zeta_n)$ lying over p. Then the n^{th} roots of unity are distinct modulo $\mathfrak{p}$.*

Proof. This lemma follows immediately from the equation:

$$n = \prod_{j=1}^{n-1}(1 - \zeta_n^j).$$

□

Note that this result does not hold for $p \mid n$. In particular, in $\mathbb{Q}(\zeta_p)$ one has

$$\zeta_p \equiv 1(\mathrm{mod}(1 - \zeta_p)).$$

Lemma 2.21. *Let p be a prime so that $p \nmid n$. Let f be the smallest positive integer so that $p^f \equiv 1(\mathrm{mod}\, n)$. Then p splits into $\varphi(n)/f$ distinct primes in $\mathbb{Q}(\zeta_n)$, each of residue class degree f. In particular, p is completely split if and only if $p \equiv 1(\mathrm{mod}\, n)$.*

Proof. Let $\mathfrak{p}$ be a prime of $\mathbb{Q}(\zeta_n)$ that lies over p. Recall from the previous section the Frobenius automorphism of $\mathbb{Q}(\zeta_n)$ that is defined by

$$\sigma_{\mathfrak{p}}(x) \equiv x^p (\operatorname{mod} \mathfrak{p})$$

for all $x \in \mathbb{Z}[\zeta_n]$. We know that $\sigma_{\mathfrak{p}}(\zeta_n)$ is again an n^{th} root of unity. Therefore, we can apply Lemma 2.20 to conclude that not only is $\sigma_{\mathfrak{p}}(\zeta_n) \equiv \zeta_n^p (\operatorname{mod} \mathfrak{p})$, but in fact $\sigma_{\mathfrak{p}}(\zeta_n) = \zeta_n^p$. We also have that the order of $\sigma_{\mathfrak{p}}$ is the degree of the residue class extension of $(\mathbb{Z}[\zeta_n]/\mathfrak{p}\mathbb{Z}[\zeta_n])/(\mathbb{Z}/p\mathbb{Z})$. Thus

$$p^f \equiv 1 (\operatorname{mod} n) \Leftrightarrow \zeta_n^{p^f} = \zeta_n \Leftrightarrow \sigma_{\mathfrak{p}}^f = 1.$$

Recalling that the degree of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is equal to the degree of the residue class extension multiplied by the number of primes above p, we have the result. □

2.3 Infinite Galois Theory

It will often be necessary to talk about field extensions of infinite degree as well as the corresponding Galois groups. We collect some basic facts here to remind the reader of the similarities and differences between the Galois theory of infinite extensions and the more familiar finite extensions.

Let K/k be a Galois extension of fields. As is custom, we write $\operatorname{Gal}(K/k)$ to denote the set of automorphisms of K that leave k fixed pointwise. Let F be a field so that $k \subseteq F \subseteq K$ with F/k a finite extension. In particular, we have that $\operatorname{Gal}(K/F)$ is of finite index in $\operatorname{Gal}(K/k)$. We define a topology on $\operatorname{Gal}(K/k)$ by letting the sets $\operatorname{Gal}(K/F)$ form a basis of the neighborhoods of the identity in $\operatorname{Gal}(K/k)$. With this topology one has that $\operatorname{Gal}(K/k)$ is profinite and

$$\operatorname{Gal}(K/k) \cong \varprojlim_F \operatorname{Gal}(K/k)/\operatorname{Gal}(K/F) \cong \varprojlim_F \operatorname{Gal}(F/k)$$

where F is running through the finite normal subextensions F/k or any subsequence so that $\cup F = K$. The ordering used is that of inclusion and the maps are the natural maps $\operatorname{Gal}(F_2/k) \to \operatorname{Gal}(F_1/k)$ for $F_1 \subseteq F_2$. In this setting the fundamental theorem of Galois theory reads:

Theorem 2.22. *Let K/k be a Galois extension. There is a 1-1 correspondence between closed subgroups H of $\operatorname{Gal}(K/k)$ and fields F with $k \subseteq F \subseteq K$ such that*

$$H \leftrightarrow K^H$$

$$\operatorname{Gal}(K/L) \leftrightarrow L.$$

Open subgroups correspond to finite extensions.

Example 2.23. Let $\mathbb{Q}(\zeta_{p^\infty})$ be the extension of $\mathbb{Q}$ obtained by adjoining all p-power roots of unity. This extension will be very important to us as it is used to produce the $\mathbb{Z}_p$-extension of $\mathbb{Q}$. An element of $\operatorname{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ is completely determined by its action on the p-power roots of unity. Let $n \in \mathbb{N}$. For $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ we have $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\sigma_n}$ for some $\sigma_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Observe that $\sigma_n \equiv \sigma_{n-1} (\operatorname{mod} p^{n-1})$ for all $n \geq 1$. In particular, this shows we obtain an element of

$$\mathbb{Z}_p^\times \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}).$$

Conversely, it is easy to see that given $\alpha \in \mathbb{Z}_p^\times$ one gets an element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ given by the action $\sigma(\zeta_{p^n}) = \zeta_{p^n}^\alpha$. Thus we have $\mathbb{Z}_p^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$. One should also note that the closed subgroup $1 + p^n\mathbb{Z}_p$ corresponds to its fixed field $\mathbb{Q}(\zeta_{p^n})$.

Exercise 2.24. *Let $\mathbb{F}$ be a finite field and $\overline{\mathbb{F}}$ its algebraic closure. Prove that $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}) \cong \hat{\mathbb{Z}}$.*

Let K/k be a Galois extension, not necessarily finite. Let $\mathcal{O}_K$ and $\mathcal{O}_k$ be the rings of integers of K and k respectively. We would like to discuss the ramification of prime ideals as we did in the case of finite extensions. Unfortunately, it is not true in general that $\mathcal{O}_K$ and $\mathcal{O}_k$ are even Dedekind domains.

Exercise 2.25. *Show that for $K = \mathbb{Q}(\zeta_{p^\infty})$, $\mathcal{O}_K$ is not a Dedekind domain. It may be helpful to consider the prime ideal $\mathfrak{p} = (\zeta_p - 1, \zeta_{p^2} - 1, \dots)$ and its p^{th} power.*

Since it is not possible to define the ramification of a prime in terms of its prime factorization, we must find a new way. Recall that in the case of finite extensions, if e is the ramification index of some prime ideal $\wp$ at $\mathfrak{p}$, then we have $e = \#I_{\mathfrak{p}}$ where $I_{\mathfrak{p}}$ is the inertia group. We can use this fact to find a way of defining ramification in infinite extensions.

As in the finite case, define the decomposition group $D_{\mathfrak{p}}$ of a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ lying over $\wp \subset \mathcal{O}_k$ by

$$D_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(K/k) : \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

The inertia group $I_{\mathfrak{p}}$ is defined by

$$I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} : \sigma(\alpha) \equiv \alpha (\operatorname{mod} \mathfrak{p}) \text{ for all } \alpha \in \mathcal{O}_K\}.$$

One can show that $D_{\mathfrak{p}}$ and $I_{\mathfrak{p}}$ are both closed subgroups of $\mathrm{Gal}(K/k)$. We now define the ramification index of $\wp$ at $\mathfrak{p}$ to be $e = \#I_{\mathfrak{p}}$.

The situation for infinite places is a little different. However, it turns out that in the infinite case that e is always 1 or 2. In fact, $I_{\mathfrak{p}}$ is nontrivial in the infinite case only when $\wp$ is real and $\mathfrak{p}$ is complex. In this case the inertia group is generated by complex conjugation.

2.4 Class Field Theory

Class field theory provides a description of abelian extensions of number fields. For those unfamiliar with the subject or those needing a more thorough refresher then that provided here are encouraged to consult [CF] or [Milne2]. We provide here only a statement of results and only those results we will need in this course. We begin by recalling the statements of global class field theory in terms of ideals before treating the statements in the language of ideles. Finally, we give the statements of local class field theory. The interested reader should note that the statements and applications of class field theory are in general much more important and useful then the proofs of the statements.

2.4.1 Global Class Field Theory (ideals)

Let k be a number field and let $I = I_k$ be the group of fractional ideals of k. Let S be a finite set of places of k and I^S the subgroup of I generated by the prime ideals not in S. Let $\mathfrak{m}_f = \prod \wp_i^{e_i}$ be an integral ideal of k and $\mathfrak{m}_\infty$ be a square-free product of real archimedean places of k. We call $\mathfrak{m} = \mathfrak{m}_f\mathfrak{m}_\infty$ a *divisor* of k. For $\alpha \in \mathcal{O}_k$, we write $\alpha \equiv 1(\text{mod}^*\, \mathfrak{m})$ if (1) $v_{\wp_i}(\alpha - 1) \geq e_i$ for all primes $\wp_i | \mathfrak{m}_f$ and (2) $\alpha > 0$ for all the real primes dividing $\mathfrak{m}_\infty$. Set $P_{\mathfrak{m},1}$ to be the set of principal ideals of $\mathcal{O}_k$ that are generated by an element α so that $\alpha \equiv 1(\text{mod}^*\, \mathfrak{m})$. We write $S(\mathfrak{m})$ to denote the primes dividing $\mathfrak{m}$.

Definition 2.26. Let $\mathfrak{m}$ be a divisor of k. The group $C_\mathfrak{m} = I^{S(\mathfrak{m})}/P_{\mathfrak{m},1}$ is called the *ray class group of k modulo* $\mathfrak{m}$.

Theorem 2.27. *([Milne2]) Let $\mathfrak{m} = \prod \wp^{m(\mathfrak{p})}$ be a divisor of k. There is an exact sequence*

$$0 \longrightarrow U/U_{\mathfrak{m},1} \longrightarrow P_\mathfrak{m}/P_{\mathfrak{m},1} \longrightarrow C_\mathfrak{m} \longrightarrow C \longrightarrow 0 \tag{2.5}$$

and canonical isomorphisms

$$P_\mathfrak{m}/P_{\mathfrak{m},1} \cong \prod_{\substack{\wp|\infty \\ \wp|\mathfrak{m}}} \{\pm\} \times \prod_{\substack{\wp\nmid\infty \\ \wp|\mathfrak{m}}} (\mathcal{O}_k/\wp^{m(\wp)})^\times \cong \prod_{\substack{\wp|\infty \\ \wp|\mathfrak{m}}} \{\pm\} \times (\mathcal{O}_k/\mathfrak{m}_f)^\times,$$

where

$$\begin{aligned} P_\mathfrak{m} &= \{\alpha \in k^\times : \text{ord}_\wp(\alpha) = 0 \textit{ for all } \wp \mid \mathfrak{m}_f\}, \\ U &= \mathcal{O}_k^\times, \\ U_{\mathfrak{m},1} &= U \cap P_{\mathfrak{m},1}. \end{aligned}$$

Example 2.28. Let $\mathfrak{m} = 1$. In this case the ray class group $C_\mathfrak{m}$ is nothing more then the familiar ideal class group C.

Example 2.29. Let $n \in \mathbb{N}$ and set $\mathfrak{m} = n$. In this case we see that $I^{S(\mathfrak{m})}$ is the set of ideals generated by rational numbers relatively prime to n. If $(x) \in P_{\mathfrak{m},1}$, then we must have $x \equiv 1(\operatorname{mod} n)$ and $x > 0$. The exact sequence becomes

$$0 \longrightarrow \{\pm 1\} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^{\times} \longrightarrow C_{\mathfrak{m}} \longrightarrow 0.$$

Thus, we see that the ray class group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{\times}/\{\pm\}$.

Exercise 2.30. *Compute $I^{S(\mathfrak{m})}/P_{\mathfrak{m},1}$ for $k = \mathbb{Q}$ and $\mathfrak{m} = n$.*

Let K be a finite Galois extension of k. Further assume that K/k is abelian, i.e., $\operatorname{Gal}(K/k)$ is an abelian group. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ and $\wp$ a prime of $\mathcal{O}_k$ with $\mathfrak{p}|\wp$. Recall from Section 2.1 that if $\wp$ is unramified in K then there is a well defined Frobenius element $\operatorname{Frob}_{\wp}$ in $\operatorname{Gal}(K/k)$. Let S be the set of prime ideals in k that ramify in K. We can define the *Artin map*

$$\psi_{K/k} : I^S \to \operatorname{Gal}(K/k)$$

to be the map defined by

$$\psi_{K/k}(\wp_1^{e_1} \cdots \wp_r^{e_r}) = \prod_{i=1}^{r} \operatorname{Frob}_{\wp_i}^{e_i}.$$

Recall that one has a norm map $\operatorname{Nm}_{K/k} : I_K \to I_k$ defined by $\operatorname{Nm}_{K/k}(\mathfrak{p}) = \wp^{f(\mathfrak{p}/\wp)}$ where $\wp = \mathfrak{p} \cap \mathcal{O}_k$. The following proposition follows from basic properties of the Frobenius element and how it behaves with respect to field extensions.

Proposition 2.31. *Let L be an abelian extension of k so that $k \subset K \subset L$ and let S be any finite set of primes of k containing all those that ramify in L and also the primes of K lying over primes of k in S. The following diagram commutes:*

$$\begin{tikzcd}
I_K^S \arrow[r, "\psi_{L/K}"] \arrow[d, "\operatorname{Nm}_{K/k}"] & \operatorname{Gal}(L/K) \arrow[d, "\text{inclusion}"] \\
I_k^S \arrow[r, "\psi_{L/k}"] & \operatorname{Gal}(L/k).
\end{tikzcd}$$

Corollary 2.32. *Let L be an abelian extension of k. Then*

$$\operatorname{Nm}_{L/k}(I_L^S) \subset \ker(\psi_{L/k} : I^S \to \operatorname{Gal}(L/k)).$$

Definition 2.33. Let $\psi : I^S \to G$ be a group homomorphism. We say ψ *admits a divisor* if there exists a divisor $\mathfrak{m}$ of k so that $S(\mathfrak{m}) \subset S$ and $\psi(P_{\mathfrak{m},1}) = 1$, i.e., ψ admits a divisor if and only if it factors through $C_{\mathfrak{m}}$.

Theorem 2.34. *(Reciprocity Law) Let K be a finite abelian extension of k and let S be the set of primes of k ramifying in K. The Artin map $\psi_{K/k} : I^S \rightarrow$ $\mathrm{Gal}(K/k)$ admits a divisor $\mathfrak{m}$ with $S(\mathfrak{m}) = S$ and defines an isomorphism*

$$I_k^S / P_{\mathfrak{m},1} \operatorname{Nm}_{K/k}(I_K^S) \cong \mathrm{Gal}(K/k).$$

One should note that this theorem does not imply that any abelian extensions of k exist. It merely states that if you already have an abelian extension that it is a quotient of the ray class group by a particular subgroup, namely, the image of I_K^S under the norm map.

Definition 2.35. We say a subgroup $H \subset I_k^{S(\mathfrak{m})}$ is a *congruence subgroup modulo* $\mathfrak{m}$ if $P_{\mathfrak{m},1} \subset H \subset I_k^{S(\mathfrak{m})}$.

Theorem 2.36. *Let H be a congruence subgroup of $I_k^{S(\mathfrak{m})}$. There exists a unique abelian extension K/k with its only possible ramification being at the primes dividing $\mathfrak{m}$ such that $H = P_{\mathfrak{m},1} \operatorname{Nm}_{K/k}(I_K^{S(\mathfrak{m})})$ and $I_k^{S(\mathfrak{m})}/H \cong \mathrm{Gal}(K/k)$ under the Artin map.*

Note that this theorem shows that given H the associated field K is such that
1. K is a finite abelian extension of k
2. $m(\wp) = 0$ implies that $\wp$ is not ramified in K
3. the prime ideals not in $S(\mathfrak{m})$ that split in K are precisely those contained in H.

Observe that if one is given a divisor $\mathfrak{m}$ one can set $H = P_{\mathfrak{m},1}$ and use the theorem to conclude there exists a field $K_{\mathfrak{m}}$ so that $C_{\mathfrak{m}} \cong \mathrm{Gal}(K_{\mathfrak{m}}/k)$. This field $K_{\mathfrak{m}}$ is called the *ray class field.* Note that the primes of k that ramify in $K_{\mathfrak{m}}$ are precisely the primes dividing $\mathfrak{m}$. If we choose $\mathfrak{m} = 1$ then we obtain $C_{\mathfrak{m}} = C$ as noted above. In this case we call the associated ray class field the *Hilbert class field.* The Hilbert class field is the maximal unramified abelian extension of the field K. We will generally denote the Hilbert class field of a field K by H_K.

For a field $K \subset K_{\mathfrak{m}}$, set $\operatorname{Nm}(C_{K,\mathfrak{m}}) = P_{\mathfrak{m},1} \operatorname{Nm}_{K/k}(I_K^{S(\mathfrak{m})}) (\operatorname{mod} P_{\mathfrak{m},1})$. We then have the following corollary classifying abelian extensions.

Corollary 2.37. *Fix a divisor $\mathfrak{m}$. The map $K \rightarrow \operatorname{Nm}(C_{K,\mathfrak{m}})$ is a bijection from the set of abelian extensions of k contained in $K_{\mathfrak{m}}$ to the set of subgroups of $C_{\mathfrak{m}}$. We also have the following:*

$$\begin{aligned} K_1 \subset K_1 \quad &\Leftrightarrow \quad \operatorname{Nm}(C_{K_1,\mathfrak{m}}) \supset \operatorname{Nm}(C_{K_2,\mathfrak{m}}) \\ \operatorname{Nm}(C_{K_1K_2,\mathfrak{m}}) \quad &= \quad \operatorname{Nm}(C_{K_1,\mathfrak{m}}) \cap \operatorname{Nm}(C_{K_1,\mathfrak{m}}) \\ \operatorname{Nm}(C_{K_1 \cap K_2,\mathfrak{m}}) \quad &= \quad \operatorname{Nm}(C_{K_1,\mathfrak{m}}) \operatorname{Nm}(C_{K_2,\mathfrak{m}}). \end{aligned}$$

We end this section with a couple of applications that will be useful in these notes. Let K/E be a Galois extension of number fields. We know from our discussion above that for a field K we have $C_K \cong \mathrm{Gal}(H_K/K)$ as groups where we include the K in the notation for the ideal class group to avoid any confusion. We now show that they are in fact isomorphic as $\mathrm{Gal}(K/E)$-modules. Observe that we have an action of $\mathrm{Gal}(K/E)$ on $\mathrm{Gal}(H_K/K)$ given as follows. Let $\tau \in \mathrm{Gal}(K/E)$ and $\sigma \in \mathrm{Gal}(H_K/K)$. Extend τ to $\mathrm{Gal}(H_K/K)$ and denote this extension by $\tilde{\tau}$. The action is then given by $\tau \cdot \sigma = \tilde{\tau}\sigma\tilde{\tau}^{-1}$. Let $\wp$ be a prime ideal of K. Under the Artin map $\wp \mapsto \mathrm{Frob}_{\wp}$. Thus, we have that $\tau\wp$ maps to $\mathrm{Frob}_{\tau\wp} = \tilde{\tau}\,\mathrm{Frob}_{\wp}\,\tilde{\tau}^{-1} = \tau \cdot \mathrm{Frob}_{\wp}$ as desired.

With K and E as above, assume that $H_E \cap K = E$. We wish to show that the norm map $C_K \to C_E$ on ideal class groups is surjective and the following diagram commutes:

$$\begin{tikzcd}
C_K \arrow[r, "\sim"] \arrow[d, "\mathrm{Norm}"'] & \mathrm{Gal}(H_K/K) \arrow[d, "\mathrm{rest.}"] \\
C_E \arrow[r, "\sim"] & \mathrm{Gal}(H_E/E).
\end{tikzcd}$$

First note that since $H_E \cap K = E$ we have that $\mathrm{Gal}(H_E K/K) \cong \mathrm{Gal}(H_E/E)$ and since $H_E K \subset H_K$, we obtain that the map $\mathrm{Gal}(H_K/K) \to \mathrm{Gal}(H_E/E)$ is onto. Therefore, if we can show the diagram commutes we will have that the norm map on the ideal class groups is surjective. We leave the proof of the fact that the diagram commutes as an exercise. It is merely an exercise in keeping track of how the Frobenius acts, one that should be done though!

Exercise 2.38. *Prove the diagram above commutes.*

2.4.2 Local Class Field Theory

We would like to treat global class field theory from the idelic viewpoint. However, before we do that we need to review local class field theory.

Let k be a local field and let k^{ab} be the maximal abelian extension of k. The theorems of local class field theory are as follows.

Theorem 2.39. *(Local Reciprocity Law) For any nonarchimedian local field k there is a unique homomorphism*

$$\varphi_k : k^{\times} \longrightarrow \mathrm{Gal}(k^{\mathrm{ab}}/k)$$

such that
1. for any prime ϖ of k and any finite unramified extension K of k, $\varphi_k(\varpi) \mid_K = \mathrm{Frob}_{K/k}$;
2. for any finite abelian extension K of k, $\mathrm{Nm}_{K/k}(K^{\times})$ is contained in the kernel of $x \mapsto \varphi_k(x) \mid_K$ and φ_k induces an isomorphism

$$\varphi_{K/k} : k^{\times}/\,\mathrm{Nm}_{K/k}(K^{\times}) \xrightarrow{\simeq} \mathrm{Gal}(K/k);$$

3. one has

$$\mathcal{O}_k^{\times}/\bigcap_{L} \mathrm{Nm}_{L/k}(\mathcal{O}_L^{\times}) \cong I(K/k)$$

where $I(K/k)$ is the inertia subgroup of $\mathrm{Gal}(K/k)$ *and L runs through all finite subextensions of K/k.*

The maps φ_k and $\varphi_{K/k}$ are referred to as the *local Artin maps.* Note that part (2) of the local reciprocity theorem gives the following commutative diagram:

$$\begin{tikzcd}
k^\times \arrow[r, "\varphi_k"] \arrow[d] & \mathrm{Gal}(k^{\mathrm{ab}}/k) \arrow[d, "\tau\mapsto\tau|_L"] \\
k^\times/\,\mathrm{Nm}_{K/k}(K^\times) \arrow[r, "\varphi_{K/k}"] & \mathrm{Gal}(K/k)
\end{tikzcd}$$

Theorem 2.40. *(Local Existence Theorem) A subgroup N of $k^\times$ is of the form* $\mathrm{Nm}_{K/k}(K^\times)$ *for some finite abelian extension K of k if and only if it is of finite index and open.*

Corollary 2.41. *The map $K \mapsto \mathrm{Nm}(K^\times)$ is a bijection from the set of finite abelian extensions of k to the set of open subgroups of finite index in $k^\times$. Moreover, one has*

$$\begin{aligned}
K_1 \subset K_1 &\Leftrightarrow \mathrm{Nm}(K_1^\times) \supset \mathrm{Nm}(K_2^\times)\\
\mathrm{Nm}((K_1 \cdot K_2)^\times) &= \mathrm{Nm}(K_1^\times) \cap \mathrm{Nm}(K_1^\times)\\
\mathrm{Nm}((K_1 \cap K_2)^\times) &= \mathrm{Nm}(K_1^\times)\,\mathrm{Nm}(K_2^\times).
\end{aligned}$$

2.4.3 Global Class Field Theory (ideles)

We now give the theorems of global class field theory in terms of ideles. The formulation in terms of ideles allows one to study all places at once as well as to look at infinite degree field extensions. The idelic version also makes clear the relationship betweeen the global and local theories. The material in this subsection as well as a review of ideles can be found in [Milne2].

Let k be a number field. Recall that the group of ideles is defined to be

$$\mathbb{A}_k^\times = \{(x_v) \in \prod k_v^\times \mid x_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v\}.$$

Let S be a finite set of primes that contain all the archimedean primes. We write $\mathbb{A}_{k,S}^\times$ to denote

$$\prod_{v\in S} k_v^\times \times \prod_{v\notin S} \mathcal{O}_v^\times.$$

We put a topology on $\mathbb{A}_k^\times$ so that $\mathbb{A}_{k,S}^\times$ is open for all such S. This is accomplished by declaring sets of the form

$$\prod_v U_v = \begin{cases} U_v & \text{open in } k_v^\times \text{ for all } v;\\ U_v = \mathcal{O}_v^\times & \text{for almost all } v \end{cases}$$

to be open sets.

Recall that k embeds in $\mathbb{A}_k^\times$ via the diagonal embedding. This allows one to define the *idele class group* $\mathbf{C}_k$ *of* k to be $\mathbb{A}_k^\times/k$. Note that there is also a canonical surjective homomorphism

$$\begin{array}{rcl} id : \mathbb{A}_k^\times & \to & I_k \\ (x_v) & \mapsto & \prod_{v\nmid\infty} p_v^{\mathrm{ord}_{\mathfrak{p}}(x_v)} \end{array}$$

with kernel $\mathbb{A}_{k,S_\infty}^\times$ where $S_\infty = \{v|\infty\}$. In particular, this gives a description of the ideal class group in terms of ideles:

$$C_k \cong \mathbf{C}_k/(\prod_{v|\infty} k_v^\times \times \prod_{v\nmid\infty} \mathcal{O}_v^\times).$$

In particular, note that this shows the ideal class group is a quotient of the idele class group. Of course, we would like to have the same result for the ray class groups as well. Fortunately, we do.

Let $\mathfrak{m}$ be a divisor of k. For each prime $v \mid \mathfrak{m}$, we set

$$W_{\mathfrak{m}}(v) = \begin{cases} \mathbb{R}_{>0} & v \text{ real} \\ 1 + \mathfrak{m}_v^{m(v)} & v \text{ finite.} \end{cases}$$

Observe that

$$P_{\mathfrak{m},1} = k^\times \cap \prod_{v|\mathfrak{m}} W_{\mathfrak{m}}(v).$$

Set

$$\mathbb{A}_{k,\mathfrak{m}}^\times = \left(\prod_{v\nmid\mathfrak{m}} k_v^\times \times \prod_{v|\mathfrak{m}} W_{\mathfrak{m}}(v)\right) \cap \mathbb{A}_k^\times$$

and

$$W_{\mathfrak{m}} = \prod_{\substack{v\nmid\mathfrak{m} \\ v|\infty}} k_v^\times \times \prod_{v|\mathfrak{m}} W_{\mathfrak{m}}(v) \times \prod_{\substack{v\nmid\mathfrak{m} \\ v\nmid\infty}} \mathcal{O}_v^\times.$$

One then has the following theorem:

Theorem 2.42. *([Milne2]) Let $\mathfrak{m}$ be a divisor of k.*
1. The map $id : \mathbb{A}_{k,\mathfrak{m}}^\times \longrightarrow I^{S(\mathfrak{m})}$ defines an isomorphism

$$\mathbb{A}_{k,\mathfrak{m}}^\times/(P_{\mathfrak{m},1} \cdot W_{\mathfrak{m}}) \cong C_{\mathfrak{m}}.$$

2. The inclusion map $\mathbb{A}_{k,\mathfrak{m}}^\times \hookrightarrow \mathbb{A}_k^\times$ defines an isomorphism

$$\mathbb{A}_{k,\mathfrak{m}}^\times/P_{\mathfrak{m},1} \cong \mathbb{A}_k^\times/k^\times.$$

Note that by combining the two parts of the theorem we obtain the desired result that the ray class groups can be realized as quotients of the idele class group. Therefore, by studying the idele class group we are in essence studying all of the ray class groups at once.

Let K be a finite extension of k. Let $(y_\omega) \in \mathbb{A}_K^\times$ be an idele. We define the norm of (y_ω) to be the idele $(x_v) \in \mathbb{A}_k^\times$ with $x_v = \displaystyle\prod_{\omega|v} \operatorname{Nm}_{K_\omega/k_v} y_\omega$.

Proposition 2.43. *There exists a unique continuous homomorphism*

$$\varphi_k : \mathbb{A}_k^\times \longrightarrow \operatorname{Gal}(k^{\mathrm{ab}}/k)$$

with the following property: for any $K \subset k^{\mathrm{ab}}$ with K/k finite and any prime ω of K so that $\omega \mid v$, the diagram

$$\begin{tikzcd}
k_v^\times \arrow[r, "\varphi_v"] \arrow[d] & \operatorname{Gal}(K_\omega/k_v) \arrow[d] \\
\mathbb{A}_k^\times \arrow[r, "(x_v)\mapsto\varphi_k((x_v))|_K"] & \operatorname{Gal}(K/k)
\end{tikzcd}$$

commutes.

Theorem 2.44. *(Reciprocity Law) The homomorphism φ_k has the following properties:*
1. $\varphi_k(k^\times) = 1$;
2. for every finite abelian extension K/k the map φ_k defines an isomorphism

$$\varphi_{K/k} : \mathbb{A}_k^\times/(k^\times \operatorname{Nm}(\mathbb{A}_K^\times)) \xrightarrow{\simeq} \operatorname{Gal}(K/k)$$

i.e., the map φ_k defines an isomorphism

$$\varphi_{K/k} : \mathbf{C}_k/\operatorname{Nm}(\mathbf{C}_K) \xrightarrow{\simeq} \operatorname{Gal}(K/k).$$

The prime v is unramified in K/k if and only if $\mathcal{O}_v^\times \subseteq k^\times \operatorname{Nm}_{K/k}(\mathbb{A}_K^\times)$.

Theorem 2.45. *(Existence Theorem) Let $\overline{k}$ be a fixed algebraic closure of k. For every open subgroup $N \subset \mathbf{C}_k$ of finite index, there exists a unique abelian extension K/k contained in $\overline{k}$ so that $\operatorname{Nm}_{K/k} \mathbf{C}_K = N$. The prime v is unramified if and only if $k^\times \mathcal{O}_v^\times/k^\times \subseteq N$.*

Corollary 2.46. *The map $K \mapsto \operatorname{Nm}(\mathbf{C}_K)$ is a bijection from the set of finite abelian extensions of k to the set of open subgroups of finite index in $\mathbf{C}_k$. Moreover, one has*

$$\begin{array}{rcl}
K_1 \subset K_1 & \Leftrightarrow & \operatorname{Nm}(\mathbf{C}_{K_1}) \supset \operatorname{Nm}(\mathbf{C}_{K_2}) \\
\operatorname{Nm}(\mathbf{C}_{K_1 \cdot K_2}) & = & \operatorname{Nm}(\mathbf{C}_{K_1}) \cap \operatorname{Nm}(\mathbf{C}_{K_1}) \\
\operatorname{Nm}(\mathbf{C}_{K_1 \cap K_2}) & = & \operatorname{Nm}(\mathbf{C}_{K_1}) \operatorname{Nm}(\mathbf{C}_{K_2}).
\end{array}$$

Chapter 3

Some Results on the Sizes of Class Groups

This chapter serves to introduce a wide variety of results on the sizes of class groups of cyclotomic fields. Many of the major results will be presented without proof as we focus more on their applications. The interested reader can find their proofs in chapters 3-6 of [Wash].

The second main purpose of this chapter is to introduce some of the tools that will be necessary in later chapters, namely, characters, L-functions, and p-adic L-functions. We will see that p-adic L-functions play a crucial role in the main conjectures as discussed in chapter 5.

3.1 Characters

In this section we briefly review the definitions associated with Dirichlet characters. Most of the information is probably familiar and so this section can be used more as a reference for the terminology used subsequently.

Definition 3.1. A *Dirichlet character* is a multiplicative homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ where m is a positive integer.

Given such a Dirichlet character, it is easy to see that one obtains a Dirichlet character $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ for any integer n with $m|n$ by merely composing with the natural map $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$. The minimal such m so that χ gives a map $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ is called the *conductor* of χ. We write m_χ if confusion may arise. We say a character is *primitive* if it is defined modulo its conductor. Note that given any character χ we always have an associated primitive character.

Observe that for a character χ we have $\chi(-1) = \pm 1$. This allows us to split our characters into those that satisfy $\chi(-1) = 1$, the so called *even* characters, and those that satisfy $\chi(-1) = -1$, the *odd* characters.

Let χ and ψ be two characters of conductors m_χ and m_ψ respectively. We define their product $\chi\psi$ as follows. Define $\varphi : (\mathbb{Z}/\operatorname{lcm}(m_\chi, m_\psi))^\times \to \mathbb{C}^\times$ by $\varphi(n) = \chi(n)\psi(n)$. This character may or may not be primitive. We define $\chi\psi$ to be the primitive character associated to φ.

Exercise 3.2. *Prove that if* $\gcd(m_\chi, m_\psi) = 1$ *then* $m_{\chi\psi} = m_\chi m_\psi$.

Exercise 3.3. *Show that a character and the associated primitive character are either both odd or both even.*

It will often be useful for us to regard Dirichlet characters as Galois characters via the isomorphism $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ which we recall is given by $\sigma \mapsto a_\sigma$ where a_σ is such that $\sigma(\zeta_n) = \zeta_n^{a_\sigma}$. Let χ be a character of conductor n regarded as a character of $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. The kernel of χ is then a subgroup of $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and thus the fixed field of $\ker\chi$ is a subfield of $\mathbb{Q}(\zeta_n)$. We generally refer to this field as the *fixed field* of χ and denote it by $\mathbb{Q}^\chi$.

Example 3.4. Let $\chi : (\mathbb{Z}/12\mathbb{Z})^\times \to \mathbb{C}^\times$ be given by $\chi(1) = \chi(7) = 1$ and $\chi(5) = \chi(11) = -1$. Thus $\ker\chi = \{1, 7\}$. This gives that $\mathbb{Q}^\chi$ must be a degree 2 extension of $\mathbb{Q}$. However, it is easy to see that $\mathbb{Q}(\zeta_3)$ is a degree 2 extension of $\mathbb{Q}$ fixed by $\ker\chi$. Thus, $\mathbb{Q}^\chi = \mathbb{Q}(\zeta_3)$ and so χ must factor through $(\mathbb{Z}/3\mathbb{Z})^\times$, as one can easily check.

Exercise 3.5. *Define* $\chi : (\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{C}^\times$ *by* $\chi(1) = \chi(5) = 1$ *and* $\chi(3) = \chi(7) = -1$. *Show that the fixed field of* χ *is* $\mathbb{Q}(\zeta_4)$ *and hence* χ *can be regarded as a character of* $\operatorname{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z})^\times$.

Let X be a finite group of Dirichlet characters and let n be the least common multiple of the conductors of the characters in X. Thus, X is a subgroup of the group of characters of $\mathbb{Q}(\zeta_n)$. Set $\mathcal{K}$ to be the intersection of all the kernels of the characters in X and $\mathbb{Q}^X$ to be the fixed field of $\mathcal{K}$. We call $\mathbb{Q}^X$ the *field belonging to X*. We will finish this section by exhibiting a correspondence between the subgroups of X and subfields of $\mathbb{Q}^X$. First we need to recall some basic facts about finite abelian groups and their groups of characters.

Let G be a finite abelian group. We write $G^\wedge$ to denote the group of multiplicative characters of G. We will use G to stand for a finite abelian group for the remainder of this section.

Exercise 3.6. *Prove that* $G \cong G^\wedge$.

Theorem 3.7. *For G as above we have* $G \cong (G^\wedge)^\wedge$.

The map from G to $(G^\wedge)^\wedge$ is given by $g \mapsto (\chi \mapsto \chi(g))$. The main point in the proof of the above theorem is that if there exists a g so that $\chi(g) = 1$ for all $\chi \in G^\wedge$, then $g = 1$. To see this, let $H = \langle g \rangle$. We see that every character in $G^\wedge$ factors through G/H and are all distinct on G/H by assumption. However, there are $\#G$ such characters by the previous exercise and there should be only $\#(G/H)$ distinct characters on G/H, thus $H = 1$, i.e., $g = 1$. This same argument shows that we have a perfect pairing

$$G \times G^\wedge \to \mathbb{C}^\times$$

given by $(g, \chi) \mapsto \chi(g)$.

Let H be a subgroup of G and set

$$H^{\perp} = \{\chi \in G^{\wedge} : \chi(h) = 1 \;\; \forall \; h \in H\}.$$

Exercise 3.8. *Prove that* $H^{\perp} \cong (G/H)^{\wedge}$.

Proposition 3.9. *One has* $H^{\wedge} \cong G^{\wedge}/H^{\perp}$.

Proof. We have the restriction map $G^{\wedge} \to H^{\wedge}$ with kernel $H^{\perp}$. To see the map is surjective one just compares sizes. □

Exercise 3.10. *Prove that* $H \cong (H^{\perp})^{\perp}$.

We are now in a position to show the desired correspondence. First we show that $\mathbb{Q}(\zeta_n)$ actually belongs to a group of Dirichlet characters.

Proposition 3.11. *The field* $\mathbb{Q}(\zeta_n)$ *is the field associated to the group of characters* $X = \{\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \mathbb{C}^{\times}\}$.

Proof. It is clear that the field associated to X gives a subfield of $\mathbb{Q}(\zeta_n)$. We want to show that $\mathcal{K}$, the intersection of the kernels of the characters in X, is actually 1. Let $g \in \mathcal{K}$. Then we have that $\chi(g) = 1$ for every $\chi \in X$. Using $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and $X = G^{\wedge}$, we see from the above results that this implies $g = 1$ as claimed. □

We continue with the notation that X is the group of characters associated to $\mathbb{Q}(\zeta_n)$. Note we have a perfect pairing

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \times X \to \mathbb{C}^{\times}.$$

Let K be a finite abelian field. (Recall the "finite abelian" refers to the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.) The Kronecker-Weber theorem shows that $K \subset \mathbb{Q}(\zeta_n)$ for some n. Set

$$Y = \{\chi \in X : \chi(\sigma) = 1 \;\; \forall \; \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)\}.$$

Observe that

$$\begin{aligned} Y &= \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)^{\perp} \\ &\cong (\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})/\,\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K))^{\wedge} \\ &= \mathrm{Gal}(K/\mathbb{Q})^{\wedge}. \end{aligned}$$

Thus, given a field K we have associated a group of Dirichlet characters Y. Now suppose we are given a subgroup Y of X. Let K be the fixed field of

$$Y^{\perp} = \{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) : \chi(\sigma) = 1 \;\; \forall \; \chi \in Y\}$$

where we have used the isomorphism $G \cong (G^\wedge)^\wedge$. Note this is our "$\mathcal{K}$" from before. Galois theory shows $Y^\perp = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)$. Thus, we have

$$\begin{aligned} Y &= (Y^\perp)^\perp \\ &= \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})^\perp \\ &\cong \mathrm{Gal}(K/\mathbb{Q})^\wedge. \end{aligned}$$

Thus, we have a 1-1 correspondence between subgroups of X and subfields of $\mathbb{Q}(\zeta_n)$ given by

$$\begin{aligned} K &\longleftrightarrow \mathrm{Gal}(K/\mathbb{Q})^\wedge \\ Y &\longleftrightarrow \mathbb{Q}(\zeta_n)^{Y^\perp}. \end{aligned}$$

For the remainder of these notes when we talk of the field belonging to a character or group of characters or the group of characters belonging to a field the notions of this section are what is meant.

We now introduce the Teichmuller character. As usual we assume p is an odd prime with the understanding that this can all be carried out in the case of $p = 2$ but would require more notation.

Lemma 3.12. *There are precisely $p-1$ distinct $(p-1)$th roots of unity in $\mathbb{Z}_p$. Moreover, these roots of unity remain distinct modulo p.*

Proof. Let $f(x) = x^{p-1} - 1 \in \mathbb{Q}_p[x]$. It is clear that $f(x)$ can have at most $p-1$ roots in $\mathbb{Q}_p$. Let $a \in \mathbb{Z}_p$, $a \neq 0$. We have that $f(a) = 0 (\operatorname{mod} p)$. Since $f'(a) \neq 0 (\operatorname{mod} p)$, Hensel's lemma gives that there is a unique root of $f(x)$ in $\mathbb{Z}_p$ that is congruent to a modulo p. This gives that there are $p-1$ distinct roots of unity in $\mathbb{Z}_p$, i.e., $\mu_{p-1} \subset \mathbb{Z}_p^\times$. □

Therefore, for each nonzero $a \in \mathbb{Z}_p$ we have that there corresponds to a a well defined root of unity in $\mathbb{Z}_p$. We define $\omega : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ by setting $\omega(a)$ to be the root of unity corresponding to a. As usual one can extend this by 0 if one wants a map $\mathbb{Z}_p \to \mathbb{Z}_p$. Observe in the above construction that what happens is $a \in \mathbb{Z}_p$ maps to $\overline{a} \in \mathbb{F}_p$ and then is lifted back to $\mathbb{Z}_p$ via Hensel's lemma. This shows that ω is a p-adic Dirichlet character of conductor p. One could view this as a complex Dirichlet character, but it is best to view it as a p-adic object.

Exercise 3.13. *Show that ω is an odd character.*

The following proposition will be applied in the following sections to study sizes of class groups.

Proposition 3.14. *Let $Y = \{1, \omega^2, \omega^4, \dots, \omega^{p-3}\}$. The field determined by Y is $\mathbb{Q}(\zeta_p)^+ := \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.*

Proof. It is easy to see that $X = \{1, \omega, \omega^2, \dots, \omega^{p-2}\}$ is the group of characters corresponding to $\mathbb{Q}(\zeta_p)$. (There are $p-1$ of them and they are all distinct, so must be all of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})^\wedge$.) It is easy to see that we must have $|Y^\perp| =$

$|X|/|Y| = 2$. Since all the characters in Y are even characters we must have that 1 and -1 comprise $Y^{\perp}$. The fixed field of this is then $\mathbb{Q}(\zeta_p)^+$ as this is the totally real subfield of $\mathbb{Q}(\zeta_p)$ and we want the largest field fixed by -1, i.e., by complex conjugation. □

3.2 L-functions and Class Numbers

In this section we review some basic results about L-functions attached to characters. The facts given here either will be used later or are included to illustrate the analogy with p-adic L-functions. Proofs are omitted as the results are assumed either to be familiar or can be taken on faith as the proofs will not be used in these notes. The interested reader can consult [Jan] or [Wash] for the proofs and more information on L-functions.

Let χ be a Dirichlet character of conductor n extended to $\mathbb{Z}$ as indicated above. The L-function attached to χ is given by

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}, \quad \mathrm{Re}(s) > 1.$$

It is well known that $L(s,\chi)$ can be analytically continued to the entire complex plane if $\chi \neq 1$. If $\chi = 1$ then $L(s,\chi)$ is just the Riemann zeta function, which has meromorphic continuation to the complex plane with a simple pole of residue 1 at $s = 1$. The L-function $L(s,\chi)$ has a convergent Euler product given by

$$L(s,\chi) = \prod_p (1 - \chi(p)p^{-s})^{-1}, \quad \mathrm{Re}(s) > 1.$$

Remark 3.15. The L-function $L(s,\chi)$ also satisfies a functional equation relating $L(s,\chi)$ to $L(1-s,\overline{\chi})$. However, we will not need the precise form of the functional equation so omit a discussion of it.

Recall the *Bernoulli numbers* are defined by

$$\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} B_m \frac{t^m}{m!}.$$

Similarly, we define the *generalized Bernoulli numbers* by

$$\sum_{j=1}^{n} \frac{\chi(j) t e^{jt}}{e^{nt} - 1} = \sum_{m=0}^{\infty} B_{m,\chi} \frac{t^m}{m!}$$

where χ is a Dirichlet character of conductor n.

Exercise 3.16. *Set $\delta = 0$ if χ is even and $\delta = 1$ if χ is odd. Prove that $B_{m,\chi} = 0$ if $m \not\equiv \delta (\bmod 2)$ with the exception of $B_{1,1}$.*

The generalized Bernoulli numbers play a large role in arithmetic due to their relation to the special values of L-functions. In particular, we have the following theorem.

Theorem 3.17. *([Wash] Theorem 4.2) For $m \geq 1$ we have*

$$L(1-m,\chi) = -\frac{B_{m,\chi}}{m}.$$

We now come to Dirichlet's class number formula. One should view this as an example of a larger philosophy prevalent in number theory. In particular, given an object of number theoretic interest (a "motivic" object) X, there is associated to X an L-function $L(s,X)$. This L-function is an analytic object and can be studied using tools from complex analysis. One expects that the special values of this L-function should then provide arithmetic information back about X. In the current situation the object of interest is a number field K and the arithmetic information we are interested in is the size of the class group of K.

Theorem 3.18. *(Dirichlet's Class Number Formula) Let K be a number field and let X be the group of characters that K belongs to. We have*

$$\prod_{\substack{\chi\in X\\ \chi\neq 1}} L(1,\chi) = \frac{2^{r_1}(2\pi)^{r_2}R_K}{\omega_K\sqrt{|D_K|}}h_K$$

where r_1 is the number of real embeddings of K into $\mathbb{C}$, r_2 is the number of pairs of complex conjugate embeddings of K into $\mathbb{C}$, R_K is the regulator of K, ω_K is the number of roots of unity in K, D_K is the discriminant of K, and h_K is the size of the class group of K. For definitions of any of these terms please consult [Milne1].

Remark 3.19. This formulation of the class number formula may not look like the one presented in most algebraic number theory courses. We have used the fact that

$$\zeta_K(s) = \prod_{\chi\in X} L(s,\chi)$$

and that $\zeta(s)$ has a simple pole with residue 1 at $s=1$ to arrive at the present formulation.

We now specialize to the case of $K=\mathbb{Q}(\zeta_n)$. Note that $\mathbb{Q}(\zeta_n)$ is a degree 2 extension of the field $\mathbb{Q}(\zeta_n+\zeta_n^{-1})$, a field that sits inside $\mathbb{R}$. What we are really using here is that $\mathbb{Q}(\zeta_n)$ is a CM-field. Set h_n to be the class number of $\mathbb{Q}(\zeta_n)$ and h_n^+ to be the class number of $\mathbb{Q}(\zeta_n+\zeta_n^{-1})$. We will need the following proposition.

Proposition 3.20. *Let K/E be an extension of number fields so that there is no nontrivial unramified subextension F/E with* $\mathrm{Gal}(F/E)$ *abelian. Then h_E divides h_K.*

Proof. Let H be the maximal unramified abelian extension of E. From class field theory we know that $\mathrm{Gal}(H/E)$ is isomorphic to the ideal class group of E. Our assumption implies that $K \cap H = E$. Thus, we have $h_E = [H : E] = [HK : K]$ where we use the fact that $\mathrm{Gal}(HK/K) \cong \mathrm{Gal}(H/E)$. This isomorphism also gives that $\mathrm{Gal}(HK/K)$ is an unramified abelian extension of K and so sits inside the maximal unramified abelian extension of K. Thus, $h_E | h_K$ as claimed. □

Theorem 3.21. *For n a positive integer we have that $h_n^+ \mid h_n$.*

Proof. This follows immediately from the previous proposition when one observes that $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is totally ramified at the real place. □

Definition 3.22. Define the *relative class number* of $\mathbb{Q}(\zeta_n)$ to be $h_n^- := h_n/h_n^+$.

With some work one can show using Dirichlet's class number formulae that the following formula for h_n^- holds

$$h_n^- = 2^a 2n \prod_{\substack{\chi \in X \\ \chi(-1)=-1}} \left(-\frac{1}{2} B_{1,\chi}\right)$$

where X is the group of characters associated to $\mathbb{Q}(\zeta_n)$ and a is 0 if n is a prime power and 1 otherwise. In particular, taking p to be prime we have

$$h_p^- = 2p \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-2} \left(-\frac{1}{2} B_{1,\omega^j}\right). \tag{3.1}$$

We will use this formula in the following section to prove that $p \mid h_p^-$ if and only if $p \mid B_j$ for some $j = 2, 4, \ldots, p-3$.

3.3 p-adic L-functions

We give here a brief introduction to p-adic L-functions. Proofs that are purely analytic in nature are omitted with appropriate references given. These L-functions will be important when we discuss the main conjectures of Iwasawa theory. Here we just give some basic facts and return to them when we come to the main conjectures.

Theorem 3.23. *([Wash], Theorem 5.11) Let χ be a Dirichlet character. There exists a p-adic meromorphic function (analytic if $\chi \neq 1$) $\mathcal{L}_p(s,\chi)$ defined on $\{s \in \mathbb{C}_p : |s| < p^{1-1/(p-1)}\}$ such that*

$$\mathcal{L}_p(1-n,\chi) = -(1 - \chi\omega^{-n}(p)p^{n-1}) \frac{B_{n,\chi\omega^{-n}}}{n}, \quad n \geq 1.$$

If $\chi = 1$ then $\mathcal{L}_p(s,1)$ is analytic except for a pole at $s = 1$ with residue $1 - 1/p$.

Remark 3.24. One should note that $\chi\omega^{-n}$ is the primitive character associated to the character $a \mapsto \chi(a)\omega^{-n}(a)$. In general one does not have $\chi\omega^{-n}(a) = \chi(a)\omega^{-n}(a)$.

One should view the p-adic L-function $\mathcal{L}_p(s,\chi)$ as a p-adic interpolation of the usual L-function $L(s,\chi)$. In particular for $n \geq 1$ we have

$$\mathcal{L}_p(1-n,\chi) = (1-\chi\omega^{-n}(p)p^{n-1})L(1-n,\chi\omega^{-n}).$$

Thus, if $n \equiv 0 (\operatorname{mod} p-1)$ then we obtain

$$\mathcal{L}_p(1-n,\chi) = (1-\chi(p)p^{n-1})L(1-n,\chi) = L^{(p)}(1-n,\chi).$$

The pth Euler factor must be removed in order for the p-adic L-function to converge. In general, if p is allowed to divide $1/n^s$ then the p-adic absolute value of such terms would get arbitrarily large and so the sum of the terms would not converge.

If χ is an odd character it is easy to see that $B_{n,\chi\omega^{-n}} = 0$. Thus the p-adic L-function of an odd character is identically 0. However, if χ is even then the p-adic L-function is not identically 0. The zeros of the p-adic L-function are not well understood.

Though the proof of the existence of $\mathcal{L}_p$ is omitted, it is not a difficult proof. In general it is believed that one can associate p-adic L-functions to a wide class of classical L-functions. Unfortunately, proving the existence of such p-adic L-functions in other settings can be extremely difficult.

We conclude this section with some congruence results that follow from the existence of the p-adic L-function as given in Theorem 3.23.

Theorem 3.25. *Let χ be a nontrivial character and suppose $p^2 \nmid m_\chi$. (Note we are again ignoring the case of $p = 2$, though it can easily be handled!) One has that*

$$\mathcal{L}_p(s,\chi) = a_0 + a_1(s-1) + a_2(s-1)^2 + \cdots$$

where $|a_0|_p \leq 1$ and $p \mid a_i$ for all $i \geq 1$.

Proof. See ([Wash] Theorem 5.12). □

Corollary 3.26. *Let m and n be integers with $m \equiv n (\operatorname{mod} p-1)$ and $n \not\equiv 0 (\operatorname{mod} p-1)$. Then one has*

$$\frac{B_m}{m} \equiv \frac{B_n}{n} (\operatorname{mod} p).$$

Proof. Note that since $m \equiv n (\operatorname{mod} p-1)$ we have $\mathcal{L}_p(s,\omega^m) = \mathcal{L}_p(s,\omega^n)$. We know that

$$\mathcal{L}_p(1-m,\omega^m) = -(1-p^{m-1})\frac{B_m}{m}$$

and similarly for $\mathcal{L}_p(s,\omega^n)$. Using the previous theorem and the fact that $m \equiv n \not\equiv 0 (\operatorname{mod} p-1)$ we can write

$$\mathcal{L}_p(s,\omega^m) = a_0 + a_1(s-1) + a_2(s-1)^2 + \cdots$$

where $|a_0|_p \leq 1$ and $p \mid a_i$ for all $i \geq 1$. Thus,

$$\mathcal{L}_p(1-m, \omega^m) = a_0 + a_1(-m) + a_2(-m^2)^2 + \cdots \equiv a_0 (\operatorname{mod} p)$$

and similarly for $\mathcal{L}_p(1-n, \omega^n)$. Thus, $\mathcal{L}_p(1-m, \omega^m) \equiv \mathcal{L}_p(1-n, \omega^n) (\operatorname{mod} p)$. The result now follows. □

Corollary 3.27. *Let $m, n \in \mathbb{Z}$ and χ a nontrivial character with $p^2 \nmid m_\chi$. Then one has that $\mathcal{L}_p(m, \chi)$ is p-integral and*

$$\mathcal{L}_p(m, \chi) \equiv \mathcal{L}_p(n, \chi) (\operatorname{mod} p).$$

Proof. This follows immediately from the previous theorem. □

Corollary 3.28. *Let n be an odd integer and $n \not\equiv -1 (\operatorname{mod} p-1)$. Then we have*

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} (\operatorname{mod} p)$$

and both sides are p-integral.

Proof. We begin by observing that $\omega^{n+1} \neq 1$ since $n \not\equiv -1 (\operatorname{mod} p-1)$. We also have that $\omega^n \neq 1$ since n is odd and so $\omega^n(p) = 0$. By Theorem 3.23 we have

$$\mathcal{L}_p(-n, \omega^{n+1}) = -(1-p^n)\frac{B_{n+1}}{n+1}$$

and

$$\begin{aligned}\mathcal{L}_p(0, \omega^{n+1}) &= -(1-\omega^n(p))B_{1,\omega^n} \\ &= -B_{1,\omega^n}.\end{aligned}$$

Using these equalities and the facts that $\mathcal{L}_p(-n, \omega^{n+1})$ and $\mathcal{L}_p(0, \omega^{n+1})$ are both p-integral and congruent modulo p by Corollary 3.27 we obtain the result. □

Theorem 3.29. *Let p be an odd prime. Then $p \mid h_p^-$ if and only if $p \mid B_j$ for some $j = 2, 4, \ldots, p-3$. Here it is understood that $p|B_j$ means that p divides the numerator of B_j.*

Proof. Recall from equation (3.1) that

$$h_p^- = 2p \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-2} \left(-\frac{1}{2}B_{1,\omega^j}\right).$$

We begin by studying $2p\left(-\frac{1}{2}B_{1,\omega^{p-2}}\right) = -pB_{1,\omega^{p-2}}$. Note that $B_{1,\omega^{p-2}} = B_{1,\omega^{-1}}$. Using the definition of $B_{1,\omega^{-1}}$ one sees that

$$B_{1,\omega^{-1}} = \frac{1}{p}\sum_{a=1}^{p-1} a\omega^{-1}(a).$$

Thus we have

$$2p\left(-\frac{1}{2}B_{1,\omega^{p-2}}\right) = -\sum_{a=1}^{p-1} a\omega^{-1}(a).$$

Modulo p we have that $a \equiv \omega(a)$ and so we obtain

$$2p\left(-\frac{1}{2}B_{1,\omega^{p-2}}\right) \equiv -(p-1) \equiv 1 (\operatorname{mod} p).$$

Thus,

$$h_p^- \equiv \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-4} \left(-\frac{1}{2}B_{1,\omega^j}\right) (\operatorname{mod} p).$$

Now we apply the previous corollary to obtain

$$\prod_{\substack{j=1 \\ j \text{ odd}}}^{p-4} \left(-\frac{1}{2}B_{1,\omega^j}\right) \equiv \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-4} \left(-\frac{1}{2}\frac{B_{j+1}}{j+1}\right) (\operatorname{mod} p).$$

From this the theorem follows immediately. □

Definition 3.30. We say a prime p is *irregular* if $p \mid B_j$ for some $j = 2, 4, \ldots, p-3$. If a prime is not irregular it is said to be *regular.*

Note that the previous theorem shows that p is an irregular prime if and only if $p \mid h_p^-$. We will see in the next section that $p \mid h_p$ if and only if $p \mid B_j$ for some $j = 2, 4, \ldots, p-3$. Thus, p is an irregular prime if and only if $p \mid h_p$. This is also often used as the definition of an irregular prime.

Theorem 3.31. *There are infinitely many irregular primes.*

It is also believed that there are infinitely many regular primes. In fact, numerical evidence suggests that around 61% of all primes are regular primes. However, no one yet knows how to prove there are infinitely many regular primes.

3.4 p-adic L-functions and Class Numbers

We now give a short section on the p-adic class number formula. We include this not only for the analogy with the classical Dirichlet class number formula, but also because of its application to proving a result on class numbers. The p-adic class number formula is usually developed in order to prove the following result.

Theorem 3.32. *Let $\chi \neq 1$ be an even Dirichlet character. Then $\mathcal{L}_p(1, \chi) \neq 0$.*

However, since these notes are focused more on class numbers combined with the fact that we did not pursue the analogous result for classical L-functions $L(s, \chi)$, we will have the following theorem as our goal.

Theorem 3.33. *If $p \mid h_p^+$, then $p \mid h_p^-$. In particular, $p \mid h_p$ if and only if $p \mid B_j$ for some $j = 2, 4, \ldots, p-3$.*

We now state, but do not prove the p-adic class number formula. For a complete proof and for a definition of the p-adic regulator $R_p(K)$ see ([Wash], Chapter 5). We will not need the definition of $R_p(K)$ here.

Theorem 3.34. *Let K be a totally real abelian number field with $[K : \mathbb{Q}] = n$. Let X be the group of Dirichlet characters corresponding to K. One has*

$$\prod_{\substack{\chi \in X \\ \chi \neq 1}} \left(1 - \frac{\chi(p)}{p}\right)^{-1} \mathcal{L}_p(1, \chi) = \frac{2^{n-1} h_K R_p(K)}{\sqrt{\Delta_K}}.$$

We will also need the following proposition. We again omit the proof.

Proposition 3.35. *Suppose K is a totally real Galois number field. If there is only one prime $\wp$ of K such that $\wp \mid p$ and if $e(\wp/p) \leq p-1$, then*

$$\left| \frac{[K : \mathbb{Q}] R_p(K)}{\sqrt{\Delta_K}} \right|_p \leq 1.$$

Proof. See ([Wash], Proposition 5.33). □

Proof. (of Theorem 3.33) Recall that the group of characters that corresponds to $\mathbb{Q}(\zeta_p)^+$ is $\{1, \omega^2, \omega^4, \ldots, \omega^{p-3}\}$, i.e., the even characters of $\mathbb{Q}(\zeta_p)$. Set $n = (p-1)/2$. Since $\mathbb{Q}(\zeta_p)^+$ is a totally real abelian number field, the p-adic class number formula gives

$$\prod_{\substack{j=2 \\ j \text{ even}}}^{p-3} \mathcal{L}_p(1, \omega^j) = \frac{2^{n-1} h_p^+ R_p^+}{\sqrt{\Delta_p^+}}$$

since $\omega^j(p) = 0$ for $j = 2, 4, \ldots, p-3$. We know that $\mathbb{Q}(\zeta_p)^+$ satisfies the hypotheses of Proposition 3.35 so we have

$$\left| \frac{[\mathbb{Q}(\zeta_p)^+ : \mathbb{Q}] R_p^+}{\sqrt{\Delta_p^+}} \right|_p = \left| \frac{R_p^+}{\sqrt{\Delta_p^+}} \right|_p \leq 1.$$

If $p \mid h_p^+$, the we must have $p \mid \mathcal{L}_p(1, \omega^{j_0})$ for some $j_0 \in \{2, 4, \ldots, p-3\}$. Corollary 3.27 shows that

$$\begin{aligned} -B_{1,\omega^{j_0-1}} &= -\left(1 - \frac{\omega^{j_0-1}(p)}{p}\right)^{-1} B_{1,\omega^{j_0-1}} \\ &= \mathcal{L}_p(0, \omega^{j_0}) \\ &\equiv \mathcal{L}_p(1, \omega^{j_0}) (\operatorname{mod} p) \\ &\equiv 0 (\operatorname{mod} p). \end{aligned}$$

Thus, $p \mid B_{1,\omega^{j_0-1}}$. Using that all the B_{1,ω^i} are p-integral and that we have

$$h_p^- \equiv \prod_{\substack{i=1 \\ i \text{ odd}}}^{p-4} \left(-\frac{1}{2}B_{1,\omega^i}\right) (\operatorname{mod} p)$$

we have that $h_p^- \equiv 0 (\operatorname{mod} p)$, as desired. □

We conclude this section with the following open conjecture of Vandiver.

Conjecture 3.36. *(Vandiver) For p a prime one has $p \nmid h_p^+$.*

3.5 Herbrand's Theorem

In this section we seek to prove a much stronger criterion then that given in Theorem 3.33 by looking at "pieces" of the class group rather then the entire class group. This description is known as Herbrand's theorem. We will also state the converse of this theorem which is due to Ribet ([Ribet]). We will return to the proof of the converse in later chapters as it provides a nice overview of the method Wiles used to prove the main conjecture of Iwasawa theory for totally real fields ([Wiles2]).

Before we can state any results we need to formulate what we mean by "pieces" of the ideal class group. We begin with some generalities. Let G be a finite abelian group and $G^\wedge$ the group of multiplicative characters of G as before. Let R be a commutative ring that contains $|G|^{-1}$ and all the values of all the $\chi \in G^\wedge$. We define the orthogonal idempotents of the group ring $R[G]$ to be the elements

$$\varepsilon_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \in R[G].$$

Exercise 3.37. *Prove the following results:*
1. $\varepsilon_\chi^2 = \varepsilon_\chi$
2. $\varepsilon_\chi \varepsilon_\psi = 0$ *if* $\chi \neq \psi$
3. $\displaystyle\sum_{\chi \in G^\wedge} \varepsilon_\chi = 1$
4. $\varepsilon_\chi \sigma = \chi(\sigma)\varepsilon_\chi$.

Proposition 3.38. *Let M be a module over $R[G]$. Then we have $M = \bigoplus_\chi \varepsilon_\chi M$.*

Proof. This proposition follows easily from the properties listed in the exercise. □

Note that if we view $\sigma \in G$ as acting on M, the space $\varepsilon_\chi M$ are the eigenspaces of this action with eigenvalue $\chi(\sigma)$.

We now specialize to the case that the module we are considering is an ideal class group. Let C be the ideal class group of a finite abelian extension $K/\mathbb{Q}$ and set $G = \operatorname{Gal}(K/\mathbb{Q})$. Choose n so that $K \subseteq \mathbb{Q}(\zeta_n)$. The group ring $\mathbb{Z}[G]$

naturally acts on C. Given $x = \sum x_\sigma \sigma \in \mathbb{Z}[G]$ and $\mathfrak{a}$ a fractional ideal of K, the action is given by

$$x \cdot \mathfrak{a} = \mathfrak{a}^x = \prod_\sigma (\sigma \mathfrak{a})^{x_\sigma}.$$

Now let A denote the p-Sylow subgroup of the class group C. We obtain an action of $\mathbb{Z}_p[G]$ on A. To see this, observe that $\mathbb{Z}_p$ acts on A by

$$(\sum_{j=0}^{\infty} a_j p^j) \cdot \mathfrak{a} = \prod_{j=1}^{\infty} (\mathfrak{a}^{a_j p^j})$$

due to the fact that $p^m A = 0$ for large enough m.

For a real number x, let $\{x\}$ denote the fractional part of x, i.e., $x - \{x\} \in \mathbb{Z}$ and $0 \leq \{x\} < 1$.

Definition 3.39. The *Stickelberger element of* K is defined by

$$\theta = \theta(K) = \sum_{\substack{a (\operatorname{mod} n) \\ \gcd(a,n)=1}} \left\{ \frac{a}{n} \right\} \sigma_a^{-1} \in \mathbb{Q}[G]$$

where σ_a is the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ given by $\zeta_n \mapsto \zeta_n^a$ restricted to K. The *Stickelberger ideal* $I(K)$ *of* K is defined to be $\mathbb{Z}[G] \cap \theta\mathbb{Z}[G]$.

We require the following theorem that will be stated without proof.

Theorem 3.40. *(Stickelberger's Theorem) The Stickelberger ideal annihilates the ideal class group of* K*, i.e., if* $\mathfrak{a}$ *is a fractional ideal of* K, $\beta \in \mathbb{Z}[G]$ *is such that* $\beta\theta \in \mathbb{Z}[G]$*, then* $(\beta\theta) \cdot \mathfrak{a}$ *is principal.*

Suppose now that $K = \mathbb{Q}(\zeta_p)$ for p an odd prime. Recall that $G^\wedge = \{\omega^i : 0 \leq i \leq p-2\}$. We use the group ring $\mathbb{Z}_p[G]$. In this case the orthogonal idempotents are

$$\varepsilon_i := \varepsilon_{\omega^i} = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^i(a) \sigma_a^{-1}$$

for $0 \leq i \leq p-2$ and the Stickelberger element is given by

$$\theta = \frac{1}{p} \sum_{a=1}^{p-1} a \sigma_a^{-1}.$$

Observe that we have

$$\begin{aligned}
\varepsilon_i \theta &= \frac{1}{p} \sum_{a=1}^{p-1} a \varepsilon_i \sigma_a^{-1} \\
&= \frac{1}{p} \sum_{a=1}^{p-1} a \omega^i(\sigma_a^{-1}) \varepsilon_i \\
&= \frac{1}{p} \sum_{a=1}^{p-1} a \omega^{-i}(a) \varepsilon_i \\
&= B_{1,\omega^{-i}} \varepsilon_i.
\end{aligned}$$

and similarly for $c \in \mathbb{Z}$ we have

$$\varepsilon_i(c - \sigma_c)\theta = (c - \omega^i(c))B_{1,\omega^{-i}}\varepsilon_i.$$

Proposition 3.41. *Let $c \in \mathbb{Z}$ with $p \nmid c$. Then $(c - \sigma_c)\theta \in \mathbb{Z}[G]$.*

Proof. We begin by observing

$$(c - \sigma_c)\theta = \sum_{a=1}^{p-1} c \left\{ \frac{a}{p} \right\} \sigma_a^{-1} - \sum_{a=1}^{p-1} \left\{ \frac{a}{p} \right\} \sigma_c \sigma_a^{-1}.$$

It is easy to see that $\sigma_c\sigma_a^{-1} = \sigma_{ca^{-1}}$. Thus, by changing the index of summation on the second sum we obtain

$$(c - \sigma_c)\theta = \sum_{a=1}^{p-1} \left(c \left\{ \frac{a}{p} \right\} - \left\{ \frac{ac}{p} \right\} \right) \sigma_a^{-1}.$$

Using that $\left\{ \frac{a}{p} \right\} = \frac{a}{p}$ and that $x - \{x\} \in \mathbb{Z}$ we see that $(c - \sigma_c)\theta \in \mathbb{Z}[G]$ as desired. □

Let A denote the p-Sylow subgroup of the class group of $\mathbb{Q}(\zeta_p)$. As was observed above, A is a $\mathbb{Z}_p[G]$-module and so we have the decomposition

$$A = \bigoplus_{i=0}^{p-2} A_i$$

where it is customary to write A_i for $\varepsilon_i A$. Stickelberger's theorem along with the previous proposition imply that $(c - \sigma_c)\theta$ annihilates A and hence each A_i for $p \nmid c$. In particular, we have shown that $(c - \omega^i(c))B_{1,\omega^{-i}}$ annihilates A_i.

Note that if $i \neq 0$ is even, then $B_{1,\omega^{-i}} = 0$ and so we have really shown nothing new. For $i = 0$ we get that $(c-1)/2$ annihilates A_0 for any c with $p \nmid c$, and so it must be that $A_0 = 0$. Now consider the case that i is odd. If $i \neq 1$, then there exists a c so that $c \not\equiv \omega^i(c) (\operatorname{mod} p)$ and so we can ignore the factor $(c - \omega^i(c))$ and obtain that $B_{1,\omega^{-i}}$ annihilates A_i. If $i = 1$, set $c = 1 + p$. Then

$$\begin{aligned} (c - \omega(c))B_{1,\omega^{-1}} &= pB_{1,\omega^{-1}} \\ &= \sum_{a=1}^{p-1} a\omega^{-1}(a) \\ &= p - 1 \not\equiv 0 (\operatorname{mod} p). \end{aligned}$$

Since A_1 is necessarily a p-group we must have $A_1 = 0$. Thus, we have the following proposition.

Proposition 3.42. *The pieces of the class group A_0 and A_1 are both 0 and for $i = 3, 5, \ldots, p-2$ we have that $B_{1,\omega^{-i}}$ annihilates A_i.*

We now are ready to state Herbrand's theorem. Suppose that $A_i \neq 0$ for some $i = 3, 5, \ldots, p-2$, i.e., the i^{th} part of the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$ is nontrivial. Since $B_{1,\omega^{-i}}$ annihilates this nontrivial p-group, we must have that $p \mid B_{1,\omega^{-i}}$. However, we know that $B_{1,\omega^{-i}} \equiv \frac{B_{p-i}}{p-i} (\operatorname{mod} p)$. Thus we have Herbrand's theorem.

Theorem 3.43. *(Herbrand's Theorem) Let i be odd and $3 \leq i \leq p-2$. If $A_i \neq 0$, then $p \mid B_{p-i}$.*

Note this is stronger then Theorem 3.33 in one direction. There it was stated if $p \mid h_p$ then p divides some Bernoulli number. Here we get the exact Bernoulli number in terms of which piece of the class group is nontrivial.

Theorem 3.44. *([Ribet]) Let i be odd with $3 \leq i \leq p-2$. If $p \mid B_{p-i}$, then $A_i \neq 0$.*

Ribet is able to prove the converse to Herbrand's theorem by actually constructing elements in the i^{th} part of the p-Sylow subgroup of the class group of $\mathbb{Q}(\zeta_p)$. He accomplishes this by using modular forms. In particular, he produces a congruence between an Eisenstein series and a cusp form and then uses this congruence and some results on Galois representations to find an element of order p in the appropriate piece of the class group. We will return to this argument later in the notes.

We close this chapter with the following strengthening of the result $p \mid h_p^+$ implies $p \mid h_p^-$.

Theorem 3.45. *Let i be even and j odd with $i + j \equiv 1 (\operatorname{mod} p-1)$. Then*

$$p\text{-}rank(A_i) \leq p\text{-}rank(A_j) \leq 1 + p\text{-}rank(A_i)$$

where the p-rank of a finite abelian group G is the dimension of G/pG as a vector space over $\mathbb{F}_p$.

To actually see this is a strenghtening of the result $p \mid h_p^+$ implies $p \mid h_p^-$ requires some work. Recall that we defined h_p^+ to be the size of the class group of $\mathbb{Q}(\zeta_p)^+$. We then showed $h_p^+ \mid h_p$ and so defined $h_p^- = h_p/h_p^+$. We will now show that h_p^+ and h_p^- are sizes of pieces of the class group of $\mathbb{Q}(\zeta_p)$.

We denote complex conjugation $\sigma_{-1} \in \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ by J as is customary. Write C_p for the class group of $\mathbb{Q}(\zeta_p)$ and C_{p^+} for the ideal class group of $\mathbb{Q}(\zeta_p)^+$. Let C_p^- be the (-1)-eigenspace of C_p for the action of J, i.e.,

$$C_p^- = \{\mathfrak{a} \in C_p : (1+J) \cdot \mathfrak{a} = 1\}.$$

Recall that in the class field theory section we proved that if $H_{\mathbb{Q}(\zeta_p)^+} \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p)^+$, then the norm map $C_p \to C_{p^+}$ is surjective where $H_{\mathbb{Q}(\zeta_p)^+}$ is the Hilbert class field of $\mathbb{Q}(\zeta_p)^+$. However, we know that $\mathbb{Q}(\zeta_p)$ is ramified over $\mathbb{Q}(\zeta_p)^+$ at the archimedean primes, so this condition is satisfied. Now we observe that we have an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & C_p^- \arrow[r] & C_p \arrow[r, "\mathrm{Norm}"] & C_{p^+} \arrow[r] & 1. \end{tikzcd}$$

To see that C_p^- is precisely the kernel of the norm map see ([Milne1], page 63) for properties of the norm map and recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p)^+) \cong \{1, J\}$. Thus we see that h_p^- is the order of C_p^-, a piece of the class group of $\mathbb{Q}(\zeta_p)$.

Since we are concerned with only the p-divisibility in the above theorem, we can restrict to working with the p-part of the class group. Define $\varepsilon_- = \frac{1-J}{2}$ and $\varepsilon_+ = \frac{1+J}{2}$. It is an elementary calculation to show that the (-1)-eigenspace of J acting on A is precisely $\varepsilon_- A$. Thus we write $A^- = \varepsilon_- A$ and similarly we define $A^+ = \varepsilon_+ A$. We have that $A = A^- \oplus A^+$. The above result then shows that A^+ is precisely the p-part of C_{p^+} as desired. One can show that

$$\varepsilon_+ = \sum_{i \text{ even}} \varepsilon_i$$

and

$$\varepsilon_- = \sum_{i \text{ odd}} \varepsilon_i,$$

i.e.,

$$A^- = A_1 \oplus A_3 \oplus \cdots \oplus A_{p-2}$$

and

$$A^+ = A_0 \oplus A_2 \oplus \cdots \oplus A_{p-3}.$$

The fact that the above theorem generalizes the statement $p \mid h_p^+$ implies $p \mid h_p^-$ is now clear.

Chapter 4

$\mathbb{Z}_p$-extensions

4.1 Introduction

Let p be an odd prime. All of the results in this chapter follow if $p = 2$ as well, but we restrict ourselves to odd primes in order to simplify the notation. For the general results one should consult [Wash].

Given a number field K, a *$\mathbb{Z}_p$-extension of K* is a field extension K_∞ of K such that $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Note here that we are looking at the additive group of p-adic integers. It is important in Iwasawa theory to keep track of which structures one is using.

First we need to show that any given number field actually has at least one $\mathbb{Z}_p$-extension. We begin with $\mathbb{Q}$. Recall that one has

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) \cong (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z}).$$

Let $\mathbb{Q}_n$ be the fixed field of $(\mathbb{Z}/p\mathbb{Z})^\times$, i.e., $\mathbb{Q}_n = \mathbb{Q}(\zeta_{p^{n+1}})^{(\mathbb{Z}/p\mathbb{Z})^\times}$. From Galois theory we know that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$. Let $\mathbb{Q}_\infty = \bigcup \mathbb{Q}_n$. Then we have that

$$\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}_p.$$

Thus, the rational numbers have a $\mathbb{Z}_p$-extension.

To show that the general number field K has a $\mathbb{Z}_p$-extension, set $K_\infty = K\mathbb{Q}_\infty$. Thus we have that $\mathrm{Gal}(K_\infty/K) \cong \mathrm{Gal}(\mathbb{Q}_\infty/K \cap \mathbb{Q}_\infty)$. We now use that $\mathrm{Gal}(\mathbb{Q}_\infty/K \cap \mathbb{Q}_\infty)$ is a closed subgroup of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ and so of the form $p^n\mathbb{Z}_p$ for some $n \in \mathbb{N}$. Thus, $\mathrm{Gal}(K_\infty/K) \cong p^n\mathbb{Z}_p \cong \mathbb{Z}_p$ as desired. This $\mathbb{Z}_p$-extension is known as the *cyclotomic $\mathbb{Z}_p$-extension* of K. It is possible that K has other $\mathbb{Z}_p$-extensions as well, but we now know that every number field has at least one $\mathbb{Z}_p$-extension.

Let K_∞ now be any $\mathbb{Z}_p$-extension of K. We wish to show that it is possible to consider K_∞ as a union of a sequence of intermediate fields:

$$K = K_0 \subset K_1 \subset \cdots \subset K_\infty = \bigcup K_n$$

where one has

$$\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Recall from the section on infinite Galois theory that the intermediate fields correspond precisely to the closed subgroups of $\mathbb{Z}_p$. Let H be such a closed subgroup and let $h \in H$ be the element with minimal valuation. Observe that $h\mathbb{Z}$ is necessarily contained in H. Since H is closed we obtain that $h\mathbb{Z}_p$ is actually in H. However, since we chose h to have minimal valuation, it must be that $H = h\mathbb{Z}_p = p^n\mathbb{Z}_p$ for some n. Thus, we have the intermediate fields as desired.

The main theorem we will prove in this chapter is the following.

Theorem 4.1. *Let K_∞/K be a $\mathbb{Z}_p$-extension and let e_n be the integer so that $p^{e_n} \| h_n$ where h_n is the order of the class group of K_n. There exist integers $\lambda \geq 0$, $\mu \geq 0$, ν, and n_0 so that*

$$e_n = \lambda n + \mu p^n + \nu$$

for all $n \geq n_0$ where λ, μ, and ν are all indepedent of n.

4.2 Power Series Rings

One of the main objects of study in Iwasawa theory is the Iwasawa algebra $\Lambda = \mathbb{Z}_p[\![T]\!]$, i.e., the power series ring in T with coefficients in $\mathbb{Z}_p$. We devote this section to establishing a few general results that will be needed in subsequent sections.

Let $K/\mathbb{Q}_p$ be a finite extension, $\mathcal{O} := \mathcal{O}_K$ the ring of integers of K, $\mathfrak{p}$ the maximal ideal of $\mathcal{O}$, and ϖ a uniformizer, i.e., $\mathfrak{p} = (\varpi)$. We begin by proving a division algorithm for the algebra $\Lambda_{\mathcal{O}} := \mathcal{O}[\![T]\!]$.

Proposition 4.2. *Let $f, g \in \Lambda_{\mathcal{O}}$ with $f = a_0 + a_1T + \cdots$ with $a_i \in \mathfrak{p}$ for $0 \leq i \leq n-1$ and $a_n \in \mathcal{O}^\times$. Then there exists a unique $q \in \Lambda_{\mathcal{O}}$ and $r \in \mathcal{O}[T]$ with* $\deg r \leq n-1$ *so that*

$$g = qf + r.$$

Proof. We begin by defining a shifting operator $\tau_n := \tau : \Lambda_{\mathcal{O}} :\longrightarrow \Lambda_{\mathcal{O}}$ defined by

$$\tau\left(\sum_{i=0}^{\infty} b_iT^i\right) = \sum_{i=n}^{\infty} b_iT^{i-n}.$$

This operator is clearly $\mathcal{O}$-linear. Furthermore, one has

- $\tau(T^nh(T)) = h(T)$
- $\tau(h(T)) = 0$ if and only if h is a polynomial of degree $\leq n-1$

By our description of $f(T)$ we have $P(T)$ and $U(T)$ so that

$$f(T) = \varpi P(T) + T^nU(T) \tag{4.1}$$

where $P(T)$ is a polynomial of degree less then or equal to $n-1$ and $U(T)$ is invertible in $\Lambda_{\mathcal{O}}$ since the leading coefficient is $a_n \in \mathcal{O}^{\times}$. Set

$$q(T) = \frac{1}{U(T)} \sum_{j=0}^{\infty} (-1)^j \varpi^j \left(\tau \circ \frac{P}{U} \right)^j \circ \tau(g).$$

The definition is a bit difficult to interpret, so for example we have

$$\left(\tau \circ \frac{P}{U} \right)^3 \circ \tau(g) = \tau \left(\frac{P}{U} \left(\tau \left(\frac{P}{U} \left(\tau \left(\frac{P}{U} \left(\tau(g) \right) \right) \right) \right) \right) \right).$$

The presence of the ϖ^j forces this to converge, so it is in $\Lambda_{\mathcal{O}}$. Using equation (4.1) we have

$$qf = \varpi q P + T^n q U.$$

Applying τ we have

$$\tau(qf) = \varpi \tau(qP) + \tau(T^n qU) = \varpi \tau(qP) + qU. \tag{4.2}$$

Now we examine $\varpi \tau(qP)$:

$$\begin{aligned}
\varpi \tau(qP) &= \varpi \tau \left(\frac{P}{U} \sum_{j=0}^{\infty} (-1)^j \varpi^j \left(\tau \circ \frac{P}{U} \right)^j \circ \tau(g) \right) \\
&= \sum_{j=0}^{\infty} (-1)^j \varpi^{j+1} \left(\tau \circ \frac{P}{U} \right)^{j+1} \circ \tau(g) \\
&= \varpi \left(\tau \circ \frac{P}{U} \right) \circ \tau(g) - \varpi^2 \left(\tau \circ \frac{P}{U} \right)^2 \circ \tau(g) + \cdots \\
&= \tau(g) - \left(\tau(g) - \varpi \left(\tau \circ \frac{P}{U} \right) \circ \tau(g) + \varpi^2 \left(\tau \circ \frac{P}{U} \right)^2 \circ \tau(g) + \cdots \right) \\
&= \tau(g) - Uq.
\end{aligned}$$

Plugging this into equation (4.2) we obtain

$$\tau(qf) = \tau(g).$$

Thus we have that $\tau(qf)$ and $\tau(g)$ differ only by a polynomial of degree less then n. To see uniqueness, suppose there exists q_1, q_2, r_1, and r_2 with $g = q_1 f + r_1 = q_2 f + r_2$. Thus we have that $(q_1 - q_2)f + (r_1 - r_2) = 0$. Suppose that $q_1 \neq q_2$ and $r_1 \neq r_2$. Then we may assume that $\varpi \nmid (q_1 - q_2)$ or $\varpi \nmid (r_1 - r_2)$. Now reduce modulo ϖ, giving us that $r_1 \equiv r_2 (\operatorname{mod} \varpi)$ since $\varpi | a_i$ for $1 \leq i \leq n-1$. Thus $\varpi | (q_1 - q_2) f$. But we know $\varpi \nmid f$ since $a_n \in \mathcal{O}^{\times}$, so we must have $\varpi | (q_1 - q_2)$, a contradiction. □

Definition 4.3. Let $P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0 \in \mathcal{O}[T]$. We call $P(T)$ *distinguished* if $a_i \in \mathfrak{p}$ for $0 \leq i \leq n-1$.

Theorem 4.4. *(p-adic Weierstrass Preparation Theorem) Let $f(T) = \sum_{i=0}^{\infty} a_i T^i \in \Lambda_{\mathcal{O}}$ and suppose there exists $n \in \mathbb{N}$ with $a_i \in \mathfrak{p}$ for $0 \leq i \leq n-1$ but $a_n \in \mathcal{O}^{\times}$. Then there exist a unique $U(T) \in \Lambda_{\mathcal{O}}$ a unit and a unique $P(T) \in \mathcal{O}[T]$ a distinguished polynomial of degree n so that*

$$f(T) = P(T)U(T).$$

If $f(T) \in \Lambda_{\mathcal{O}}$ is nonzero, then there exists a unique $\mu \in \mathbb{Z}$, $\mu \geq 0$, $P(T) \in \mathcal{O}[T]$ a distinguished polynomial of degree at most n, and a unit $U(T) \in \Lambda_{\mathcal{O}}$ so that

$$f(T) = \varpi^{\mu} P(T)U(T).$$

Proof. We begin by applying Proposition 4.2 to $g(T) = T^n$ and $f(T)$ to obtain $q(T) = \sum_{i=0}^{\infty} q_i T^i \in \Lambda_{\mathcal{O}}$ and $r(T) \in \mathcal{O}[T]$ with

$$T^n = f(T)q(T) + r(T) \tag{4.3}$$

where $\deg r(T) \leq n-1$. If we consider this equation modulo ϖ we see that

$$T^n \equiv q(T)(a_n T^n + a_{n+1}T^{n+1} + \cdots) + r(T) (\operatorname{mod} \varpi).$$

Since $\deg r(T) \leq n-1$, we must have $r(T) \equiv 0 (\operatorname{mod} \varpi)$. Thus, $T^n - r(T)$ is a distinguished polynomial, call it $P(T)$. Looking back at equation (4.3) and looking at the coefficients of T^n we have $q_0 a_n \equiv 1 (\operatorname{mod} \varpi)$. Thus, $\varpi \nmid q_0$, which implies that $q_0 \in \mathcal{O}^{\times}$, i.e., $q(T)$ is a unit. So we have

$$T^n - r(T) = f(T)q(T)$$

i.e.,

$$f(T) = P(T)U(T)$$

where $U(T) = q(T)^{-1}$.

The uniqueness statement is not difficult. Any distinguished polynomial can be written as $P(T) = T^n - r(T)$. Then translate the equation $f(T) = P(T)U(T)$ into an equation of the form $T^n = f(T)q(T) + r(T)$ and use the uniqueness in Proposition 4.2.

For the last statement, just factor out the largest power of ϖ possible. □

Corollary 4.5. *Let $f(T) \in \Lambda_{\mathcal{O}}$ be nonzero. There are only finitely many $z \in \mathbb{C}_p$ with $|z|_p < 1$ and $f(z) = 0$.*

Proof. Write $f(T) = \varpi^m P(T)U(T)$. Since U is a unit, $U(z) \neq 0$. Thus it must be that $P(z) = 0$. Since P is a polynomial we have the result. □

Lemma 4.6. *Let $P(T) \in \mathcal{O}[T]$ be distinguished and let $g(T) \in \mathcal{O}[T]$. Suppose that $\frac{g(T)}{P(T)} \in \Lambda_{\mathcal{O}}$, then $\frac{g(T)}{P(T)} \in \mathcal{O}[T]$.*

Proof. Let $f(T) \in \Lambda_{\mathcal{O}}$ so that $\dfrac{g(T)}{p(T)} = f(T)$, i.e., $g(T) = f(T)P(T)$. Let z be a root of $P(T)$. Then

$$0 = P(z) = z^n + (\text{multiple of } \varpi)$$

since P is distinguised. Then $\varpi | z$ implies $|z|_p < 1$. Thus we have $f(T)$ converges at z and so $g(z) = 0$, i.e., $(T - z)|g(T)$. Continuing in this pattern, possibly enlarging $\mathcal{O}$ to contain all the roots of $P(T)$, we see that $P(T)|g(T)$ as polynomials. □

4.3 A Structure Theorem on $\Lambda_{\mathcal{O}}$-modules

We continue with the notation of the last section. Note that from the previous section we have that $\Lambda_{\mathcal{O}}$ is a UFD whose irreducibles are ϖ and irreducible distinguished polynomials. The units are elements in $\Lambda_{\mathcal{O}}$ whose constant term is in $\mathcal{O}^{\times}$.

In this section we state a powerful structure theorem allowing us to determine the structure of finitely generated $\Lambda_{\mathcal{O}}$-modules. We will use this to study certain Galois groups in the following section.

Lemma 4.7. *Let $f, g \in \Lambda_{\mathcal{O}}$ be relatively prime. The ideal (f, g) generated by f and g is of finite index in $\Lambda_{\mathcal{O}}$.*

Proof. Let $h \in (f, g)$ have minimal degree. We can write $h(T) = \varpi^n H(T)$ for some integer n and where $H = 1$ or H is a distinguished polynomial (by Weierstrass preparation theorem). If $H \neq 1$ we can write $f = qH + r$ with $\deg r < \deg H$. This gives us

$$\begin{aligned} \varpi^n f &= q\varpi^n H + \varpi^n r \\ &= qh + \varpi^n r. \end{aligned}$$

However, this shows that $\varpi^n r \in (f, g)$ and has smaller degree then h, a contradiction. Now suppose that $H = 1$ and so $h = \varpi^n$. We may assume that $\varpi \nmid f$ for if it does divide f we can use g instead since f and g are relatively prime. We may also assume that f is distinguished for if not we can just look at $P(T) = f(T)/u(T)$ by the Weierstrass preparation theorem since this generates the same ideal. We have that $(\varpi^n, f) \subseteq (f, g)$ and so $\Lambda_{\mathcal{O}}/(\varpi^n, f) \supseteq \Lambda_{\mathcal{O}}/(g, f)$. The division algorithm shows that everything in $\Lambda_{\mathcal{O}}$ is congruent modulo (ϖ^n, f) to a polynomial of degree less then the degree of f with coefficients modulo ϖ^n. However, there are only finitely many choices for such polynomials and so (ϖ^n, f) has finite index, and hence so does (f, g). □

Lemma 4.8. *Let $f, g \in \Lambda_{\mathcal{O}}$ be relatively prime. Then:*
1. the natural map

$$\Lambda_{\mathcal{O}}/(fg) \longrightarrow \Lambda_{\mathcal{O}}/(f) \oplus \Lambda_{\mathcal{O}}/(g)$$

is an injection with finite cokernel;
2. there is an injection

$$\Lambda_{\mathcal{O}}/(f) \oplus \Lambda_{\mathcal{O}}/(g) \longrightarrow \Lambda_{\mathcal{O}}/(fg)$$

with finite cokernel.

Proof. 1. The fact that this map is an injection follows immediately from the fact that $\Lambda_{\mathcal{O}}$ is a UFD. It remains to show that the cokernel is finite. Consider $(a(\operatorname{mod} f), b(\operatorname{mod} g))$. Suppose that $a - b \in (f, g)$. Then there exists α, β so that $a - b = f\alpha + g\beta$. Set $\gamma = a - f\alpha = b + g\beta$ and observe that $\gamma \equiv a(\operatorname{mod} f)$ and $\gamma \equiv b(\operatorname{mod} g)$. Thus, γ is in the image of the map. Let $r_1, \ldots, r_n$ be the representatives of $\Lambda_{\mathcal{O}}/(f, g)$. This is a finite set by the previous lemma. We then have that

$$\{(0(\operatorname{mod} f), r_i(\operatorname{mod} g) : 1 \leq i \leq n\}$$

is a set of representatives for the cokernel of the map.
2. Set $M = \Lambda_{\mathcal{O}}/(fg)$ and $N = \Lambda_{\mathcal{O}}/(f) \oplus \Lambda_{\mathcal{O}}/(g)$. We know that $M \subseteq N$ of finite index by what we have just shown. Let P be a distinguished polynomial in $\Lambda_{\mathcal{O}}$ that is relatively prime to fg. Note that in $\Lambda_{\mathcal{O}}$, $P^k \to 0$ (where we use that $\displaystyle\bigcap_{n=0}^{\infty} (\varpi, T)^{n+1} = 0$) and so we have $P^k N \subseteq M$ for some k. Now suppose that $(P^k x, P^k y) = 0$ in N for some $(x, y) \in N$. We must have that $f \mid P^k x$ and $g \mid P^k y$. We chose P so that $\gcd(P, fg) = 1$ and so we have that necessarily $f \mid x$ and $g \mid y$. Thus, $(x, y) = 0$ in N. Hence, the map is injective:

$$N \xrightarrow{P^k} M.$$

The image of the map contains $(P^k \cdot 1, P^k \cdot 0) = (P^k, 0) = (P^k, fg)$. This is of finite index by the previous lemma, so the cokernel must be finite. □

Next we determine the prime ideals of $\Lambda_{\mathcal{O}}$ as well as show it has a unique maximal ideal.

Proposition 4.9. *The primes of $\Lambda_{\mathcal{O}}$ are $0, (\varpi, T), (\varpi)$ and the ideals $(P(T))$ for $P(T)$ irreducible and distinguished. The ideal (ϖ, T) is the unique maximal ideal.*

Proof. It is easy to see that the given ideals are prime ideals; it remains to show they are the only prime ideals. Let $\wp \subset \Lambda_{\mathcal{O}}$ be a non-zero prime ideal. Let $h \in \wp$ have minimal degree. Using the Weierstrass preparation theorem we can write $h = \varpi^n H$ with $H = 1$ or $H \in \wp$. If $H = 1$ then we cannot have $H \in \wp$ for then $\wp = \Lambda_{\mathcal{O}}$. Suppose $H \neq 1$ and $H \in \wp$. In this case H must be irreducible by the minimality of the degree of h. Thus, $(H) \subseteq \wp$. If $(H) = \wp$ we are done. Assume $(H) \neq \wp$ so that there exists $g \in \wp$ with $H \nmid g$. Since H is irreducible we must have that H and g are relatively prime. Now apply Lemma 4.7 to conclude that (H, g), and hence $\wp$, is of finite index in $\Lambda_{\mathcal{O}}$. Thus, $\Lambda_{\mathcal{O}}/\wp$ is a finite $\mathcal{O}$-module and so $\varpi^N \in \wp$ for some large N. Since $\wp$ is prime this implies

that $\varpi \in \wp$. We also have that $T^i \equiv T^j (\operatorname{mod} \wp)$ for some $i < j$ since $\wp$ is of finite index. However, $1 - T^{j-i} \in \Lambda_{\mathcal{O}}^{\times}$ implies that $T \in \wp$. Thus we have that $(\varpi, T) \subseteq \wp$. However, $\Lambda_{\mathcal{O}}/(\varpi, T) \cong \mathcal{O}/\varpi$ and so (ϖ, T) is maximal and hence $\wp = (\varpi, T)$.
One sees that this argument gives the case where $H = 1$ and $\varpi^n \in \wp$ as well. Now since all primes are contained in (ϖ, T) it is the only maximal ideal. □

Lemma 4.10. *Let $f \in \Lambda_{\mathcal{O}} - \Lambda_{\mathcal{O}}^{\times}$. Then $\Lambda_{\mathcal{O}}/(f)$ is infinite.*

Proof. Assume $f \neq 0$. The Weierstrass preparation theorem allows us to write $f = \varpi^n H$ with $H = 1$ or distinguished. Observe that $(f) \subseteq (\varpi)$ or $(f) \subseteq (H)$ and so it is enough to consider $f = \varpi$ and f distinguished. If f is distinguished one applies the division algorithm to get the result. If $f = \varpi$, $\Lambda_{\mathcal{O}}/(\varpi) \cong (\mathcal{O}/\varpi)[\![T]\!]$, which is infinite. □

Lemma 4.11. *The ring $\Lambda_{\mathcal{O}}$ is a Noetherian ring.*

Proof. Since $\mathcal{O}$ is Noetherian we apply the standard fact from algebra that A Noetherian implies $A[\![T]\!]$ is Noetherian. □

Definition 4.12. Two $\Lambda_{\mathcal{O}}$-modules M and N are said to be *pseudo-isomorphic*, written $M \sim N$, if there is an exact sequence

$$0 \longrightarrow A \longrightarrow M \longrightarrow N \longrightarrow B \longrightarrow 0$$

with A and B finite $\Lambda_{\mathcal{O}}$-modules.

Remark 4.13. One should note that $M \sim N$ does not imply that $N \sim M$. However, it is equivalent if they are finitely generated $\Lambda_{\mathcal{O}}$-torsion $\Lambda_{\mathcal{O}}$-modules.

Exercise 4.14. *Show that $(p, T) \sim \Lambda$ but $\Lambda \nsim (p, T)$.*

We conclude this section with the structure theorem that will be instrumental in proving Theorem 4.1.

Theorem 4.15. *Let M be a finitely generated $\Lambda_{\mathcal{O}}$-module. Then*

$$M \sim \Lambda_{\mathcal{O}}^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda_{\mathcal{O}}/(\varpi^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda_{\mathcal{O}}/(f_j(T)^{m_j}) \right)$$

where r, s, t, n_i and m_j are in in $\mathbb{Z}$ and $f_j(T)$ are distinguished and irreducible. This decomposition is uniquely determined by M.

Proof. The proof is essentially the same proof as the structure theorem for modules over a PID. One uses row and column operations. See ([Wash], Theorem 13.12) for the details. □

4.4 Proof of Iwasawa's theorem

In this section we prove Theorem 4.1. We do this by making use of the structure theorem of the last section. Let K be a number field and K_∞/K a $\mathbb{Z}_p$-extension with $K = K_0 \subset K_1 \subset \cdots \subset K_\infty$ with $\text{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$ as Section 4.1. Write $\Gamma = \text{Gal}(K_\infty/K)$ and let γ_0 be a topological generator of Γ. Note that the isomorphism $\mathbb{Z}_p \cong \Gamma$ is given by $x \mapsto \gamma_0^x$. Let L_n be the maximal unramified abelian p-extension of K_n. Set $X_n = \text{Gal}(L_n/K_n)$ so that X_n is the p-Sylow subgroup of the ideal class group of K_n. Note that what we are interested in is studying the power of p dividing the order of X_n. Let $L = \bigcup_{n\geq 0} L_n$, $X = \text{Gal}(L/K_\infty)$, and $G = \text{Gal}(L/K)$. Note that it is not uncommon for some authors to refer to L as L_∞. However, we have reserved the subscript ∞ to denote a $\mathbb{Z}_p$-extension. We have the following diagram of fields (including their Galois groups):

$$\begin{tikzcd}
& L \arrow[dl, dash, "X"'] \arrow[ddl, dash, "G"] \\
K_\infty \arrow[d, dash, "\Gamma"'] & \\
K &
\end{tikzcd}$$

Observe that if we take K_n for any $n \geq 0$ we have that K_∞/K_n is still a $\mathbb{Z}_p$-extension and we have the same X as for K. This will be important as we wish to reduce our arguments to the case where any prime that ramifies in K_∞ is totally ramified. We will accomplish this by replacing K with K_n for some n. We will then obtain results on X and it is important to know that this "new" X is the original one we are interested in.

Exercise 4.16. *Prove that the X one obtains from the $\mathbb{Z}_p$-extension K_∞/K_n is the same X as one obtains from the $\mathbb{Z}_p$-extension K_∞/K for any $n \geq 0$.*

Proposition 4.17. *All $\mathbb{Z}_p$-extensions are unramified away from p, i.e., if λ is a prime of K which does not lie above p, then K_∞/K is unramified at λ.*

Proof. Let $I_\lambda \subset \text{Gal}(K_\infty/K)$ be the inertia group of λ. We know the inertia group is a closed subgroup, so in this case we have I_λ is either 0 or $p^n\mathbb{Z}_p$ for some n. If $I_\lambda = 0$ we are done, so assume that $I_\lambda = p^n\mathbb{Z}_p$ for some n. The inertia group of an archimedian prime must have order 1 or 2 and since I_λ has infinite order we can rule out the case that λ is a ramified archimedian prime. For each m choose a place λ_m so that λ_m lies over λ_{m-1} and so on setting $\lambda_0 = \lambda$. We can complete each field K_m at λ_m and obtain a tower of fields $K_\lambda = K_{0,\lambda} \subset K_{1,\lambda_1} \subset \cdots$. Set $\hat{K}_\infty = \bigcup_{m\geq 0} K_{m,\lambda_m}$. Observe that $I_\lambda \subset \text{Gal}(\hat{K}_\infty/K_\lambda)$. Now let U be the units of K_λ. We know from local class field theory that there is a surjective map $U \to I_\lambda$, i.e., a surjective map

$U \to p^n\mathbb{Z}_p$. However, the local unit theorem from algebraic number theory gives that $U \cong$ (finite group) $\times \mathbb{Z}_\ell^a$ for some $a \in \mathbb{Z}$ and some prime $\ell \subset \mathbb{Z}$ with $\lambda \mid \ell$. However, we know that $p^n\mathbb{Z}_p$ has no torsion, so we must have a continuous surjective map $\mathbb{Z}_\ell^a \to p^n\mathbb{Z}_p$. Combining this with the natural projection map we obtain a continuous surjective map

$$\mathbb{Z}_\ell^a \to p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p.$$

However, this would give a closed subgroup of index p in $\mathbb{Z}_\ell^a$, which cannot happen. Thus it must be that $I_\lambda = 0$. □

Proposition 4.18. *At least one prime ramifies in the extension K_∞/K and there is an $m \geq 0$ such that every prime that ramifies in K_∞/K_m is totally ramified.*

Proof. It is easy to see that at least one prime must ramify. The maximal abelian unramified extension is a finite extension and K_∞/K is an infinite extension, so at least one prime must ramify.

We know from the previous proposition only the primes lying over p can possibly ramify, call these primes that ramify $\wp_1, \ldots, \wp_r$ and the corresponding inertia groups $I_1, \ldots, I_r$. Since each I_i is a closed subgroup, so is $\bigcap I_i$. Thus we have that there is some $m \in \mathbb{Z}$ so that

$$\bigcap I_i = p^m\mathbb{Z}_p.$$

Recall that $\mathrm{Gal}(K_m/K) \cong \mathbb{Z}/p^m\mathbb{Z} \cong \mathbb{Z}_p/p^m\mathbb{Z}_p$, so we have that $\mathrm{Gal}(K_\infty/K_m) \cong p^m\mathbb{Z}_p$ and so is contained in I_i for all $i = 1, \ldots, r$. Thus, we see that $\wp_i$ must be totally ramified in K_∞/K_m for all $i = 1, \ldots, r$. □

We now fix an m be as in Proposition 4.18.

Exercise 4.19. *For $n \geq m$ prove that $K_{n+1} \cap L_n = K_n$.*

We now make the simplifying assumption that $m = 0$. We will see how to remove this assumption shortly, but for now it makes the notation much easier. This assumption is in effect in all the lemmas as well until stated otherwise. The previous exercise shows that we have $\mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_{n+1}/K_n)$ using the following diagram of fields:

$$\begin{tikzcd}
 & L_nK_{n+1} \arrow[dl, dash] \arrow[dr, dash] & \\
L_n \arrow[dr, dash] & & K_{n+1} \arrow[dl, dash] \\
 & L_n \cap K_{n+1} &
\end{tikzcd}$$

Since we know that $X_{n+1} = \mathrm{Gal}(L_{n+1}/K_{n+1})$ and $L_nK_{n+1} \subset L_{n+1}$, we see that $\mathrm{Gal}(L_nK_{n+1}/K_{n+1})$, and hence X_n, is a quotient of X_{n+1}. Thus we have an onto map $X_{n+1} \to X_n$. Similarly, if we take K_∞ in the above exercise we have that

$$X_n = \mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_\infty/K_\infty)$$

and so we have

$$\begin{aligned}\varprojlim X_n &= \varprojlim \mathrm{Gal}(L_n/K_n)\\ &\cong \varprojlim \mathrm{Gal}(L_nK_\infty/K_\infty)\\ &= \mathrm{Gal}((\bigcup L_nK_\infty)/K_\infty)\\ &= \mathrm{Gal}(L/K_\infty)\\ &= X.\end{aligned}$$

Thus we have that X is a projective limit of the groups X_n. Recall that $\Gamma_n = \Gamma/\Gamma^{p^n} \cong \mathbb{Z}/p^n\mathbb{Z} \cong \mathrm{Gal}(K_n/K)$. The important thing to note is that the structure on Γ_n is multiplication. Let $\gamma_n \in \Gamma_n$. We extend γ_n to an element $\tilde{\gamma}_n \in \mathrm{Gal}(L_n/K)$. Let $x_n \in X_n$. There is an action of γ_n on x_n given by

$$\gamma_n \cdot x_n = \tilde{\gamma}_n x_n \tilde{\gamma}_n^{-1}.$$

Exercise 4.20. *Check that this action is well-defined. It may help to recall that X_n is abelian!*

This gives that X_n is a $\mathbb{Z}_p[\Gamma_n]$-module. (It has a $\mathbb{Z}_p$-action because it is a p-group!) Since we have shown that $X \cong \varprojlim X_n$, we can represent elements of X in the form $(x_0, x_1, \ldots, x_n, \ldots)$ with $x_i \in X_i$. Using that $\Lambda \cong \varprojlim \mathbb{Z}_p[\Gamma_n]$, we define an action of Λ on X componentwise so that X is a Λ-module. As before, if $\gamma \in \Gamma$ and $x \in X$, define

$$\gamma \cdot x = \tilde{\gamma} x \tilde{\gamma}^{-1}$$

where $\tilde{\gamma}$ is an extension of γ to $G_m := \mathrm{Gal}(L/K_m)$.

Let $\wp_1, \ldots, \wp_s$ be the primes which ramify in K_∞/K. Fix a prime $\mathfrak{p}_i$ of L lying over $\wp_i$. As usual, let $I_i = I(\mathfrak{p}_i/\wp_i) \subset G$ be the inertia group. By definition we have that L/K_∞ is unramified, so necessarily we have $I_i \cap X = \{e\}$. Thus we have an injection $I_i \hookrightarrow G/X \cong \Gamma$. Now we use that K_∞/K is totally ramified at $\wp_i$ to conclude that this injection is a surjection and hence an isomorphism. Thus,

$$G = I_iX = XI_i$$

for $i = 1, \ldots, s$. Let $\sigma_i \in I_i$ be the element that maps to the topological generator γ_0 in Γ. This gives that σ_i is a topological generator of I_i. Now using that $G = XI_1$ we have that $I_i \subset XI_1$ for $i = 1, \ldots, s$. Thus there exists $a_i \in X$ so that

$$\sigma_i = a_i\sigma_1.$$

Lemma 4.21. *We have*

$$[G, G] = (\gamma_0 - 1) \cdot X = TX.$$

Proof. We identify Γ with I_1 and define the action of Γ on X via this identification, i.e.,

$$\gamma \cdot x = \gamma x \gamma^{-1}.$$

Let $g_1, g_2 \in G$. Using that $G = \Gamma X$ we have elements $\gamma_1, \gamma_2 \in \Gamma$ and $x_1, x_2 \in X$ so that $g_1 = \gamma_1 x_1$ and $g_2 = \gamma_2 x_2$. We have

$$\begin{aligned} g_1 g_2 g_1^{-1} g_2^{-1} &= \gamma_1 x_1 \gamma_2 x_2 x_1^{-1} \gamma_1^{-1} x_2^{-1} \gamma_2^{-1} \\ &= (\gamma_1 \cdot x_1) \gamma_1 \gamma_2 x_2 x_1^{-1} \gamma_1^{-1} x_2^{-1} \gamma_2^{-1} \\ &= (\gamma_1 \cdot x_1)((\gamma_1 \gamma_2) \cdot (x_2 x_1^{-1}))(\gamma_2 \cdot x_2^{-1}) \end{aligned}$$

where we have used that Γ is abelian. Also observe that

$$\begin{aligned} ((1-\gamma_2)\gamma_1 \cdot x_1)((\gamma_1 - 1)\gamma_2 \cdot x_2) &= ((1-\gamma_2) \cdot \gamma_1 x_1 \gamma_1^{-1})((\gamma_1 - 1) \cdot \gamma_2 x_2 \gamma_2^{-1} \\ &= (\gamma_1 x_1 \gamma_1^{-1})(\gamma_2 \gamma_1 x_1^{-1} \gamma_1^{-1} \gamma_2^{-1})(\gamma_1 \gamma_2 x_2 \gamma_2^{-1} \gamma_1^{-1})(\gamma_2 x_2^{-1} \gamma_2^{-1}) \\ &= (\gamma_1 \cdot x_1)((\gamma_1 \gamma_2) \cdot (x_2 x_1^{-1}))(\gamma_2 \cdot x_2^{-1}) \end{aligned}$$

where we have used that Γ and X are abelian. Thus we have

$$g_1 g_2 g_1^{-1} g_2^{-1} = ((1-\gamma_2)\gamma_1 \cdot x_1)((\gamma_1 - 1)\gamma_2 \cdot x_2).$$

In particular, if we set $\gamma_2 = e$ and $\gamma_1 = \gamma_0$ we have that $(\gamma_0 - 1) \cdot x_2 \in [G, G]$. Thus,

$$(\gamma_0 - 1) \cdot X \subseteq [G, G].$$

Now let $\gamma \in \Gamma$ be arbitrary. Since γ_0 is a topological generator, there exists $c \in \mathbb{Z}_p$ so that $\gamma = \gamma_0^c$. Thus,

$$\begin{aligned} 1 - \gamma &= 1 - \gamma_0^c \\ &= 1 - (1+T)^c \\ &= 1 - \sum_{n=0}^{\infty} \binom{c}{n} T^n \in T\Lambda \end{aligned}$$

where we have used that γ_0 corresponds to $1 + T$. Thus we have that

$$(1-\gamma_2)\gamma_1 \cdot x_1 \in (\gamma_0 - 1) \cdot X$$

and

$$(1-\gamma_1)\gamma_2 \cdot x_2 \in (\gamma_0 - 1) \cdot X.$$

Thus, we have that $[G, G] \subseteq (\gamma_0 - 1) \cdot X$. □

Note here that the corresponding statement in [Wash] is in terms of the closure of the commutator and not the commutator itself. However, we have shown that $TX = [G, G]$ and TX is closed (it is the image of the compact set X), so we have that $[G, G]$ is its own closure.

For $n \geq 0$, define

$$\nu_n = 1 + \gamma_0 + \cdots + \gamma_0^{p^n - 1}.$$

Observe that

$$\begin{aligned}\nu_n &= \frac{\gamma_0^{p^n}-1}{\gamma_0-1}\\ &= \frac{(1+T)^{p^n}-1}{T}.\end{aligned}$$

Let Y_0 be the $\mathbb{Z}_p$-submodule of of X that is generated by $\{a_i : 2 \leq i \leq s\}$ and TX. Note here that we do not include a_1. Set $Y_n = \nu_n \cdot Y_0$. The following lemma is crucial for proving Theorem 4.1 as it allows to relate information about X back to information about X_n.

Lemma 4.22. *For $n \geq 0$ we have*

$$X_n \cong X/Y_n.$$

Proof. We begin with the base case of $n = 0$. In this case we know that $K \subset L_0 \subset L$ and that L_0 is the maximal abelian unramified p-extension of K. Since L/K is also a p-extension, it must be that L_0/K is the maximal abelian unramified p-subextension of L/K. Thus, we must have that $\mathrm{Gal}(L/L_0)$ is generated by by $\tilde{G}$ and all of the inertia groups $I_i, 1 \leq i \leq s$. In particular, we have that $\mathrm{Gal}(L/L_0)$ is the closure of the subgroup generated by $(\gamma_0 - 1) \cdot X$, I_1, and $\{a_i : 2 \leq i \leq s\}$. Thus, we have

$$\begin{aligned}X_0 &= \mathrm{Gal}(L_0/K)\\ &= G/\,\mathrm{Gal}(L/L_0)\\ &= XI_1/\overline{\langle(\gamma_0-1)\cdot X, a_2, \ldots, a_s, I_1\rangle}\\ &\cong X/\overline{\langle(\gamma_0-1)\cdot X, a_2, \ldots, a_s\rangle}\\ &= X/Y_0.\end{aligned}$$

Thus we have the case $n = 0$. Now suppose $n \geq 1$. We only need to translate the above proof into this case. Replace K by K_n and so γ_0 is replaced by $\gamma_0^{p^n}$ since $\mathrm{Gal}(K_\infty/K_n) \cong \Gamma^{p^n}$. In particular, this changes the σ_i to $\sigma_i^{p^n}$. We have that

$$\begin{aligned}\sigma_i^{k+1} &= (a_i\sigma_1)^{k+1}\\ &= a_i\sigma_1 a_i \sigma_1^{-1}\sigma_1^2 a_i \sigma_1^{-2}\cdots\sigma_1^k a_i \sigma_1^{-k}\sigma_1^{k+1}\\ &= (1+\sigma_1+\cdots+\sigma_1^k)\cdot a_i\sigma_1^{k+1}.\end{aligned}$$

Thus,

$$\sigma_i^{p^n} = (\nu_n a_i)\cdot\sigma_1^{p^n}.$$

This shows we should replace a_i in the above argument with $\nu_n \cdot a_i$. It is clear that we should replace $(\gamma_0 - 1)\cdot X$ by $(\gamma_0^{p^n} - 1)\cdot X = \nu_n(\gamma_0 - 1)\cdot X$. (Incidently, this shows how to proceed with the above proofs if one does not want to simplify to the case of $n = 0$!) Thus, the Y_0 becomes Y_n and we are done. □

Lemma 4.23. *Let M be a compact Λ-module. If $M/(p,T)M$ is finitely generated, then M is a finitely generated Λ-module. In particular, if $M/(p,T)M$ is finite, then M is a finitely generated Λ-module.*

Proof. Let U be a neighborhood of 0 in M. We have already seen that $(p,T)^n \to 0$ in Λ. Thus, given any $m \in M$ there is a neighborhood U_m so that $(p,T)^n U_m \subseteq U$ for large enough n. Now we use that M is compact to conclude we can choose a finite cover of M. Therefore, taking N to be the maximum n needed for this finite set we have that $(p,T)^N M \subset U$. Since U is an arbitrary neighborhood of 0, we have that $\cap((p,T)^n M) = 0$. Now let $m_1, \ldots, m_n$ generate $M/(p,T)M$. Set $N = \Lambda m_1 + \cdots \Lambda m_n \subseteq M$. Observe that N is compact since it is the image of Λ, thus it is closed. This implies that M/N is a compact Λ-module. Our assumption that $m_1, \ldots, m_n$ generates $M/(p,T)M$ gives that $N+(p,T)M = M$. Thus we have

$$(p,T)(M/N) = (N + (p,T)M)/N = M/N.$$

Hence,

$$(p,T)^n(M/N) = (M/N)$$

for all $n \geq 0$. Now from what we've shown above we get that $M/N = 0$, i.e., $m_1, \ldots, m_n$ generate M. □

Corollary 4.24. *The Λ-module $X = \mathrm{Gal}(L/K_\infty)$ is a finitely generated module.*

Proof. Recall that $\nu_1 = \dfrac{(1+T)^p - 1}{T}$. It is clear that $\nu_1 \in (p,T)$. Thus we have that $Y_0/(p,T)Y_0$ is a quotient of $Y_0/\nu_1 \cdot Y_0 = Y_0/Y_1 \subsetneq X/Y_1 = X_1$. We know that X_1 is a finite set and so we get that $Y_0/(p,T)Y_0$ is finite and applying Lemma 4.23 we get that Y_0 is finitely generated. Now $X/Y_0 = X_0$, which is finite, thus X itself must be finitely generated as a Λ-module. □

Of course all of these results have been shown under the assumption that K_∞/K is totally ramified at the primes that ramify. We now remove this assumption. Let K_∞/K be a $\mathbb{Z}_p$-extension and let K_m be as in Proposition 4.18. Recall that X is the same for K as for K_m. Therefore we have that X is a finitely generated Λ-module by Corollary 4.24. For $n \geq m$, we replace ν_n by $\nu_{n,m}$ given by

$$\begin{aligned}\nu_{n,m} &= \frac{\nu_n}{\nu_m} \\ &= 1 + \gamma_0^{p^m} + \gamma_0^{2p^m} + \cdots + \gamma_0^{p^n - p^m}.\end{aligned}$$

Note that this works out because $\mathrm{Gal}(K_\infty/K_m) \cong \Gamma^{p^m}$ is generated by $\gamma_0^{p^m}$. Making these appropriate substitutions we obtain

Lemma 4.25. *Let K_∞/K be a $\mathbb{Z}_p$-extension. One has X is a finitely generated Λ-module and there exists $m \geq 0$ so that*

$$X_n \cong X/\nu_{n,m} \cdot Y_m$$

for every $n \geq m$ where Y_m is defined as above.

We are now in a position to apply our structure theorem on finitely generated Λ-modules (Theorem 4.15) to X as well as Y_m. Observe that we obtain the same answer whether we use X or Y_m. This is because X/Y_m is finite and the theorem is given in terms of a pseudo-isomorphism. Thus, we have

$$X \sim Y_m \sim \Lambda^r \oplus \left(\bigoplus \Lambda/(p^{\mu_i})\right) \oplus \left(\bigoplus \Lambda/(f_j(T)^{m_j})\right). \tag{4.4}$$

Our next step is to calculate $M/\nu_{n,m} \cdot M$ for each summand M on the right side of equation (4.4). We will be able to use this to obtain the bounds we desire on $|X_n|$.

Case 1: $M = \Lambda$

Observe that $\nu_{n,m}$ is not a unit in Λ, in fact, it is a distinguished polynomial! In particular, we can apply Lemma 4.10 to conclude that $\Lambda/(\nu_{n,m})$ is infinite. However, we already know that $Y_m/\nu_{n,m} \cdot Y_m$ is finite. Thus we must have that $r = 0$.

Case 2: $M = \Lambda/(p^k)$ for some $k > 0$.

In this case we need to investigate $\Lambda/(p^k, \nu_{n,m})$. It was remarked above that $\nu_{n,m}$ is a distinguished polynomial. We can apply the division algorithm to conclude that the elements of $\Lambda/(p^k, \nu_{n,m})$ are precisely the polynomials modulo p^k of degree less then $\deg \nu_{n,m} = p^n - p^m$. Hence,

$$|M/\nu_{n,m}M| = (p^k)^{p^n - p^m} = p^{kp^n + c}$$

where $c = -kp^m$, a constant depending on the field K.

Case 3: $M = \Lambda/(f(T)^r)$

Let $g(T) = f(T)^r$. Suppose g has degree d. Since f is a distinguished polynomial, so is g. Thus we have that

$$T^k \equiv p \cdot (\text{poly}) (\operatorname{mod} g)$$

for $k \geq d$. Note that we will use "poly" to stand for a polynomial several times in this argument, it is not meant to be the same polynomial at each step. Let $p^n \geq d$. We have

$$\begin{aligned} (1+T)^{p^n} &= 1 + p \cdot (\text{poly}) + T^{p^n} \\ &\equiv 1 + p \cdot (\text{poly}) (\operatorname{mod} g). \end{aligned}$$

In particular, we see that

$$\begin{aligned} (1+T)^{p^{n+1}} &= ((1+T)^{p^n})^p \\ &\equiv (1 + p \cdot (\text{poly}))^p (\operatorname{mod} g) \\ &\equiv 1 + p^2 \cdot (\text{poly}) (\operatorname{mod} g). \end{aligned}$$

Set $P_n(T) = (1+T)^{p^n} - 1$. We have

$$\begin{aligned} P_{n+2}(T) &= (1+T)^{p^{n+2}} - 1 \\ &= ((1+T)^{p^{n+1}} - 1)(1 + (1+T)^{p^{n+1}} + \cdots + (1+T)^{p^{n+1}(p-1)}) \\ &= P_{n+1}(T)(1 + (1+T)^{p^{n+1}} + \cdots + (1+T)^{p^{n+1}(p-1)}) \\ &\equiv P_{n+1}(T)(1 + \cdots + 1 + p^2 \cdot (\text{poly}))(\operatorname{mod} g) \\ &\equiv P_{n+1}(T)(p + p^2 \cdot (\text{poly}))(\operatorname{mod} g) \\ &\equiv p(1 + p \cdot (\text{poly}))P_{n+1}(T)(\operatorname{mod} g). \end{aligned}$$

Using that $1 + p \cdot (\text{poly})$ is necessarily a unit in Λ, we see that $\dfrac{P_{n+2}(T)}{P_{n+1}(T)}$ acts on $\Lambda/(g)$ as p times a unit as long as $p^n \geq d$.
Assume now that we have $n_0 > m$, $p^{n_0} \geq d$, and $n \geq n_0$. Observe that

$$\frac{\nu_{n+2,m}}{\nu_{n+1,m}} = \frac{\nu_{n+2}}{\nu_{n+1}} = \frac{P_{n+2}}{P_{n+1}}.$$

Thus,

$$\begin{aligned} \nu_{n+2,m}M &= \frac{P_{n+2}}{P_{n+1}}\nu_{n+1,m}M \\ &= p\nu_{n+1,m}M. \end{aligned}$$

Therefore we have

$$|M/\nu_{n+2,m}M| = |M/pM| \cdot |pM/p\nu_{n+1,m}M|.$$

Note that since g is a distinguished polynomial we have $\gcd(p,g) = 1$. In particular, this means that multiplication by p is an injective map. Thus,

$$|pM/p\nu_{n+1,m}M| = |M/\nu_{n+1,m}M|.$$

We also have

$$M/pM \cong \Lambda/(p,g) = \Lambda/(p,T^d),$$

and so $|M/pM| = p^d$.

Exercise 4.26. *Prove that*

$$|M/\nu_{n,m}M| = p^{d(n-n_0-1)}|M/\nu_{n_0+1,m}M|$$

for $n \geq n_0 + 1$.

Therefore, if $|M/\nu_{n,m}M|$ is finite for all n we obtain $|M/\nu_{n,m}M| = p^{dn+c}$ for $n \geq n_0 + 1$ and c a constant depending on the field K. If $M/\nu_{n,m}M$ is infinite for any n, then M cannot occur as was observed in Case 1. Thus we have shown the following.

Proposition 4.27. *Suppose*

$$N = \Lambda^r \oplus \left(\bigoplus \Lambda/p^{\mu_i}\right) \oplus \left(\bigoplus \Lambda/(f_j(T))\right)$$

where each f_j is distinguished. Let $\mu = \sum \mu_i$ and $\lambda = \sum \deg f_j$. If $N/\nu_{n,m}N$ is finite for all n, then $r = 0$ and there exists n_0 and c such that

$$|N/\nu_{n,m}N| = p^{\mu p^n + \lambda n + c}$$

for all $n \geq n_0$.

We know that Y_m is pseudo-isomorphic to an appropriate N as given in the previous proposition. We also know the order of $N/\nu_{n,m}N$ for all $n \geq n_0$. Therefore, it remains to relate this order to the order of $Y_m/\nu_{n,m}Y_m$. The issue here is that the "A" and "B" we obtain in using the definition of pseudo-isomorphism could vary with n. We know from the above lemma that the order of $Y_m/\nu_{n,m}Y_m$ is determined as we want it up to the order of A and B, so we need to show that for large enough n the orders of these are constant as well. The main work left is contained in the following lemma, which is essentially an exercise in applying the Snake Lemma.

Lemma 4.28. *Suppose M and N are Λ-modules with $M \sim N$ and $M/\nu_{n,m}M$ is finite for all $n \geq m$. For some constant a and some n_0 one has*

$$|M/\nu_{n,m}M| = p^a |N/\nu_{n,m}N|$$

for all $n \geq n_0$

Proof. The fact that $M \sim N$ implies that t we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker\phi \arrow[r] & M \arrow[r, "\phi"] & N \arrow[r] & \operatorname{coker}\phi \arrow[r] & 0 \end{tikzcd}$$

with $\ker\phi$ and $\operatorname{coker}\phi$ finite. Using this exact sequence we obtain the following commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & \ker\phi'_n \arrow[d] & \ker\phi \arrow[d] & \ker\phi''_n \arrow[d] & \\
0 \arrow[r] & \nu_{n,m}M \arrow[r] \arrow[d, "\phi'_n"] & M \arrow[r] \arrow[d, "\phi"] & M/\nu_{n,m}M \arrow[r] \arrow[d, "\phi''_n"] & 0 \\
0 \arrow[r] & \nu_{n,m}N \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & N/\nu_{n,m}N \arrow[r] \arrow[d] & 0 \\
 & \operatorname{coker}\phi'_n \arrow[d] & \operatorname{coker}\phi \arrow[d] & \operatorname{coker}\phi''_n \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Our goal is to prove that for large enough n we have $|\ker\phi''_n|$ and $|\operatorname{coker}\phi''_n|$ are constant. We prove this by showing each is bounded and decreasing. We begin by showing each is bounded. It is clear that $|\operatorname{coker}\phi''_n| \leq |\operatorname{coker}\phi|$ since one obtains representatives of $\operatorname{coker}\phi''_n$ from those of $\operatorname{coker}\phi$. To see that $|\ker\phi''_n|$ we apply the snake lemma to obtain the long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \ker\phi'_n \arrow[r] & \ker\phi \arrow[r] & \ker\phi''_n \arrow[r] & {} \\
\operatorname{coker}\phi'_n \arrow[r] & \operatorname{coker}\phi \arrow[r] & \operatorname{coker}\phi''_n \arrow[r] & 0.
\end{tikzcd}$$

From this we see that

$$\begin{aligned}|\ker\phi''_n| &\leq |\ker\phi|\cdot|\operatorname{coker}\phi'_n| \\ &\leq |\ker\phi|\cdot|\operatorname{coker}\phi|\end{aligned}$$

where we have used that $|\operatorname{coker}\phi'_n| \leq |\operatorname{coker}\phi|$, which follows from the fact that one obtains representatives of $\operatorname{coker}\phi'_n$ by multiplying those of $\operatorname{coker}\phi$ by $\nu_{n,m}$. Thus, $|\ker\phi''_n|$ is bounded as well.

We now show that $|\operatorname{coker}\phi''_n|$ is decreasing. Let $n' \geq n \geq 0$. Then we have $|\operatorname{coker}\phi''_{n'}| \leq |\operatorname{coker}\phi''_n|$ since $\nu_{n',m}N = \nu_{n,m}\left(\frac{\nu_{n',m}}{\nu_{n,m}}\right)N \subseteq \nu_{n,m}N$. Thus, we have for large enough n that $|\operatorname{coker}\phi''_n|$ is constant.

It only remains to show that $|\ker\phi''_n|$ is constant for large enough n. Using the snake lemma we have

$$|\ker\phi'_n|\cdot|\ker\phi''_n|\cdot|\operatorname{coker}\phi| = |\ker\phi|\cdot|\operatorname{coker}\phi'_n|\cdot|\operatorname{coker}\phi''_n|,$$

Thus, we need to show that for large enough n one has $|\ker\phi'_n|$ and $|\operatorname{coker}\phi'_n|$ are constants. It is clear from the commutative diagram that $\ker\phi'_n \subset \ker\phi$, so we easily obtain that $|\ker\phi'_n|$ is bounded. To see it is decreasing, just observe that $\nu_{n',m}M \subseteq \nu_{n,m}M$, which in turn implies that $\ker\phi'_{n'} \subseteq \ker\phi'_n$.

We now deal with $|\operatorname{coker}\phi'_n|$. The fact that $|\operatorname{coker}\phi'_n| \le |\operatorname{coker}\phi|$ was mentioned above. Now we need to show that $|\operatorname{coker}\phi'_n|$ is decreasing. Let $\nu_{n',m}y \in \nu_{n',m}N$. Fix a set of representatives of $\operatorname{coker}\phi'_n$ and let $z \in \nu_{n,m}N$ be the representative for $\nu_{n,m}y$ in $\operatorname{coker}\phi'_n$. Observe that

$$\nu_{n,m}y - z = \phi(\nu_{n,m}x)$$

for some $x \in M$ since it is necessarily in $\operatorname{im}(\phi'_n)$ and this injects into $\operatorname{im}(\phi)$. Thus we have

$$\left(\frac{\nu_{n',m}}{\nu_{n,m}}\right)\nu_{n,m}y - \left(\frac{\nu_{n',m}}{\nu_{n,m}}\right)z = \left(\frac{\nu_{n',m}}{\nu_{n,m}}\right)\phi(\nu_{n,m}x),$$

i.e., we have

$$\begin{aligned}\nu_{n',m}y - \left(\frac{\nu_{n',m}}{\nu_{n,m}}\right)z &= \phi(\nu_{n',m}x)\\ &= \phi'_{n'}(\nu_{n',m}x).\end{aligned}$$

Thus, by multiplying representatives of $\operatorname{coker}\phi'_n$ by $\dfrac{\nu_{n',m}}{\nu_{n,m}}$ we obtain representatives for $\operatorname{coker}\phi'_{n'}$, which proves that $|\operatorname{coker}\phi'_{n'}| \le |\operatorname{coker}\phi'_n|$.

Summarizing, we have the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker\phi''_n \arrow[r] & M/\nu_{n,m}M \arrow[r] & N/\nu_{n,m}N \arrow[r] & \operatorname{coker}\phi''_n \arrow[r] & 0. \end{tikzcd}$$

and n_0 so that if $n \ge n_0$ then the terms $|\ker\phi''_n|$ and $|\operatorname{coker}\phi''_n|$ are constant and thus we obtain the result. □

It is now simple to complete the proof of Theorem 4.1. We have shown that there exists integers n_0, ν, $\lambda \ge 0$, and $\mu \ge 0$ so that

$$\begin{aligned}p^{e_n} &= |X_n|\\ &= |X/Y_m| \cdot |Y_m/\nu_{n,m}Y_m|\\ &= p^b|N/\nu_{n,m}N|\\ &= p^{\lambda n+\mu p^n+\nu}\end{aligned}$$

for all $n \ge n_0$.

We close this section with some applications of the work we have done. Recall that $X_n \cong A_n$ where A_n is the p-Sylow subgroup of the ideal class group of K_n. In general we continue to use X_n in our notation with the exception of incorporating the common notation that h_n denotes the order of the class group of K_n. In particular, the order of A_n is the p-part of h_n. We will also need Nakayama's Lemma.

Lemma 4.29. *(Nakayama's Lemma) Let M be a finitely generated R-module and I an ideal of R contained in the Jacobson radical of R. Then $IM = M$ implies $M = 0$.*

Proof. See Proposition 2.6 in [AM]. □

Proposition 4.30. *Let K_∞/K be a $\mathbb{Z}_p$-extension in which exactly one prime ramifies. Moreover, assume the prime that ramifies is totally ramified. Then we have*

$$X_n \cong X/((1+T)^{p^n} - 1)X$$

and $p \nmid h_0$ if and only if $p \nmid h_n$ for all $n \geq 0$.

Proof. We begin by observing that K_∞/K satisfies the assumption we were working under when we proved Lemma 4.22. In particular, $s = 1$ and so $Y_0 = TX$. Thus,

$$\begin{aligned} Y_n &= \nu_n TX \\ &= \left(\frac{(1+T)^{p^n} - 1}{T}\right) TX, \end{aligned}$$

which clearly gives the first result.
Suppose $p \nmid h_0$. In particular, this gives that $X_0 = 0$, i.e., $X/TX = 0$. However, this implies that $X/(p,T)X = 0$. Combining this with Nakayama's Lemma we have that $X = 0$ and we are done. □

One should observe that we cannot apply Theorem 4.1 directly to conclude the statement about divisibility of h_n because Theorem 4.1 is only true for $n \geq n_0$ for some n_0 and not all $n \geq 0$.

Definition 4.31. Let A be a finite abelian group. The *p-rank of A* is given by

$$p\text{-rank}(A) = \dim_{\mathbb{Z}/p\mathbb{Z}}(A/pA).$$

Lemma 4.32. *Let N be given by*

$$N = \left(\bigoplus_{i=1}^{s} \Lambda/(p^{\mu_i})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T))\right)$$

where the f_j are distinguished polynomials. Set $\mu = \sum k_i$. Then $\mu = 0$ if and only if p-rank $(N/\nu_{n,m}N)$ is bounded as $n \to \infty$.

Proof. Recall that $\nu_{n,m}$ is a distinguished polynomial of degree $p^n - p^m$. Therefore, if take n large enough so that $p^n - p^m$ is larger then the maximum of the degrees of the f_j, we have

$$\begin{aligned} N/(p,\nu_{n,m})N &= \left(\bigoplus_{i=1}^{s}\Lambda/(p,\nu_{n,m})\right)\oplus\left(\bigoplus_{i=1}^{t}\Lambda/(p,f_j,\nu_{n,m})\right)\\ &= \left(\bigoplus_{i=1}^{s}\Lambda/(p,T^{p^n-p^m})\right)\oplus\left(\bigoplus_{i=1}^{t}\Lambda/(p,T^{\deg f_j})\right)\\ &\cong (\mathbb{Z}/p\mathbb{Z})^{s(p^n-p^m)+\lambda} \end{aligned}$$

for $\lambda = \sum \deg f_j$. From this last equation it is clear that the p-rank is bounded if and only if $s = 0$, i.e., if and only if $\mu = 0$. □

Proposition 4.33. *Let μ be as in Theorem 4.1. Then $\mu = 0$ if and only if p-rank (X_n) is bounded as $n \to \infty$.*

Proof. The previous lemma implies that $\mu = 0$ if and only if p-rank $(N/\nu_{n,m}N)$ is bounded where N is as above. Recall we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker\phi_n'' \arrow[r] & Y_m/\nu_{n,m}Y_m \arrow[r, "\phi_n''"] & N/\nu_{n,m}N \arrow[r] & \operatorname{coker}\phi_n'' \arrow[r] & 0 \end{tikzcd}$$

where we know $|\ker\phi_n''|$ and $|\operatorname{coker}\phi_n''|$ are bounded independent of n for large enough n. This implies that $\mu = 0$ if and only if p-rank $(Y_m/\nu_{n,m}Y_m)$ is bounded. However, we know that $X_n \cong X/\nu_{n,m}Y_m$ and $X/Y_m \cong X_m$ is finite. Thus, X_n differs from $Y_m/\nu_{n,m}Y_m$ by a finite group bounded independent of n. The result now follows. □

Chapter 5

The Iwasawa Main Conjecture

5.1 Introduction

In this section we will give the necessary background and then state the Iwasawa main conjecture. The goal is to understand the statement of the main conjecture for totally real fields as well as to outline Wiles' proof. We will state the main conjecture for totally real fields, but then restrict ourselves to the case of $\mathbb{Q}$ to outline the proof. The main conjecture was known for abelian extensions of $\mathbb{Q}$ by work of Mazur and Wiles ([MW]) by geometric methods, but we outline here the methods used to prove the conjecture for totally real fields. Our restriction to $\mathbb{Q}$ is one of convenience, allowing us to work with classical rather then Hilbert modular forms. For the general case the reader should consult Wiles' original paper [Wiles2]. Though this section is phrased in terms of totally real fields, one should keep in mind the corresponding statements for abelian extensions as these are the ones that will be used in section 5.2.

Let F be a totally real number field and let $F \subset F_1 \subset \cdots \subset F_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of F. Let $\gamma_0 \in \operatorname{Gal}(F_\infty/F)$ be the element corresponding to $1 \in \mathbb{Z}_p$ under the isomorphism $\operatorname{Gal}(F_\infty/F) \cong \mathbb{Z}_p$ so that γ_0 is a topological generator of $\operatorname{Gal}(F_\infty/F)$. One should observe that F_∞, and hence all the F_n, is totally ramified at p. Thus, the inertia group at p is the entire Galois group.

Let χ be a p-adic valued Artin character of F and F^χ the associated field. Recall this means that χ factors through $\operatorname{Gal}(F^\chi/F)$. Following Wiles we say χ is of type S if $F^\chi \cap F_\infty = F$ and of type W if $F^\chi \subset F_\infty$. Note that in [Wash] these are referred to as type 1 and type 2. We will assume throughout that F^χ is totally real as well.

Exercise 5.1. *Let $F = \mathbb{Q}$ and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Q}}_p^\times$ be a primitive Dirichlet character. Prove that χ is type S if and only if $\operatorname{ord}_p(N) \leq 1$. It may be helpful to consider the ramification of p.*

Assume now that χ is of type S. Set $F_n^\chi = F_n F^\chi$ so that $F_\infty^\chi = F_\infty F^\chi = \bigcup F_n^\chi$. The fact that χ is of type S gives the isomorphisms

$$\Gamma = \mathrm{Gal}(F_\infty^\chi / F^\chi) \xrightarrow{\sim} \mathrm{Gal}(F_\infty / F) \cong \mathbb{Z}_p$$

and

$$\Delta = \mathrm{Gal}(F_\infty^\chi / F_\infty) \xrightarrow{\sim} \mathrm{Gal}(F^\chi / F)$$

One obtains similar isomorphisms replacing F_∞^χ and F_∞ by F_n^χ and F_n respectively. We think of γ_0 as an element of Γ. We have the following diagram.

$$\begin{tikzcd}
& F_\infty^\chi \arrow[dl, dash, "\Gamma"'] \arrow[dr, dash, "\Delta"] & \\
F^\chi \arrow[dr, dash] & & F_\infty \arrow[dl, dash, "\mathbb{Z}_p"] \\
& F &
\end{tikzcd}$$

As in chapter 4 we let L_n denote the maximal abelian unramified pro-p extension of F_n^χ. Set $X_n = \mathrm{Gal}(L_n / F_n^\chi)$ so that X_n is isomorphic to the p-Sylow subgroup of the ideal class group of F_n^χ. Let $L = \bigcup L_n F_n^\chi$ and observe we have

$$\begin{aligned}
X &= \mathrm{Gal}(L / F_\infty^\chi) \\
&= \varprojlim \mathrm{Gal}(L_n F_\infty^\chi / F_\infty^\chi) \\
&\cong \varprojlim \mathrm{Gal}(L_n / F_n^\chi) \\
&\cong \varprojlim X_n
\end{aligned}$$

as in chapter 4. We have the following diagram of fields:

$$\begin{tikzcd}
& & L \arrow[dl, dash] \arrow[dr, dash, "X"] & & \\
& L_n \arrow[dl, dash] \arrow[dr, dash, "X_n"] & & F_\infty^\chi \arrow[dl, dash, "\Gamma^{p^n}"] \arrow[dr, dash, "\Delta"] & \\
L_0 \arrow[dr, dash, "X_0"'] & & F_n^\chi \arrow[dl, dash, "\Gamma/\Gamma^{p^n}"] \arrow[dr, dash] & & F_\infty \arrow[dl, dash, "p^n\mathbb{Z}_p"] \\
& F^\chi \arrow[dr, dash] & & F_n \arrow[dl, dash, "\mathbb{Z}/p^n\mathbb{Z}"] & \\
& & F & &
\end{tikzcd}$$

As before we have that $\mathrm{Gal}(F_\infty^\chi/F) \cong \Delta\times\Gamma$ acts on X via conjugation. Since X is pro-p we also have a natural action of $\mathbb{Z}_p$ on X. Thus X is a $\mathbb{Z}_p[\![\Delta \times \Gamma]\!]$-module and hence a $\mathbb{Z}_p[\![\Gamma]\!]$-module. We will again make use of the fact that $\mathbb{Z}_p[\![\Gamma]\!] \cong \Lambda = \mathbb{Z}_p[\![T]\!]$ via $\gamma_0 \mapsto 1+T$. Recall we saw in chapter 4 that

$$X \sim \left(\bigoplus_i \Lambda/(p^{\mu_i})\right) \oplus \left(\bigoplus_j \Lambda/(f_j(T)^{m_j})\right) \tag{5.1}$$

with the $f_j(T)$ irreducible and distinguished in $\mathbb{Z}_p[T]$.

Set $V = X \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p$. We have

$$V \cong \bigoplus_j \overline{\mathbb{Q}}_p[T]/(f_j(T)^{m_j})$$

as tensoring with $\overline{\mathbb{Q}}_p$ kills the kernel, cokernel, and the $\Lambda/(p^{\mu_i})$'s in equation (5.1). Thus, V is a finite dimensional vector space. Setting

$$f_X(T) = \prod_j f_j(T)^{m_j}$$

and recalling that $T \leftrightarrow \gamma_0 - 1$ under the isomorphism $\Lambda \cong \mathbb{Z}_p[\![\Gamma]\!]$ we see that $f_X(T)$ is the characteristic polynomial of $\gamma_0 - 1$ acting on V. We can gain more information by recalling our previous work on orthogonal idempotents. The vector space V is clearly a $\overline{\mathbb{Q}}_p[\Delta]$-module, so we have

$$V = \bigoplus_{\psi\in\Delta^\wedge} \varepsilon_\psi V.$$

Recall that we can view χ as a character of $\mathrm{Gal}(F^\chi/F) \cong \Delta$. We are interested in

$$V^\chi = \varepsilon_\chi V = \{v \in V : \sigma v = \chi(\sigma)v \ \ \forall\, \sigma \in \Delta\}.$$

It is clear that V^χ is still a Γ-module (γ_0 acts as $1{+}T$ as before.) Set $f_\chi(T)$ to be the characteristic polynomial of $\gamma_0 - 1$ acting on V^χ. Note that $f_\chi(T) \mid f_X(T)$. This characteristic polynomial gives us half of the information we need to state the main conjecture. Before moving to the other half, one should observe that by tensoring up with $\overline{\mathbb{Q}}_p$ we lose all of the information contained in $\mu_\chi = \sum \mu_i$ in equation (5.1). We will return to this and see how we can reformulate the above approach to preserve this data.

It is now necessary to revisit p-adic L-functions. For the field $\mathbb{Q}$ these were introduced in chapter 3. In this chapter the basic properties such as the interpolation of classical L-functions was stated. Given a character ψ of a totally real field F so that F^ψ is again totally real Deligne and Ribet ([DR]) proved the existence of a p-adic L-function $\mathcal{L}_p(s,\psi)$ associated to ψ generalizing the one already discussed for $\mathbb{Q}$ with the same interpolation properties. Define

$$H_\psi(T) = \begin{cases} \psi(\gamma_0)(1+T) - 1 & \psi \text{ of type W or trivial} \\ 1 & \text{otherwise.} \end{cases}$$

Deligne and Ribet also proved that there exists $G_\psi(T) \in \mathbb{Z}_p[\psi][\![T]\!]$ such that

$$\mathcal{L}_p(1-s,\psi) = G_\psi((1+p)^s - 1)/H_\psi((1+p)^s - 1)$$

where $\mathcal{O}_\psi := \mathbb{Z}_p[\psi]$ is the ring generated over $\mathbb{Z}_p$ by the values of ψ. We will use the notation Λ_ψ to denote $\mathcal{O}_\psi[\![T]\!]$. We will also need that if ρ is a character of type W then

$$G_{\psi\rho}(T) = G_\psi(\rho(\gamma_0)(1+T) - 1).$$

Let χ be an odd character and set $\psi = \chi^{-1}\omega$ where ω again denotes the Teichmuller character. Since ψ is an even character we have the existence of the p-adic L-function along with G_ψ. Applying the Weierstrass preparation theorem to $G_\psi((1+p)(1+T)^{-1} - 1)$ we have

$$G_\psi((1+p)(1+T)^{-1} - 1) = \varpi^{\mu_\chi^{\mathrm{an}}} g_\psi(T) u_\psi(T)$$

where ϖ is a uniformizer of $\mathcal{O}_\psi$, $g_\psi(T)$ is a distinguished polynomial, and $u_\psi(T)$ is a unit in Λ_ψ. Note that the "an" is added to the μ_χ to distinguish it as the "analytic" μ-invariant. Observe that if χ is of type S then $H_\psi(T) = 1$ unless $\chi = \omega$.

Theorem 5.2. *(Main conjecture of Iwasawa theory) For χ odd of type S and p an odd prime one has*

$$f_\chi(T) = g_{\chi^{-1}\omega}(T).$$

For what is known in the case of $p = 2$ the reader should consult [Wiles2]. Note we do not need the assumption that χ is of type S for the abelian extensions of $\mathbb{Q}$. See [MW] for the statements in this case.

As was mentioned above, because of the fact that we formed a vector space V from X by tensoring up with $\overline{\mathbb{Q}}_p$ we lost the information contained in μ_χ and μ_χ^{an} in the main conjecture. We now describe another approach so as to retain this information. Suppose now that in addition to being odd of type S that χ also has order prime to p. We write X^χ to denote $(X \otimes_{\mathbb{Z}_p} \mathcal{O}_\chi)^\chi$ where

$$\begin{aligned}(X \otimes_{\mathbb{Z}_p} \mathcal{O}_\chi)^\chi &= \{x \in X \otimes_{\mathbb{Z}_p} \mathcal{O}_\chi : \sigma x = \chi(\sigma)x \ \ \forall\, \sigma \in \Delta\} \\ &\cong X \otimes_{\mathbb{Z}_p[\Delta]} \mathcal{O}_\chi.\end{aligned}$$

where $\mathcal{O}_\chi$ is viewed as a $\mathbb{Z}_p[\Delta]$-module via the ring homomorphism induced by χ. One should note that it is necessary for us to tensor with $\mathbb{Z}_p[\chi]$ for this to make sense. In particular, without tensoring up with $\mathbb{Z}_p[\chi]$ the term $\chi(\sigma)x$ does not make sense. We have that X^χ is a finitely generated torsion Λ_χ-module and has characteristic polynomial of form $\varpi^{\mu_\chi} f_\chi(T)$.

Theorem 5.3. *(μ-invariant conjecture) Let p be an odd prime and χ an odd character of order prime to p of type S. Then*

$$\mu_\chi = \mu_\chi^{\mathrm{an}}.$$

The strong form of the μ-invariant conjecture also asserts that these μ-invariants are 0 for cyclotomic $\mathbb{Z}_p$-extensions. For abelian extensions the strong version of the conjecture is know, see ([Wash], Theorem 7.15) for example. However, it is known that for non cyclotomic $\mathbb{Z}_p$-extensions that the μ-invariants may not be zero. For example, Iwasawa constructed a non-cyclotomic $\mathbb{Z}_p$-extension with $\mu > 0$ in [Iwas1].

There is a more compact way to state main conjectures that captures Theorems 5.2 and 5.3 in one statement. Let M be a module so that

$$M \sim \left(\bigoplus_i \Lambda/p^{\mu_i} \right) \oplus \left(\bigoplus_j \Lambda/(f_j(T)^{m_j}) \right)$$

with the $f_j(T)$ irreducible and distinguished. The ideal generated by the characteristic polynomial $p^{\sum \mu_i} \prod f_j(T)^{m_j}$ is called the *characteristic ieal* of M and we write it as $\mathrm{char}_\Lambda(M)$. The main conjecture can then be stated as the following equality of ideals in Λ_χ

$$\mathrm{char}_{\Lambda_\chi}(X^\chi) = (G_{\chi^{-1}\omega}((1+p)(1+T)^{-1} - 1)).$$

Note here that the $u_{\chi^{-1}\omega}(T)$ that occurs in the application of Weierstrass preparation to $G_{\chi^{-1}\omega}((1+p)(1+T)^{-1}-1)$ is a unit in Λ_χ so plays no role in the above equality.

Proving a "main conjecture" is a very difficult task. Currently there are two basic methods used to proved main conjectures. The easiest one to apply is the use of an Euler system. Unfortunately, constructing an Euler system is very difficult in its own right and very few Euler systems are known. Kolyvagin was able to significantly simplify Mazur and Wiles' proof of the main conjecture for $\mathbb{Q}$ by using an appropriate Euler system. For more information on Euler systems the reader is urged to consult [Rubin].

The other method is the "geometric" method. In this method one uses congruences and p-adic representations coming from modular forms. This is the method we will be concerned with. We will develop some of the necessary background material in the following sections before giving an outline of the argument used. However, before we develop the background we give one application of the main conjecture to the size of class groups in the next section.

5.2 The Main Conjecture and Class Groups

Let p be an odd prime and let F be an abelian imaginary extension of $\mathbb{Q}$ of degree prime to p. Let $\chi : \mathrm{Gal}(F/\mathbb{Q}) \to \mathcal{O}_\chi^\times$ be an odd character. Set $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. We view χ as a character on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $g = [\mathcal{O}_\chi : \mathbb{Z}_p]$. Write A_F for the p-Sylow subgroup of the class group of F. As usual, we write A_F^χ to denote the χ-isotypical piece of A_F, namely,

$$A_F^\chi = A_F \otimes_{\mathbb{Z}_p[\Delta]} \mathcal{O}_\chi.$$

The goal of this section is to use the main conjecture to prove the following result.

Theorem 5.4. *Suppose $\chi \neq \omega$, then*

$$|A_F^\chi| = |\mathcal{O}_\chi/(\mathcal{L}_p(0, \chi^{-1}\omega))|.$$

In particular,

$$v_p(|A_F^\chi|) = g v_p(L(0, \chi^{-1}))$$

where $v_p(a)$ denotes the p-adic valuation of a.

Though the theorem is true as stated, the case that $\chi(p) = 1$ is much more difficult to prove so we stick to the case that $\chi(p) \neq 1$. See ([MW], Chapter 1 § 10).

We begin by reducing to the case that $F = \mathbb{Q}^\chi$. To see this we prove something slightly more general. Let K/E be an abelian extension of number fields with $[K : E]$ prime to p and χ factors through $\mathrm{Gal}(E/\mathbb{Q})$. We show that the natural mapping

$$A_E^\chi \to A_K^\chi$$

is in fact an isomorphism. Once this is shown it is easy to see we may reduce to the case $F = \mathbb{Q}^\chi$ by setting $K = F$ and $E = \mathbb{Q}^\chi$. We begin by showing the following elementary result.

Lemma 5.5. *Let K/E be a Galois extension of number fields with $[K : E] = n$ and $\gcd(n, h_E) = 1$. Then the natural map $C_E \to C_K$ is an injection.*

Proof. The natural map $C_E \to C_K$ arises from the map $I_E \to I_K$ given by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ where I_E denotes the fractional ideals of $\mathcal{O}_E$ and similarly for I_K. Let $\mathfrak{a} \in I_E$ be such that $\mathfrak{a}$ becomes principal in I_K, i.e., there exists an $\alpha \in K$ so that $\mathfrak{a}\mathcal{O}_K = (\alpha)$. Recall that if we map $\mathfrak{a}$ into I_K and then back to I_E via the norm map we obtain $\mathrm{Nm}(\mathfrak{a}\mathcal{O}_K) = \mathfrak{a}^{[K:E]}$. We also have that since $\mathfrak{a}\mathcal{O}_K$ is principal, $\mathrm{Nm}(\mathfrak{a}\mathcal{O}_K) = (\mathrm{Nm}(\alpha))$. Thus, we see that $\mathfrak{a}^{[K:E]} = (\mathrm{Nm}(\alpha))$, i.e., $\mathfrak{a}^{[K:E]}$ is 0 in the class group of E. Thus, we must have that the order of $\mathfrak{a}$ divides $[K : E]$ as well as h_E. However, these were assumed to be relatively prime so it must be that the order of $\mathfrak{a}$ is 1 and so the map is injective. □

Using this lemma we see that A_E^χ injects into A_K^χ. The fact that χ factors through $\mathrm{Gal}(E/\mathbb{Q})$ means that χ is trivial on $\mathrm{Gal}(K/E)$. In particular, using the definition of A_K^χ applied to the $\sigma \in \mathrm{Gal}(K/E)$ we see that $\mathrm{Gal}(K/E)$ leaves the ideals in A_K^χ fixed. In particular, for any prime ideal $\mathfrak{p}$ in A_K^χ, we have that $\sigma\mathfrak{p} = \mathfrak{p}$ fpr every $\sigma \in \mathrm{Gal}(K/E)$. However, we know that $\mathrm{Gal}(K/E)$ permutes the primes $\mathfrak{p}$ lying over $\wp$ in E. Thus, there is only one prime over $\wp$ for each prime ideal $\wp \in A_E^\chi$. This shows that the above map is also a surjection and hence an isomorphism as claimed.

Let L_n, L, X_n, and X be defined as in the previous section. In particular, our goal is to determine the p-adic valuation of $|X_0^\chi|$. By our choice of χ we have that $X_0^\chi = (X/TX)^\chi = X^\chi/TX^\chi$. Recall that X^χ is a finitely generated torsion Λ_χ-module. Set ϖ to be a uniformizer of $\mathcal{O}_\chi$. Recall that we have

$$X^\chi \sim \left(\bigoplus_i \Lambda_\chi/\varpi^{\mu_{\chi,i}} \right) \oplus \left(\bigoplus_j \Lambda_\chi/(f_{\chi,j}(T)^{m_j}) \right)$$

where we set $\mu_\chi = \sum \mu_{\chi,i}$ and the $f_{\chi,j}$ are all irreducible distinguished polynomials. In fact, since we are assuming χ is an odd character we have that the above pseudo-isomorphism is actually an injection with finite cokernel C. For a proof of this, see ([Wash], Proposition 13.28). Thus we have

$$\begin{tikzcd}
0 \arrow[r] & X^\chi \arrow[r] \arrow[d, "T^{(1)}"] & (\bigoplus_i \Lambda_\chi/\varpi^{\mu_{\chi,i}}) \oplus \left(\bigoplus_j \Lambda_\chi/(f_{\chi,j}(T)^{m_j})\right) \arrow[r] \arrow[d, "T^{(2)}"] & C \arrow[r] \arrow[d, "T^{(3)}"] & 0 \\
0 \arrow[r] & X^\chi \arrow[r] & (\bigoplus_i \Lambda_\chi/\varpi^{\mu_{\chi,i}}) \oplus \left(\bigoplus_j \Lambda_\chi/(f_{\chi,j}(T)^{m_j})\right) \arrow[r] & C \arrow[r] & 0
\end{tikzcd}$$

where $T^{(i)}$ is just multiplication by T.

Lemma 5.6. *The kernel of the map $T^{(2)}$ is 0.*

Proof. Suppose $\ker T^{(2)} \neq 0$. Then we must have $T \mid \prod_j f_{\chi,j}(T)^{m_j}$. The main conjecture then implies that $T \mid G_{\chi^{-1}\omega}((1+p)(1+T)^{-1} - 1)$, i.e., we have

$$\begin{aligned} 0 &= G_{\chi^{-1}\omega}((1+p) - 1) \\ &= \mathcal{L}_p(0, \chi^{-1}\omega) \\ &= (1 - \chi^{-1}(p))L(0, \chi^{-1}) \end{aligned}$$

where we have used that $\chi \neq \omega$ to conclude that $H_{\chi^{-1}\omega} = 1$. However, we know that $\chi(p) \neq 1$ by assumption and $L(0, \chi^{-1}) \neq 0$ since χ is odd. Thus the kernel must be 0. □

We can now apply the Snake lemma as well as the fact that $\ker T^{(2)} = 0$ to conclude we have an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \ker T^{(3)} \arrow[r] & \operatorname{coker} T^{(1)} \arrow[r] & \operatorname{coker} T^{(2)} \arrow[r] & \operatorname{coker} T^{(3)} \arrow[r] & 0.
\end{tikzcd}$$

We also have the exact sequence

$$\begin{tikzcd}
0 \arrow[r] & C[T] \arrow[r] & C \arrow[r, "\cdot T"] & C \arrow[r] & C/TC \arrow[r] & 0
\end{tikzcd}$$

where $C[T] = \{c \in C : Tc = 0\}$. We now use the fact that given an exact sequence of finite groups

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & D \arrow[r] & 0 \end{tikzcd}$$

we have that $|A| \cdot |B| \cdot |C|^{-1} \cdot |D|^{-1} = 1$ to conclude that $|C[T]| = |C/TC|$. Now, observing that $C[T] = \ker T^{(3)}$ and $C/TC = \operatorname{coker} T^{(3)}$ we obtain that $|\operatorname{coker} T^{(1)}| = |\operatorname{coker} T^{(2)}|$. Thus, we have the following string of equalities.

$$\begin{aligned}
|A_F^\chi| &= |X_0^\chi| \\
&= |X^\chi/TX^\chi| \\
&= |\operatorname{coker} T^{(1)}| \\
&= |\operatorname{coker} T^{(2)}| \\
&= |\bigoplus_i \Lambda_\chi/(\varpi^{\mu_{\chi,i}}, T)| \cdot |\bigoplus_j \Lambda_\chi/(f_{\chi,j}(T)^{m_j}, T)| \\
(1) \qquad &= |\Lambda_\chi/(f_\chi(T), T)| \\
&= |\mathcal{O}_\chi/f(0)| \\
(2) \qquad &= |\mathcal{O}_\chi/G_{\chi^{-1}\omega}(p)| \\
&= |\mathcal{O}_\chi/\mathcal{L}_p(0, \chi^{-1}\omega)|
\end{aligned}$$

where we used in equation (1) that $\mu_\chi = 0$ by the main conjecture since this is an abelian field and we used the main conjecture in equation (2) as well. In particular, we have that

$$|\mathcal{O}_\chi/\mathcal{L}_p(0, \chi^{-1}\omega)| = |\mathcal{O}_\chi/(L(0, \chi^{-1})(1 - \chi^{-1}(p)))|.$$

Thus,

$$v_p(A_F^\chi) = v_p(|\mathcal{O}_\chi/(L(0, \chi^{-1})(1 - \chi^{-1}(p)))|) = g \cdot v_p(L(0, \chi^{-1}))$$

as claimed.

5.3 Classical Modular Forms

In this section we give a very brief overview of the theory of classical modular forms. It is assumed the reader is familiar with the theory and we include this section to set notation mainly. Those wishing to read a more complete account of the theory are encouraged to consult any of the following: [DS], [Kob], [Milne3], or [Miyake]. For a more advanced overview that contains references to proofs one should consult [DI].

We denote the complex upper half plane by $\mathfrak{h}$. The group $\mathrm{GL}_2^+(\mathbb{R})$ acts on $\mathfrak{h}$ via linear fractional transformations, i.e., for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$ and $z \in \mathfrak{h}$ we have $gz = \frac{az+b}{cz+d}$. The two subgroups of $\mathrm{SL}_2(\mathbb{Z})$ that we will be interested in are

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 (\operatorname{mod} N) \right\}.$$

Define $j(g,z) = cz + d$.

Exercise 5.7. *For $g_1, g_2 \in \mathrm{GL}_2^+(\mathbb{Z})$ and $z \in \mathfrak{h}$, show*

$$j(g_1 g_2, z) = j(g_1, g_2 z) j(g_2, z).$$

For f a complex valued function on $\mathfrak{h}$ and $k \geq 0$ an integer we write

$$(f|_k g)(z) = (\det g)^{k/2} j(g,z)^{-k} f(gz).$$

A *modular form of weight k and level N* on $\Gamma_1(N)$ is a holomorphic function $f : \mathfrak{h} \to \mathbb{C}$ so that $f|_k g = f$ for every $g \in \Gamma_1(N)$ and f is holomorphic at the cusps, i.e., f is holomorphic at the points in $\mathbb{P}^1(\mathbb{Q})$. We write $M_k(\Gamma_1(N))$ to denote the complex vector space of modular forms of weight k on $\Gamma_1(N)$. Observe that if $f \in M_k(\Gamma_1(N))$, then f is periodic of period 1 and so has a Fourier expansion. We write this expansion as

$$f(z) = \sum_{n=0}^{\infty} a_f(n) q^n$$

where $q = e^{2\pi i z}$. For a ring $\mathcal{O}$, we write $M_k(\Gamma_1(N), \mathcal{O})$ to indicate the space of modular forms that have Fourier coefficients lying in $\mathcal{O}$.

Observe that $\Gamma_1(N) \subset \Gamma_0(N)$ and is a normal subgroup. In fact, one has $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ via the map $\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \mapsto d$. We have an action of $\Gamma_0(N)$ on $M_k(\Gamma_1(N))$ via $f \mapsto f|_k g$ for $g \in \Gamma_0(N)$. This gives an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $M_k(\Gamma_1(N))$ and so we can decompose this space with respect to the characters of $(\mathbb{Z}/N\mathbb{Z})^\times$. Write

$$M_k(N,\chi) = \{ f \in M_k(\Gamma_1(N)) : f|_k g = \chi(d) f \ \ \forall g \in \Gamma_0(N) \}.$$

Then we have

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi} M_k(N,\chi).$$

The space $M_k(N,\chi)$ is referred to as the *space of modular forms of weight k, level N and character χ.*

A modular form f is called a *cusp form* if it vanishes at all the cusps. We write $S_k(\Gamma_1(N))$ for the subspace of $M_k(\Gamma_1(N))$ of cusp forms. Note that for a cusp form f, the Fourier coeffience $a_f(0) = 0$. Similarly we can define $S_k(N,\chi)$ and have a decomposition

$$S_k(\Gamma_1(N)) = \bigoplus_{\chi} S_k(N,\chi).$$

Hecke operators are linear operators that act on each space of modular forms so far defined. We omit their precise definition and content ourselves with listing relevant properties. The reader who has never encountered Hecke operators is urged to read the brief account given in [Kob] as a quick introduction. For each $n \in \mathbb{N}$ there is an associated Hecke operator T_n. For $\gcd(n, N) = 1$ there is also an operator $\langle n \rangle$. Note the following facts:
(1) Hecke operators commute.
(2) For $\gcd(n, m) = 1$, $T_{nm} = T_n T_m$.
(3) Let ℓ be a prime. Then

$$T_{\ell^r} = \begin{cases} (T_\ell)^r & \ell \mid N \\ T_\ell T_{\ell^{r-1}} - \ell \langle \ell \rangle T_{\ell^{r-2}} & \ell \nmid N. \end{cases}$$

(4) Let $f \in M_k(N, \chi)$. The action of T_ℓ on f is given by

$$T_\ell f = \begin{cases} \sum_{n=0}^{\infty} a_f(\ell n) q^n & \ell \mid N \\ \sum_{n=0}^{\infty} a_f(\ell n) q^n + \chi(\ell) \ell^{k-1} \sum_{n=0}^{\infty} a_f(n) q^{n\ell} & \ell \nmid N. \end{cases}$$

Let $\mathbb{T}(k, N) \subseteq \mathrm{End}_{\mathbb{C}}(M_k(\Gamma_1(N))$ denote the $\mathbb{Z}$-subalgebra generated by the T_n's, or equivalently by the T_ℓ's and $\langle \ell \rangle$'s. We will drop the k and N when they are clear from the context. Given an integer M, we write $\mathbb{T}^{(M)}$ to denote the subalgebra generated by the T_n's with $\gcd(n, M) = 1$. There is a perfect pairing

$$S_k(\Gamma_1(N)) \times \mathbb{T} \to \mathbb{C}$$

given by $(f, t) \mapsto a_{tf}(1)$. In particular, we can use this perfect pairing and the fact that $S_k(\Gamma_1(N), \mathcal{O})$ is a $\mathbb{T}_{\mathcal{O}} := \mathbb{T} \otimes \mathcal{O}$-module to conclude that we have $S_k(\Gamma_1(N), \mathcal{O}) \cong \mathrm{Hom}_{\mathcal{O}}(\mathbb{T}, \mathcal{O})$.

Let $f \in S_k(\Gamma_1(N))$ and $g \in M_k(\Gamma_1(M))$. There is an inner product known as the Petersson product given by

$$\langle f, g \rangle_N = \mathrm{vol}(\Gamma_1(N) \backslash \mathfrak{h})^{-1} \int_{\Gamma_1(N) \backslash \mathfrak{h}} f(z) \overline{g(z)} y^k \frac{dx dy}{y^2}$$

where $z = x + iy$. This integral always converges. The Petersson product is a perfect pairing on $S_k(\Gamma_1(N)) \times S_k(\Gamma_1(N))$. The orthogonal complement of $S_k(\Gamma_1(N))$ in $M_k(\Gamma_1(N))$ is the space of Eisenstein series denoted by $E_k(\Gamma_1(N))$.

The Petersson product is Hecke equivariant, i.e., for $\ell \nmid N$ we have $\langle T_\ell f, g \rangle_N = \langle f, \langle \ell \rangle T_\ell g \rangle_N$. Note that for $f \in S_k(N, \chi)$ one has $\langle \ell \rangle f = \chi(\ell) f$. One can use these results to conclude that $\mathbb{T}^{(N)}$ can be simultaneously diagonalized on $S_k(N, \chi)$, i.e., $S_k(N, \chi)$ has a basis of simultaneous eigenforms for $\mathbb{T}^{(N)}$. Thus we can write $S_k(N, \chi) = \bigoplus V_i$ where each V_i is an eigenspace for the action of $\mathbb{T}^{(N)}$. For each V_i there exists a unique $M \mid N$ and a unique $f \in S_k(M, \chi)$ so that $f \in V_i$ and satisfies the following properties:
(1) $a_f(1) = 1$
(2) f is a simultaneous eigenform for all T_ℓ and $\langle \ell \rangle$ (including $\ell \mid M$)
(3) The set $\left\{ f(ez) : e \mid \frac{N}{M} \right\}$ forms a basis of V_i. (Note: If $M = N$ then V_i is 1-dimensional. Also observe that if $\ell \mid N$ but $\ell \nmid M$ then T_ℓ is not the same

on $S_k(N,\chi)$ as on $S_k(M,\chi)$. So while f is an eigenform for $\mathbb{T}_k(M)$ it is not necessarily an eigenform for $\mathbb{T}_k(N)$.)
(4) $T_\ell f = a_f(\ell)f$.
The forms f where V_i is 1-dimensional are referred to as *newforms*. They are "new" in the sense that they do not come from a form on a space of lower level. The following fact will also be useful. Let $f_1, \dots, f_r$ be a basis of newforms for $S_k^{\text{new}}(\Gamma_1(N))$ and suppose each of these newforms has coefficients in some number field L. The action of $\mathbb{T}(k,N)$ on the space of newforms gives the following isomorphism

$$\mathbb{T} \otimes L \cong \prod_{i=1}^{r} L.$$

Let $f \in M_k(\Gamma_1(N))$. Associated to f is a complex analytic function $L(s,f)$ defined by

$$L(s,f) = \sum_{n=1}^{\infty} a_f(n) n^{-s},$$

which converges in some right half plane. This L-function has analytic continuation to $\mathbb{C}$ if $f \in S_k(\Gamma_1(N))$ and meromorphic continuation to $\mathbb{C}$ with the only possible poles at $s = 0, k$ in general. There is also a functional equation, but we will not make use of it so omit it. Suppose now that f is an eigenform for $\mathbb{T}$. In this case $L(s,f)$ has an Euler product given by

$$L(s,f) = \prod_{\ell \nmid N} (1 - a_f(\ell)\ell^{-s} + \chi(\ell)\ell^{k-1-2s})^{-1} \prod_{\ell \mid N} (1 - a_f(\ell)\ell^{-s})^{-1}.$$

We will also require the following information about Eisenstein series. Recall the space $E_k(\Gamma_1(N))$ is the orthogonal complement to the space of cusp forms in $M_k(\Gamma_1(N))$. Let χ_1 and χ_2 be Dirichlet characters of conductor M_1 and M_2 respectively. We assume that either both characters are primitive or if $k = 2$ and χ_1 and χ_2 are both trivial then $M_1 = 1$ and M_2 is prime. Define terms $a(n)$ by

$$\sum_{n=1}^{\infty} a(n) n^{-s} = L(s,\chi_1) L(s-k+1,\chi_2),$$

i.e.,

$$a(n) = \sum_{0<d \mid n} \chi_1(n/d)\chi_2(d) d^{k-1} \qquad (n \geq 1).$$

Note this gives $a(\ell) = \chi_1(\ell) + \chi_2(\ell)\ell^{k-1}$ for primes ℓ. Define $a(0)$ by

$$a(0) = \begin{cases} -\frac{1}{24}(1-M_2) & \text{if } k=2 \text{ and } \chi_1 = 1 = \chi_2 \\ 0 & \text{if } k \neq 1 \text{ and } \chi_1 \neq 1 \\ 0 & \chi_1 \neq 1 \neq \chi_2 \\ \frac{L(1-k,\chi_1\chi_2)}{2} & \text{otherwise.} \end{cases}$$

Then there exists a modular form

$$E^{(k)}_{\chi_1,\chi_2}(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(M_1M_2, \chi_1\chi_2).$$

In fact, this modular form is a normalized eigenform for $\mathbb{T}^{(M_1M_2)}$. Moreover,

$$E_k(N,\chi) = \left\langle E^{(k)}_{\chi_1,\chi_2}(ez) : e \mid \frac{N}{M_1M_2},\ \chi = \chi_1\chi_2 \right\rangle.$$

Exercise 5.8. *(For the representation theory people.) Reconcile the above statements about Eisenstein series with what you know from representation theory.*

Let $f \in S_k(N,\chi)$ be a normalized eigenform for $\mathbb{T}$, i.e., $a_f(1) = 1$ and $T_n f = a_f(n)f$ for all n. We shall make use of the fact that there exists a number field K_f such that $a_f(n) \in K_f$ for all n. In fact, one can show that $a_f(n) \in \mathcal{O}_f := \mathcal{O}_{K_f}$ for all n. Fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ for ℓ a prime. Let λ be a prime of $\mathcal{O}_f$ lying over ℓ and let $\mathcal{O}_{f,\lambda}$ denote the completion of $\mathcal{O}_f$ at λ. There exists a continuous representation

$$\rho_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_{f,\lambda})$$

where $\mathrm{GL}_2(\mathcal{O}_{f,\lambda})$ gets the topology inherited from $\mathcal{O}_{f,\lambda}$ and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ gets the profinite topology. This map is a continuous homomorphism of topological groups such that
(1) $\rho_{f,\lambda}$ is unramified at all $p \nmid \ell N$ (action of inertia group at p is trivial)
(2) $\det \rho_{f,\lambda}(\mathrm{Frob}_p) = \chi(p)p^{k-1}$ for $p \nmid \ell N$
(3) $\mathrm{trace}(\rho_{f,\lambda}(\mathrm{Frob}_p)) = a_f(p)$ for $p \nmid \ell N$
(4) $\rho_{f,\lambda}$ is irreducible.
There are also Galois representations attached to Eisenstein series but these are no longer irreducible.

Let K be a finite extension of $\mathbb{Q}_\ell$ for some prime ℓ. Let $\mathcal{O}$ denote the ring of integers of K and set $k = \mathcal{O}/\varpi$ where ϖ is the maximal ideal of $\mathcal{O}$. We fix the appropriate embeddings: $K \hookrightarrow \overline{\mathbb{Q}}_\ell$, $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$, and $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. The Hecke algebras $\mathbb{T}_K$ and $\mathbb{T}_k$ are Artinian and so only have a finite number of prime ideals, all of which are maximal. The Hecke algebra $\mathbb{T}_\mathcal{O}$ is finitely generated and free as an $\mathcal{O}$-module. Thus, the maximal ideals are those lying over ϖ of $\mathcal{O}$ and the minimal primes are those lying over $(0) \subset \mathcal{O}$. This is a consequence of the going up and going down theorems, see ([Mats], Theorems 9.4, 9.5). Thus, the natural maps $\mathbb{T}_\mathcal{O} \hookrightarrow \mathbb{T}_\mathcal{O} \otimes_\mathcal{O} K \cong \mathbb{T}_K$ and $\mathbb{T}_\mathcal{O} \twoheadrightarrow \mathbb{T}_\mathcal{O} \otimes_\mathcal{O} k \cong \mathbb{T}_k$ give bijections

$$\{\text{maximal ideals of } \mathbb{T}_K\} \leftrightarrow \{\text{minimal primes of } \mathbb{T}_\mathcal{O}\}$$
$$\{\text{maximal ideals of } \mathbb{T}_k\} \leftrightarrow \{\text{maximal primes of } \mathbb{T}_\mathcal{O}\}.$$

Using the fact that $\mathcal{O}$ is complete we can apply ([Mats] Theorems 8.7, 8.15) to conclude that the natural map

$$\mathbb{T}_\mathcal{O} \to \prod_{\mathfrak{m}} \mathbb{T}_{\mathcal{O},\mathfrak{m}}$$

is an isomorphism where the product is over the finite set of maximal ideals of $\mathbb{T}_{\mathcal{O}}$. Each $\mathbb{T}_{\mathcal{O},\mathfrak{m}}$ is a complete local $\mathcal{O}$-algebra which is finitely generated and free as an $\mathcal{O}$-module. Moreover, each minimal prime $\mathfrak{p}$ of $\mathbb{T}_{\mathcal{O}}$ is contained in a unique $\mathfrak{m}$.

We now connect the ideals of the Hecke algebras back to what they tell us about eigenforms. Let $f \in S_k(N, \overline{K})$ be a normalized eigenform for $\mathbb{T}$. One has that the map $T_n \mapsto a_f(n)$ from $\mathbb{T} \to \overline{K}$ induces a K-algebra homomorphism $\mathbb{T}_K \to \overline{K}$. The image is the finite extension of K generated by the Fourier coefficients of f. The kernel of this map is a maximal ideal of $\mathbb{T}_K$ that depends only on the $\mathrm{Gal}(\overline{K}/K)$-conjugacy class of f. Thus, a $\mathrm{Gal}(\overline{K}/K)$ conjugacy class of normalized eigenforms gives rise to a maximal ideal of $\mathbb{T}_K$. The analogous statement for $\mathbb{T}_k$ holds as well. In fact, we have the following result.

Theorem 5.9. *The following diagram commutes with the vertical maps being bijective and the horizontal maps being surjective. Note the top horizontal map is nothing more then the Deligne-Serre lifting lemma ([DS], Lemma 6.11).*

$$\begin{tikzcd}
\left\{\begin{array}{c} \textit{normalized eigenforms in} \\ S_m(N,\overline{K}) \textit{ modulo} \\ \mathrm{Gal}(\overline{K}/K)\textit{-conjugacy} \end{array}\right\} \arrow[r] \arrow[d] & \left\{\begin{array}{c} \textit{normalized eigenforms in} \\ S_m(N,\overline{k}) \textit{ modulo} \\ \mathrm{Gal}(\overline{k}/k)\textit{-conjugacy} \end{array}\right\} \arrow[d] \\
\{\textit{maximal ideals of } \mathbb{T}_K\} \arrow[d, leftrightarrow] & \{\textit{maximal ideals of } \mathbb{T}_k\} \arrow[d, leftrightarrow] \\
\{\textit{minimal primes of } \mathbb{T}_{\mathcal{O}}\} \arrow[r, two heads] & \{\textit{maximal primes of } \mathbb{T}_{\mathcal{O}}\}
\end{tikzcd}$$

We will mainly be interested in "ordinary" modular forms. .

Definition 5.10. Let K_f be a number field containing all the Fourier coefficients of $f \in S_k(N, \chi)$ and $\mathcal{O}_f$ be the ring of integers of K_f. We say f is ordinary at p if $a_f(p) \in \mathcal{O}_{f,\wp}^{\times}$ for every prime $\wp | p$ in $\mathcal{O}_f$.

Exercise 5.11. *Prove that f being ordinary at p is equivalent to the statement that*

$$x^2 - a_f(p)x + \chi(p)p^{k-1}$$

has at least one root that is a unit modulo $\wp$ for each $\wp | p$ in $\mathcal{O}_f$.

An important feature of ordinary forms is the fact that given an eigenform $f \in S_k(N, \chi)$ that is ordinary at p one has that the Galois representation attached to f has the following nice form when restricted to the absolute decomposition group D_p of p:

$$\rho_f|_{D_p} \simeq \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

where χ_2 is unramified at p and satisfies

$$\chi_2(\mathrm{Frob}_p) = \left\{ \begin{array}{cc} \text{unit root of } x^2 - a_f(p)x + \chi(p)p^{k-1} & p \nmid N \\ a_f(p) & p|N. \end{array} \right.$$

Note here that the $\simeq$ means that $\rho_f|_{D_p}$ can be conjugated into this form.

We will also need Hida's ordinary projector e. To avoid confusion we adopt the convention that we will write U_p for T_p when we are thinking of T_p in $\mathbb{T}(k, N)$ with $p \mid N$. Let $\mathcal{O}$ be a finite extension of $\mathbb{Z}_p$ and K the field of fractions of $\mathcal{O}$. Set

$$e = \lim_{m\to\infty} U_p^{m!}.$$

This is well defined and acts on $M_k(\Gamma_0(Np^r), \mathcal{O})$ where $r \geq 1$ ([Hida1], page 236). In fact, e is an idempotent. Given an eigenform f, ef is nonzero if and only if f is ordinary at p.

Exercise 5.12. *Prove that ef is nonzero if and only if f is ordinary at p.*

Let f be an ordinary form of level N. If $p \nmid N$, we can still consider f as an element of $M_k(\Gamma_0(Np))$ and so have an action of e on f. One has then that ef is an eigenform of level Np if $p \nmid N$ and an eigenform of level N if $p|N$. The eigenform ef has the same eigenvalues as f away from p (Hecke operators T_n commute with U_p for $p \nmid n$) and has the unit root of $x^2 - a_f(p)x + \chi(p)p^{k-1}$ as its eigenvalue at p. The form ef is called the *p-stabilized newform* associated to f.

We write $M_k^0(\Gamma_0(N), K)$ for $eM_k(\Gamma_0(N), K)$ and likewise for S_k^0. It is convention to refer to $M_k^0(\Gamma_0(N), K)$ as the ordinary forms. However, one should be aware that this is an abuse of language as an ordinary form does not necessarily lie in here. What is true is that if f is an ordinary form, then ef is nonzero and in $M_k^0(\Gamma_0(N), K)$. So $M_k^0(\Gamma_0(N), K)$ consists of the p-stabilized newforms associated to the ordinary forms in $M_k(\Gamma_0(N), K)$.

We will need the following theorem when we study Λ-adic modular forms.

Theorem 5.13. *([Wiles1], page 539) For fixed N, $\dim_K M_k^{(0)}(\Gamma_0(Np), K)$ is bounded independent of k.*

Proof. We give here an outline of the proof of this theorem, leaving many of the details to the reader. The main idea is to make use of the Eichler-Shimura isomorphism:

$$M_k(\Gamma, \mathbb{C}) \oplus \overline{S_k(\Gamma, \mathbb{C})} \xrightarrow{\sim} \mathrm{H}^1(\Gamma, L_{k-2}(\mathbb{C}))$$

where we have group cohomology on the right with $L_{k-2}(\mathbb{C})$ denoting the symmetric polynomial algebra in two variables of degree $k-2$ over $\mathbb{C}$. The action of Γ on $L_{k-2}(\mathbb{C})$ is given by $\gamma \cdot P(x,y) = P((x,y)\gamma^{-1}\det\gamma)$. It is possible to define Hecke operators on the cohomology group corresponding to the Hecke operators on modular forms. The point here is that $M_k(\Gamma_0(Np), \mathbb{C}) \hookrightarrow \mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathbb{C}))$, so we can prove the theorem by bounding the dimension of $\mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathbb{C}))$. Observe that we can define e as above since we have the appropriate Hecke operator acting on the cohomology group. With $\mathcal{O}$ as above we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & L_{k-2}(\mathcal{O}) \arrow[r, "\cdot\varpi"] & L_{k-2}(\mathcal{O}) \arrow[r] & L_{k-2}(\mathbb{F}) \arrow[r] & 0 \end{tikzcd}$$

where $\mathbb{F} = \mathcal{O}/\varpi$. This gives an injection

$$e\mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathcal{O})) \otimes \mathbb{F} \hookrightarrow e\mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathbb{F}))$$

where we have used that tensoring with $\mathbb{F}$ kills off the kernel. Thus, we have

$$\begin{aligned}\dim_{\mathbb{C}}(e\mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathbb{C}))) &\leq \mathrm{rank}_{\mathcal{O}}(e\mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathcal{O}))) \\ &\leq \dim_{\mathbb{F}}(e\mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathbb{F}))).\end{aligned}$$

Thus, it remains to bound the dimension of $e\mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathbb{F}))$ independent of k. Define $j : L_{k-2}(\mathbb{F}) \to \mathbb{F}$ by

$$\sum_{m=0}^{k-2} A_m x^{k-2-m} y^m \mapsto A_0.$$

This is a map of $\Gamma_0(Np)$-modules that compatible with the action of $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. Thus we have a map

$$j_* : \mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathbb{F})) \to \mathrm{H}^1(\Gamma_0(Np), \mathbb{F})$$

that is U_p-equivariant. If we can show that j_* is injective on $e\mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathbb{F}))$ we will be done because everything will be bounded by the dimension of $\mathrm{H}^1(\Gamma_0(Np), \mathbb{F})$. To show j_* is injective one shows that one can define a map

$$I : \mathrm{H}^1(\Gamma_0(Np), \mathbb{F}) \to \mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathbb{F}))$$

so that $I \circ j_* = j_* \circ I = U_p$. This proves that j_* is injective on $e\mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathbb{F}))$ because U_p is invertible on $e\mathrm{H}^1(\Gamma_0(Np), L_{k-2}(\mathbb{F}))$. (Think U_p acts by a unit here since the eigenvalues are the unit roots!) The map I is defined as follows. Let $g = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. Observe that $gL_{k-2}(\mathbb{F}) \cong g\mathbb{F} \cong \mathbb{F}$ since g kills everything except the first coefficient. To ease notation set $\Gamma = \Gamma_0(Np)$. We have maps

$$\begin{tikzcd}
\mathrm{H}^1(\Gamma, \mathbb{F}) \arrow[r, "g_*"] & \mathrm{H}^1(\Gamma \cap g\Gamma g^{-1}, g\mathbb{F}) \arrow[r, "i_*"] & \mathrm{H}^1(\Gamma \cap g\Gamma g^{-1}, \mathbb{F}) \arrow[d, "j_*^{-1}"] \\
& & \mathrm{H}^1(\Gamma \cap g\Gamma g^{-1}, gL_{k-2}(\mathbb{F})) \arrow[d, "i_*"] \\
& & \mathrm{H}^1(\Gamma \cap g\Gamma g^{-1}, L_{k-2}(\mathbb{F})) \arrow[d, "\mathrm{cores}"] \\
& & \mathrm{H}^1(\Gamma, L_{k-2}(\mathbb{F})).
\end{tikzcd}$$

Define I to be the composition of these maps. It is then left to check I satisfies the properties claimed, which is left as a long tedious exercise. □

5.4 Converse to Herbrand's Theorem

In this section we will outline the Ribet's proof of the converse of Herbrand's theorem. We include this here as it provides a "classical outline" of Wiles' proof of the main conjecture. Understanding this proof will give one a good foundation to understand Wiles' proof which relies on the same method using Λ-adic modular forms instead of classical modular forms. Recall Theorem 3.44 which we state here in a more general form then that due to Ribet.

Theorem 5.14. *Let p be a fixed odd prime and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \overline{\mathbb{Q}}_p^\times$ an even primitive Dirichlet character of order prime to p. Set $\psi = \chi\omega$ and $F = \mathbb{Q}^\psi$. If $L(-1,\chi)$ is not a unit in $\overline{\mathbb{Q}}_p$, then $A_F^{\psi^{-1}} = A_F \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{F}_p(\psi^{-1}) \neq 0$ where $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ and we write $\mathbb{F}_p(\psi^{-1})$ to denote $\mathbb{F}_p$ with an action of Δ by ψ^{-1}.*

Remark 5.15. One can replace $\mathbb{Q}^\psi$ in the above theorem with any abelian extension of $\mathbb{Q}$ of order prime to p that contains $\mathbb{Q}^\psi$ and the result remains valid.

Exercise 5.16. *Show that Theorem 3.44 follows from this theorem.*

Our goal is to construct a nontrivial unramified extension of F on which Δ acts by ψ^{-1}. This is accomplished by constructing an appropriate Galois representation.

Consider the Eisenstein series $E_{1,\chi}^{(2)}(z)$. We will drop the superscript (2) as it will not change throughout the argument. Recall the constant term of $E_{1,\chi}(z)$ is given by $\frac{L(-1,\chi)}{2}$ and the ℓ^{th} Fourier coefficient is $c_E(\ell) = 1 + \chi(\ell)\ell$. Let $\mathcal{O}$ be the ring of integers of some finite extension of $\mathbb{Q}_p$ that contains all the values of χ and let ϖ be a uniformizer of $\mathcal{O}$. The first step in Ribet's argument is to produce an ordinary newform f so that the eigenvalues of f are congruent to those of $E_{1,\chi}(z)$ modulo a prime ϖ that divides $L(-1,\chi)$. Note that modulo ϖ the Eisenstein series is a semi-cusp form, i.e., it is a modular form with a constant term of 0 in the Fourier expansion about the cusp infinity. One can show that there is a modular form $g \in M_2(M,\chi)$ with constant term 1 for some M with $N \mid M$ by studying the geometry of the modular curve $X_1(p)$. In fact, one can choose M so that $\mathrm{ord}_p(M) \leq 1$ and if $\ell | M$ with $\ell \nmid Np$, then $\chi(\mathrm{Frob}_\ell) \not\equiv \ell^{-2}$ modulo any prime above p. One then sets $h(z) = E_{1,\chi}(z) - \frac{L(-1,\chi)}{2} g(z)$. The modular form h is congruent to $E_{1,\chi}$ modulo ϖ and is in fact a semi-cusp form. Note that h is not necessarily an eigenform, it is only an eigenform modulo ϖ. One then applies the Deligne-Serre lifting lemma to obtain a semi-cusp form f' that is an eigenform and congruent to $E_{1,\chi}$ modulo ϖ. A short argument then yields an ordinary newform f that is congruent to $E_{1,\chi}$ modulo ϖ.

Before we show how such a congruence can yield information about class groups, we rephrase this in terms of Hecke algebras as opposed to applying the Deligne-Serre lifting lemma itself. The reason for this is that a similar argument using Λ-adic forms will be used in the proof of the main conjecture. We look at the Hecke algebra $\mathbb{T}_{\mathcal{O}}^{(M)} := \mathbb{T}_{\mathcal{O}}^{(M)}(k, M)$. Assume that $L(-1,\chi) \notin \mathcal{O}^\times$. Recall that $h \equiv E_{1,\chi}(\operatorname{mod} \varpi)$, i.e., for any $t \in \mathbb{T}_{\mathcal{O}}^{(M)}$ if $tE_{1,\chi}(z) = c_E(t)E_{1,\chi}(z)$, then $th \equiv c_E(t)h(\operatorname{mod} \varpi)$. Note we remove the places dividing M to avoid any difficulty with the fact that $E_{1,\chi}$ is of level N. In fact, we could just remove the primes dividing $\frac{M}{N}$ and achieve the same effect, but removing the ones at M causes no difficulty. Define $\Phi : \mathbb{T}_{\mathcal{O}}^{(M)} \to \mathcal{O}/(L(-1,\chi))$ by $t \mapsto c_E(t)$. This is easily seen to be a homomorphism and $\Phi(T_\ell) = 1 + \chi(\ell)\ell$ for $\ell \nmid M$. Set $\mathfrak{m} = \Phi^{-1}(\varpi)$. We can extend this ideal to an ideal of $\mathbb{T}_{\mathcal{O}}$, call this extended ideal $\mathfrak{m}_{E_{1,\chi}}$. We know from Theorem 5.9 that there exists a minimal prime $\wp \subset \mathfrak{m}_{E_{1,\chi}}$. The minimal prime $\wp$ corresponds to a newform f of level M and character χ. To see f is congruent to $E_{1,\chi}$ away from M, observe that one can define a maximal ideal $\mathfrak{m}_f$ by defining a map $\pi_f : \mathbb{T}_{\mathcal{O}} \to \mathcal{O}$ by $t \mapsto a_f(n)$. The minimal prime $\wp \subset \mathfrak{m}_f$ as well, and so $\mathfrak{m}_{E_{1,\chi}} = \mathfrak{m}_f$.

Exercise 5.17. *Let f and g be eigenforms. Show that $f \equiv g(\operatorname{mod} \varpi)$ if and only if $\mathfrak{m}_f = \mathfrak{m}_g$.*

Note in this case it is easy to see f is ordinary at p as $\Phi(T_p) = 1$, so in particuar $\varpi \nmid a_f(p)$. The kernel of Φ contains $I = \langle T_\ell - 1 - \chi(\ell)\ell \rangle$. This ideal is referred to as the *Eisenstein ideal* ([Mazur]). It is a maximal ideal and thus we have the following isomorphism:

$$\mathbb{T}_{\mathcal{O}}^{(M)}/I \xrightarrow{\sim} \mathcal{O}/(L(-1,\chi)).$$

Even though our congruence is only at the places away from M, we can use the Chebotarev density theorem to obtain the isomorphism of Galois representations we are interested in so this poses no difficulties.

The reason one cares about such a congruence in terms of gaining information about class groups is because of what it tells in terms of Galois representations. We continue with the same set-up as above. Let $K := \mathbb{Q}_p(\{a_f(n)\})$, i.e., the finite extension of $\mathbb{Q}_p$ generated by the Fourier coefficients of f. Let $\mathcal{O}$ be the ring of integers of K. Let $\overline{\rho}_f : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\mathbb{F})$ be the residual representation obtained upon composing ρ_f with the natural map $\mathcal{O} \twoheadrightarrow \mathbb{F} = \mathcal{O}/\varpi$. Observe that the congruence to $E_{1,\chi}(z)$ modulo ϖ gives $\operatorname{trace}(\overline{\rho}_f(\operatorname{Frob}_\ell)) = \overline{a_f(\ell)} \equiv 1 + \chi(\ell)\ell(\operatorname{mod} \varpi)$ for $\ell \nmid M$. Thus, combining the Chebotarev density theorem and Brauer-Nesbitt theorem we obtain that semi-simplification of $\overline{\rho}_f$ is given by $\overline{\rho}_f^{\mathrm{ss}} = 1 \oplus \psi$ where $\psi = \chi\omega$. Thus, there exists $M \in \operatorname{GL}_2(\mathbb{F})$ so that $M\overline{\rho}_f M^{-1}$ is one of the following matrices: $\begin{pmatrix} 1 & * \\ 0 & \psi \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & \psi \end{pmatrix}$, or $\begin{pmatrix} 1 & 0 \\ * & \psi \end{pmatrix}$. Note we are assuming that the forms that have a "$*$" are nonsplit, i.e., they cannot be diagonalized. Note that since $p \mid \operatorname{cond}(\psi)$, we have that $\psi|_{I_p} \neq 1$. Pick $\sigma \in I_p$ so that $\psi(\sigma) \neq 1$. This shows that the eigenvalues of $\overline{\rho}_f(\sigma)$ are distinct in $\mathbb{F}$ and so the matrix can be diagonalized. In particular, the eigenvalues are roots of the characteristic polynomial and so exist in $\mathcal{O}$ by Hensel's lemma. Thus, $\rho_f(\sigma)$ can be diagonalized, say $\rho_f(\sigma) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ with $\alpha \neq \beta$. Using this fact one has that

$$A\overline{\rho}_f(\sigma)A^{-1} = \begin{pmatrix} \overline{\alpha} & 0 \\ 0 & \overline{\beta} \end{pmatrix}.$$

This equation implies that A must be a diagonal matrix, which in turn implies that $\overline{\rho}_f$ itself must be of the form $\begin{pmatrix} 1 & * \\ 0 & \psi \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & \psi \end{pmatrix}$, or $\begin{pmatrix} 1 & 0 \\ * & \psi \end{pmatrix}$.

Suppose that $\overline{\rho}_f$ is of the form $\begin{pmatrix} 1 & 0 \\ 0 & \psi \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ * & \psi \end{pmatrix}$. This implies we have $\rho_f(g) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$ with $b(g) \in \varpi\mathcal{O}$ for all $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The Galois representation ρ_f is irreducible, so there exists $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ so that $b(g) \neq 0$. Let n be the minimum of $\mathrm{ord}_\varpi(b(g))$ over $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Necessarily we have $n > 0$ and finite. Conjugate ρ_f by $\begin{pmatrix} 1 & 0 \\ 0 & \varpi^n \end{pmatrix}$. Call this new representation ρ_f as well. This still has entries in $\mathcal{O}$ and now $\overline{\rho}_f = \begin{pmatrix} 1 & * \\ 0 & \psi \end{pmatrix}$ with $*$ possibly 0. However, one can show this is non-split since $\overline{\rho}_f(\sigma) = \begin{pmatrix} \overline{\alpha} & 0 \\ 0 & \overline{\beta} \end{pmatrix}$ with $\overline{\alpha} \neq \overline{\beta}$. Thus, we can always choose $\overline{\rho}_f$ to be non-split of the form $\begin{pmatrix} 1 & * \\ 0 & \psi \end{pmatrix}$.

Exercise 5.18. *Prove that if there exist σ so that $\overline{\rho}_f(\sigma) = \begin{pmatrix} \overline{\alpha} & 0 \\ 0 & \overline{\beta} \end{pmatrix}$ with $\overline{\alpha} \neq \overline{\beta}$, then $\overline{\rho}_f$ is necessarily non-split.*

The Galois representation that will produce our extension is $\overline{\rho}_f|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. However, we still need to prove that this Galois representation is unramified everywhere and then show how it produces the appropriate extension. The only possibility for ramification for ρ_f is at primes $\ell | Mp$. We begin by looking at $\ell = p$. Recall that since f is ordinary at p one has that the Galois representation attached to f has the following nice form when restricted to the absolute decomposition group D_p of p:

$$\rho_f|_{D_p} \simeq \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

where χ_2 is unramified at p and satisfies

$$\chi_2(\mathrm{Frob}_p) = \begin{cases} \text{unit root of } x^2 - a_f(p)x + \chi(p)p^{k-1} & p \nmid N \\ a_f(p) & p | N. \end{cases}$$

We claim that we have

$$\rho_f|_{D_p} \subseteq \left\{ \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \right\}.$$

We use the $\sigma \in I_p \subset D_p$ as above so that $\rho_f(\sigma) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ with $\alpha \neq \beta$. The fact that f is ordinary at p implies there is a matrix A so that

$$A\rho_f(\tau)A^{-1} = \begin{pmatrix} \chi_1(\tau) & *(\tau) \\ 0 & \chi_2(\tau) \end{pmatrix}$$

for every $\tau \in D_p$ and

$$A\rho_f(\sigma)A^{-1} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}.$$

From these two equations it is a short calculation to see the claim is true. We now combine this fact with the fact that $\overline{\rho}_f$ is of the form $\begin{pmatrix} 1 & * \\ 0 & \psi \end{pmatrix}$ to conclude that

$$\overline{\rho}_f|_{D_p} = \begin{pmatrix} 1 & 0 \\ 0 & \psi \end{pmatrix}.$$

Thus, $\overline{\rho}_f|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}$ is trivial when restricted to D_p since ψ is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$. Since $I_p \subseteq D_p$, we see $\overline{\rho}_f|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}$ is unramified at p.

Let ℓ be a prime. Recall that we have a factorization of the inertia group I_ℓ into tame and wild parts:

$$\begin{tikzcd} 0 \arrow[r] & I_\ell^{\mathrm{wild}} \arrow[r] & I_\ell \arrow[r] & I_\ell^{\mathrm{tame}} \arrow[r] & 0. \end{tikzcd}$$

The wild part, I_ℓ^{wild}, is the maximal pro-ℓ subgroup of I_ℓ. In other words, elements in I_ℓ^{wild} have orders that are powers of ℓ and elements in I_ℓ^{tame} have orders that are prime to ℓ.

We also have the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & I_\ell \arrow[r] & D_\ell \arrow[r] & \hat{\mathbb{Z}} \arrow[r] & 0. \end{tikzcd}$$

Let $\sigma_\ell \in D_\ell$ be any lift of $\mathrm{Frob}_\ell \in \hat{\mathbb{Z}}$, i.e., $\sigma_\ell \cdot x = \sigma_\ell x \sigma_\ell^{-1} = x^\ell$ for any $x \in I_\ell$. Let $\beta_\ell = \psi(\sigma_\ell)$ so that $\overline{\rho}_f(\sigma_\ell) = \begin{pmatrix} 1 & * \\ 0 & \beta_\ell \end{pmatrix}$.

Let ℓ be a prime so that $\ell | M$ but $\ell \nmid N$. This gives $\psi(I_\ell) = 1$ and so $\overline{\rho}_f|_{I_\ell} \subseteq \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$. Suppose there exists $x \in I_\ell$ so that $\overline{\rho}_f(x) \neq 1$, i.e., there exists $b \neq 0$ so that $\overline{\rho}_f(x) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. We have

$$\begin{aligned} \begin{pmatrix} 1 & \beta_\ell^{-1} b \\ 0 & 1 \end{pmatrix} &= \overline{\rho}_f(\sigma_\ell)\overline{\rho}_f(x)\overline{\rho}_f(\sigma_\ell)^{-1} \\ &= \overline{\rho}_f(x^\ell) \\ &= \begin{pmatrix} 1 & \ell b \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Thus, we have that $\beta_\ell^{-1} = \ell$. If we look at $\psi(\mathrm{Frob}_\ell)$ in $\mathbb{F}$ we obtain that $\chi(\mathrm{Frob}_\ell) = \ell^{-2}$. However, our choice of M was such that this could not happen. Thus, it must be that $\overline{\rho}_f$ is trivial on I_ℓ and so we are unramified here.

Let ℓ be a prime so that $\ell || N$. Using the fact that ω is unramified away from p we see that the order of $\psi(I_\ell)$ is prime to ℓ. Thus, $\overline{\rho}_f(x)$ has order prime to ℓ for every $x \in I_\ell$. This shows that $\overline{\rho}_f|_{I_\ell}$ factors through I_ℓ^{tame}, i.e., $\overline{\rho}_f(I_\ell) = \overline{\rho}_f(I_\ell^{\text{tame}})$. However, we know that I_ℓ^{tame} is abelian, so we must have that $\overline{\rho}_f(I_\ell)$ is abelian as well. Since $\ell|N$, we have $\psi|_{I_\ell} \neq 1$ and so $\overline{\rho}_f|_{I_\ell}$ is diagonalizable. Thus, $\overline{\rho}_f|_{I_\ell} \simeq \begin{pmatrix} 1 & 0 \\ 0 & \psi \end{pmatrix}$. Since we are interested in $\overline{\rho}_f|_{\text{Gal}(\overline{\mathbb{Q}}/F)}$, we see that this is trivial on I_ℓ since ψ is trivial on $\text{Gal}(\overline{\mathbb{Q}}/F)$. Thus, $\overline{\rho}_f|_{\text{Gal}(\overline{\mathbb{Q}}/F)}$ is unramified at primes $\ell||N$.

Exercise 5.19. *1. If $\ell|N$, show that $\psi|_{I_\ell} \neq 1$.*
2. Show if $\psi|_{I_\ell} \neq 1$ and $\overline{\rho}_f(I_\ell)$ is abelian, then $\overline{\rho}_f|_{I_\ell}$ is diagonalizable. (Hint: Let $\sigma \in I_\ell$ such that $\psi(\sigma) \neq 1$. For any $\tau \in I_\ell$, write $*(\tau)$ in terms of $\psi(\tau)$ and some constant depending upon σ.)

Finally, let ℓ be a prime so that $\ell^2|N$. In this case we see that $\psi(I_\ell^{\text{wild}}) \neq 1$. Thus, $\overline{\rho}_f(I_\ell^{\text{wild}}) \subseteq \left\{ \begin{pmatrix} 1 & *_1 \\ 0 & *_2 \end{pmatrix} \right\}$ and is an ℓ-group. We claim that it is a cyclic group as well. To see this, observe that we have a homomorphism from $\overline{\rho}_f(I_\ell^{\text{wild}})$ to $\mathbb{F}^\times$ given by mapping to $*_2$. The kernel of this homomorphism is $\left\{ \begin{pmatrix} 1 & *_1 \\ 0 & 1 \end{pmatrix} \right\}$, which can easily be realized as a subgroup of $\mathbb{F}$. However, the kernel is then a subgroup of a group of an ℓ-group and a group with p-power order, thus it must be trivial. So we see $\overline{\rho}_f(I_\ell^{\text{wild}})$ injects into $\mathbb{F}^\times$ and hence is cyclic. Arguing as above we see that $\overline{\rho}_f|_{I_\ell^{\text{wild}}}$ is diagonalizable and nontrivial. Recalling that I_ℓ^{wild} is a normal subgroup of I_ℓ, we see that $\overline{\rho}_f(I_\ell^{\text{wild}})$ is stable under conjugation by $\overline{\rho}_f(I_\ell)$. This in turn implies that $\overline{\rho}_f|_{I_\ell}$ is diagonalizable. Thus, as above we obtain that $\overline{\rho}_f|_{\text{Gal}(\overline{\mathbb{Q}}/F)}$ is unramified at such an ℓ.

We have shown that $\overline{\rho}_f|_{\text{Gal}(\overline{\mathbb{Q}}/F)}$ is unramified at all primes. Recall that we showed that $\overline{\rho}_f$ is non-split, i.e., there is a $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ so that $*(\sigma) \neq 0$. However, $*$ not being zero is an open condition so there is an open subgroup of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on which $*$ does not vanish. In particular, since $\text{Gal}(F/\mathbb{Q})$ is a finite group and all open subgroups are infinite, we get that $\overline{\rho}_f|_{\text{Gal}(\overline{\mathbb{Q}}/F)}$ is non-split as well. Define a map $h : \text{Gal}(\overline{\mathbb{Q}}/F) \to \mathbb{F}$ by $h(\sigma) = *(\sigma)$ where $*$ is given by $\overline{\rho}_f|_{\text{Gal}(\overline{\mathbb{Q}}/F)} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. The map h is clearly a nontrivial homomorphism. Let $\mathbb{Q}^h$ be the splitting field of h and set $H = \text{Gal}(\mathbb{Q}^h/F)$. Then $h : H \to \mathbb{F}$ is an injective homomorphism. This shows that H is an abelian p-group as it is a subgroup of $\mathbb{F}$. The fact that $h(I_\ell) = 0$ for any prime ℓ ($\overline{\rho}_f|_{\text{Gal}(\overline{\mathbb{Q}}/F)}$ is unramified everywhere) implies that $I_\ell(\mathbb{Q}^h/F) = 0$ for every ℓ since h is injective. Thus, we have that $\mathbb{Q}^h$ is a nontrivial unramified abelian p-extension of F so sits inside A_F. This shows that the p-part of the class group of F is nontrivial. Observe that for $\delta \in \Delta$ and $x \in H$ one has

$$\overline{\rho}_f(\delta)\overline{\rho}_f(x)\overline{\rho}_f(\delta)^{-1} = \begin{pmatrix} 1 & \psi^{-1}(\delta)h(x) \\ 0 & 1 \end{pmatrix}.$$

Thus, $h(\delta x \delta^{-1}) = \psi^{-1}(\delta)h(x)$. This shows that Δ acts on H via ψ^{-1}. In particular, we see that H injects into $H \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{F}(\psi^{-1})$, which in turn sits inside of $A_F^{\psi^{-1}}$. This completes the proof of the theorem.

5.5 Λ-adic Modular Forms

In this section we introduce Λ-adic modular forms, or what have come to be known as Hida families as they were first introduced by Hida. As in section 5.3 we content ourselves with definitions and statements, leaving the interested reader to consult the references for proofs. For details one should consult [Wiles1] or [Wiles2].

Let p be a fixed odd prime and fix embeddings $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$ and $\mathbb{C}$. Let $N \geq 1$ with $\mathrm{ord}_p(N) \leq 1$. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Q}}_p^\times$ be a Dirichlet character (not necessarily primitive). Let $\mathcal{O}$ be the ring of integers of some finite extension of $\mathbb{Q}_p$ so that $\mathbb{Z}_p[\chi] \subset \mathcal{O}$. Set $\Lambda_{\mathcal{O}} = \mathcal{O}[\![T]\!]$. Set $\mathfrak{X} = \{(k,\zeta) : k \in \mathbb{Z}, k \geq 2, \zeta \in \mu_{p^\infty}\}$. For each $(k,\zeta) \in \mathfrak{X}$, let $\nu_{k,\zeta} : \Lambda_{\mathcal{O}} \to \mathcal{O}[\zeta]$ be the homomorphism given by $\nu_{k,\zeta}(1+T) = \zeta(1+p)^{k-2}$. Define a character $\psi_\zeta : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \overline{\mathbb{Q}}_p^\times$ by $\psi_\zeta(1+p) = \zeta$. We make the following definition.

Definition 5.20. A $\Lambda_{\mathcal{O}}$*-adic modular form with character* χ is a collection

$$\mathcal{F} = \{c_n(T) \in \Lambda_{\mathcal{O}} : n = 0,1,2,\dots\}$$

such that for $(k,\zeta) \in \mathfrak{X}$ with $k \geq 2$ and $\zeta \in \mu_{p^r}$ one has

$$\nu_{k,\zeta}(\mathcal{F}) = \sum_{n=0}^{\infty} \nu_{k,\zeta}(c_n(T))q^n \in M_k(Np^r, \chi\omega^{2-k}\psi_\zeta, \mathcal{O}[\zeta])$$

for all but finitely many pairs $(k,\zeta) \in \mathfrak{X}$. We denote the space of such forms by $\mathcal{M}(N,\chi)$. We say $\mathcal{F}$ is a $\Lambda_{\mathcal{O}}$*-adic cusp form* if $\nu_{k,\zeta}(\mathcal{F}) \in S_k(Np^r, \chi\omega^{2-k}\psi_\zeta, \mathcal{O}[\zeta])$ for all but finitely many $(k,\zeta) \in \mathfrak{X}$. We write $\mathcal{S}(N,\chi)$ to denote the space of such forms.

Exercise 5.21. *Prove that* $\mathcal{M}(N,\chi)$ *is a torsion-free* $\Lambda_{\mathcal{O}}$*-module.*

We give the following example of a $\Lambda_{\mathcal{O}}$-adic modular form to establish such forms actually exist. It has the added benefit of being one of the main examples we will be interested in.

Example 5.22. Let $\chi : (\mathbb{Z}/N'\mathbb{Z})^\times \to \mathcal{O}^\times$ be a primitive Dirichlet character with $N' = N$ or Np and $\gcd(N,p) = 1$. For $\ell \neq p$ define a_ℓ as follows. Recall that

$$(\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p \cong \mathbb{Z}_p^\times$$

via the map $(\delta, a) \mapsto \delta(1+p)^a$. Then a_ℓ is defined by the equation

$$\ell = \omega(\ell)(1+p)^{a_\ell}. \tag{5.2}$$

We define the $c_n(T)$'s as follows where ℓ is a prime not equal to p.

$$\begin{aligned}
c_1(T) &= 1\\
c_\ell(T) &= 1+\chi(\ell)\ell(1+T)^{a_\ell}\\
c_{\ell^r}(T) &= c_\ell(T)c_{\ell^{r-1}}(T)-\chi(\ell)\ell(1+T)^{a_\ell}c_{\ell^{r-2}}(T) \qquad (r\geq 2)\\
c_n(T) &= c_{\ell_1^{r_1}}(T)\cdots c_{\ell_s^{r_s}}(T) \qquad (\gcd(n,p)=1,\ n=\prod \ell_i^{r_i})\\
c_{p^r n}(T) &= c_n(T) \qquad (\gcd(n,p)=1)\\
c_0(T) &= \frac{1}{2}\frac{\hat{G}_\chi(T)}{\hat{H}_\chi(T)}
\end{aligned}$$

where $\hat{G}_\chi(T)=G_{\chi\omega^2}((1+p)^2(1+T)-1)$ and $\hat{H}_\chi(T)=H_{\chi\omega^2}((1+p)^2(1+T)-1)$. Note that we have $c_p(T)=c_{p\cdot 1}(T)=c_1(T)=1$. We will use this fact later!

Suppose that $\chi\neq\omega^{-2}$ so that $\hat{H}_\chi(T)=1$. Set $\mathcal{E}_\chi=\{c_n(T)\}$. We wish to show that $\mathcal{E}_\chi$ is a Λ-adic modular form. We compute $\nu_{k,\zeta}(c_0(T))$ and $\nu_{k,\zeta}(c_\ell(T))$:

$$\begin{aligned}
\nu_{k,\zeta}(c_0(T)) &= \frac{1}{2}\nu_{k,\zeta}(G_{\chi\omega^2}((1+p)^2(1+T)-1))\\
&= \frac{1}{2}G_{\chi\omega^2}((1+p)^2\zeta(1+p)^{k-2}-1)\\
&= \frac{1}{2}\mathcal{L}_p(1-k,\chi\omega^2\psi_\zeta)\\
&= \frac{1}{2}L(1-k,\chi\omega^{2-k}\psi_\zeta)(1-\chi\omega^{2-k}\psi_\zeta(p)p^{k-1})
\end{aligned}$$

and

$$\begin{aligned}
\nu_{k,\zeta}(c_\ell(T)) &= \nu_{k,\zeta}(1+\chi(\ell)\ell(1+T)^{a_\ell})\\
&= 1+\chi(\ell)\ell\zeta^{a_\ell}(1+p)^{a_\ell(k-2)}\\
&= 1+\chi(\ell)\ell\psi_\zeta(\ell)(1+p)^{a_\ell(k-2)}\\
&= 1+\chi\omega^{2-k}\psi_\zeta(\ell)\ell^{k-1}.
\end{aligned}$$

It is then easy to see that the values $\nu_{k,\zeta}(c_\ell(T))$ give the Fourier coefficients of the Eisenstein series $E^{(k)}_{1,\chi\omega^{2-k}\psi_\zeta}(z)$ for $\ell\neq p$. Unfortunately, the coefficient $\nu_{k,\zeta}(c_0(T))$ as well as those $\nu_{k,\zeta}(c_m(T))$ where $p\mid m$ do not match up with the Fourier coefficients of this Eisenstein series. However, this can be overcome by considering the following modular form:

$$E(z):=E^{(k)}_{1,\chi\omega^{2-k}\psi_\zeta}(z)-\chi\omega^{2-k}\psi_\zeta(p)p^{k-1}E^{(k)}_{1,\chi\omega^{2-k}\psi_\zeta}(pz).$$

Exercise 5.23. *Check that the Fourier coefficients of E match up with the values $\nu_{k,\zeta}(c_n(T))$ for all $n\geq 0$.*

Thus, $\mathcal{E}_\chi$ is in fact a $\Lambda_{\mathcal{O}}$-adic modular form.

Before we proceed we extend our notion of $\Lambda_{\mathcal{O}}$-adic modular form. The reason for this is that we wish to realize cuspidal newforms as specializations of $\Lambda_{\mathcal{O}}$-adic forms as was just done for Eisensteins series. Let $F_{\Lambda_{\mathcal{O}}}$ be the fraction field of $\Lambda_{\mathcal{O}}$ and let L be a finite extension of $F_{\Lambda_{\mathcal{O}}}$. Let $\mathcal{O}_L$ be the integral closure of $\Lambda_{\mathcal{O}}$ in L. Note that $\mathcal{O}_L$ is a finite free $\Lambda_{\mathcal{O}}$-module. Set

$$\mathfrak{X}_L = \{\varphi : \mathcal{O}_L \to \overline{\mathbb{Q}}_p \mid \varphi \text{ extends } \nu_{k,\zeta} \text{ for some } (k,\zeta) \in \mathfrak{X}\}.$$

Then

$$\mathcal{F} = \{c_n \in \mathcal{O}_L : n = 0, 1, 2, \dots\}$$

is an $\mathcal{O}_L$-modular form if

$$\sum_{n=0}^{\infty} \varphi(c_n) q^n \in M_k(Np^r, \chi\omega^{2-k}\psi_\zeta, \varphi(\mathcal{O}_L))$$

for all but finitely many $\varphi \in \mathfrak{X}_L$. We write $\mathcal{M}_\chi(\mathcal{O}_L)$ to denote the space of $\mathcal{O}_L$-modular forms with character χ. The space of $\mathcal{O}_L$-cusp forms with character χ is defined analogously and denoted $\mathcal{S}_\chi(\mathcal{O}_L)$.

As was the case with classical forms we can define Hecke operators on these spaces. Of course for this to be a useful notion it is important that it commutes with specialization from a $\Lambda_{\mathcal{O}}$-adic form to a classical form. Let $\mathcal{F} = \{c_n\} \in \mathcal{M}_\chi(\mathcal{O}_L)$ and define $T_\ell \mathcal{F} = \{c_n' \in \mathcal{O}_L\}$ where the c_n' are defined by

$$\begin{aligned} c_0' &= c_0 + \chi(\ell)\ell(1+T)^{a_\ell} c_0 \\ c_n' &= c_{\ell n} + \begin{cases} 0 & \ell \nmid n, \ell \nmid Np \\ \chi(\ell)\ell(1+T)^{a_\ell} c_{n/\ell} & \ell | n, \ell \nmid Np \end{cases} \\ c_n' &= c_{\ell n} \qquad\quad \ell | Np. \end{aligned}$$

Using the same type of calculations we used above on the Eisenstein series one sees that $\varphi(T_\ell \mathcal{F}) = T_\ell \varphi(\mathcal{F})$. Thus we can define an action of T_n on $\mathcal{M}_\chi(\mathcal{O}_L)$ and $\mathcal{S}_\chi(\mathcal{O}_L)$. In fact, $\mathcal{S}_\chi(\mathcal{O}_L)$ is stable under this action.

The problem we now have is that in general $\mathcal{M}_\chi(\mathcal{O}_L)$ and $\mathcal{S}_\chi(\mathcal{O}_L)$ are not finitely generated $\mathcal{O}_L$-modules. To remedy this problem we cut the spaces down via the ordinary projector. Define

$$\mathcal{M}_\chi^0(\mathcal{O}_L) = \{\mathcal{F} \in \mathcal{M}_\chi(\mathcal{O}_L) : \varphi(\mathcal{F}) \in M_k^0(Np^r, \chi\omega^{2-k}\psi_\zeta, \varphi(\mathcal{O}_L)) \text{ for a.e. } \varphi \in \mathfrak{X}_L\}.$$

Similarly we define $\mathcal{S}_\chi^0(\mathcal{O}_L) \subseteq \mathcal{M}_\chi^0(\mathcal{O}_L)$. Alternatively one can extend Hida's ordinary projector e to the space of Λ-adic forms and define the ordinary parts this way. See ([Wiles1], Prop. 1.2.1) for a proof of this fact.

Proposition 5.24. *The spaces $\mathcal{M}_\chi^0(\mathcal{O}_L)$ and $\mathcal{S}_\chi^0(\mathcal{O}_L)$ are finitely generated torsion-free $\mathcal{O}_L$-modules.*

Proof. Note that these are torsion free from a previous exercise. Let $\mathcal{F}_1, \dots, \mathcal{F}_r \in \mathcal{M}_\chi(\mathcal{O}_L)$ be linearly independent over L. Write $\mathcal{F}_i = \{c_n^i\}$. The fact that these are linearly independent means we can find $n_1, \dots, n_r$ so that $D = \det(c_{n_i}^j)_{1 \le i,j \le r} \neq$

0. Thus, we can find $\varphi \in \mathfrak{X}_L$ so that $\varphi(\mathcal{F}_i) \in M_k^0(Np^r, \chi\omega^{2-k}\psi_\zeta, \mathcal{O}[\zeta])$ and $\varphi(D) = \det(\varphi(c_{n_i}^j)) \neq 0$. From this it follows that $\varphi(\mathcal{F}_1), \dots, \varphi(\mathcal{F}_r)$ are linearly independent in $M_k^0(Np^r, \chi\omega^{2-k}\psi_\zeta, \mathcal{O}[\zeta])$. However, we know that the dimension of $M_k^0(Np^r, \chi\omega^{2-k}\psi_\zeta, \mathcal{O}[\zeta])$ is bounded independent of k by Theorem 5.13. Thus we must have that r is bounded. Now assume that r is such that the linearly independent set above is maximal. Let $\mathcal{F} \in \mathcal{M}_\chi(\mathcal{O}_L)$. The fact that r is maximal implies there exist $x_i \in L$ so that $\mathcal{F} = \sum_{i=1}^r x_i\mathcal{F}_i$. Thus, $\underline{x} = {}^t(x_1, \dots, x_r)$ is a solution of the equation $(c_{n_i}^j)\underline{x} = (c_{n_i}(\mathcal{F}))$ and so $Dx_i \in \mathcal{O}_L$ for each $1 \leq i \leq r$. Hence $D\mathcal{M}_\chi^0(\mathcal{O}_L) \subseteq \sum \mathcal{O}_L\mathcal{F}_i$. Since $\mathcal{O}_L$ is Noetherian, if follows that $D\mathcal{M}_\chi^0(\mathcal{O}_L)$ is finitely generated ([Mats], page 15). Since we are torsion free, multiplication by D is an isomorphism so we obtain that $\mathcal{M}_\chi^0(\mathcal{O}_L)$ is finitely generated. □

Lemma 5.25. *The eigenvalues of T_ℓ acting on $\mathcal{M}_\chi^0(\mathcal{O}_L) \otimes_{\mathcal{O}_L} L$ are integral over $\mathcal{O}_L$. Note we tensor with L here to ensure we have a vector space over L. Since $\mathcal{M}_\chi^0(\mathcal{O}_L)$ is torsion free, we don't lose anything.*

Proof. We have from the previous proposition that $\mathcal{M}_\chi^0(\mathcal{O}_L)$ is a finitely generated $\mathcal{O}_L$-module. Let $\mathcal{F}_1, \dots, \mathcal{F}_r$ be the $\mathcal{O}_L$ generators and let $M = (a_{i,j}) \in \mathrm{M}_{r,r}(\mathcal{O}_L)$ be the matrix giving the action of T_ℓ on the $\mathcal{F}_i$'s. Set $P(x) = \det(x - M)$. Then $P(x)$ is a monic polynomial in $\mathcal{O}_L[x]$ and satisfies $P(T_\ell) = 0$ on $\mathcal{M}_\chi^0(\mathcal{O}_L)$. Thus, the eigenvalues of T_ℓ are the roots of $P(x)$, and so integral over $\mathcal{O}_L$. □

Recall the following fact about classical modular forms. If $\mathrm{ord}_\ell(M) = \mathrm{ord}_\ell(\mathrm{cond}(\psi))$ with ψ a Dirichlet character modulo M, then T_ℓ can be diagonalized on $M_k(M, \psi, \mathbb{C})$. We have the following analogous result in the current setting.

Lemma 5.26. *If $\ell = p$ or $\mathrm{ord}_\ell(N) = \mathrm{ord}_\ell(\chi)$, then T_ℓ can be diagonalized on $\mathcal{M}_\chi^0(\mathcal{O}_L) \otimes_{\mathcal{O}_L} \overline{L}$.*

Proof. Let $p(x)$ be the minimal polynomial of T_ℓ acting on $\mathcal{M}_\chi^0(\mathcal{O}_L) \otimes_{\mathcal{O}_L} \overline{L}$. We know that T_ℓ is diagonalizable if and only if $p(x)$ has all simple roots. Let $\alpha_1, \dots, \alpha_r$ be the distinct roots of $p(x)$ and consider the polynomial $q(x) = \prod(x - \alpha_i)$. We wish to show that $q(T_\ell) = 0$. Let L' be an extension of L so that $\alpha_i \in \mathcal{O}_{L'}$ for $i = 1, \dots, r$. We know such an L' exists by the previous lemma. Consider

$$\begin{aligned}\mathfrak{X} = \{\varphi \in \mathfrak{X}_{L'} : \varphi \text{ extends } \nu_{k,\zeta}, \mathrm{ord}_\ell(Np^r) = \mathrm{ord}_\ell(\mathrm{cond}(\chi\omega^{2-k}\psi_\zeta)) \text{ and}\\ \varphi(\mathcal{F}) \in M_k(Np^r, \chi\omega^{2-k}\psi_\zeta, \varphi(\mathcal{O}_{L'})) \text{ for all } \mathcal{F} \in \mathcal{M}_\chi^0(\mathcal{O}_{L'})\}.\end{aligned}$$

Note that $\mathfrak{X}$ is an infinite set. Observe that $\varphi(p(T_\ell))$ acts on $\varphi(\mathcal{M}_\chi^0(\mathcal{O}_{L'}))$ as 0 for all $\varphi \in \mathfrak{X}$. Using our result from the classical modular forms case we have that T_ℓ is diagonalizable on $\varphi(\mathcal{M}_\chi^0(\mathcal{O}_{L'}))$. Thus, $\varphi(q(T_\ell)) = 0$ on $\varphi(\mathcal{M}_\chi^0(\mathcal{O}_{L'}))$ for every $\varphi \in \mathfrak{X}$. Since $\mathfrak{X}$ is infinite, this implies $q(T_\ell) = 0$ and we are done. □

Definition 5.27. We say that $\mathcal{F} = \{c_n\} \in \mathcal{M}_\chi(\mathcal{O}_L)$ is an *eigenform* for T_ℓ if $T_\ell \mathcal{F} = a_\ell \mathcal{F}$ for some $a_\ell \in \overline{L}$. We say $\mathcal{F}$ is a *simultaneous eigenform* if it is an eigenform for all T_ℓ and it is said to be *normalized* if $c_1 = 1$. In this case $c_n = a_n$ as in the classical case.

We have the following standard corollaries. Their proofs proceed in the same manner as in the classical case.

Corollary 5.28. *The space $\mathcal{M}_\chi^0(\mathcal{O}_L) \otimes_{\mathcal{O}_L} \overline{L}$ is spanned by forms that are simultaneous eigenforms for all T_ℓ with $\ell \nmid N$.*

Corollary 5.29. *If χ is a primitive character modulo N or modulo Np then $\mathcal{M}_\chi^0(\mathcal{O}_L) \otimes_{\mathcal{O}_L} \overline{L}$ is spanned by forms that are simultaneous eigenforms for all T_ℓ.*

Corollary 5.30. *If $\mathcal{F} \in \mathcal{M}_\chi^0(\mathcal{O}_L)$ is a simultaneous eigenform for a collection $\{T_{\ell_i}\}$ of Hecke operators, the eigenvalues a_i are integral over Λ and generate a finite extension of Λ.*

We conclude this section with the following two results about Galois representations attached to $\mathcal{F} \in \mathcal{S}_\chi(\mathcal{O}_L)$ a normalized simultaneous eigenform with χ a Dirichlet character of conductor N' with $N' = Np^a$, $\gcd(N,p) = 1$ and $a \leq 1$. One should consult [Wiles1] for the proof of these theorems.

Theorem 5.31. *There exists a representation $\rho_\mathcal{F} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(L)$ such that*
1. $\rho_\mathcal{F}$ is continuous, i.e., there exists a finitely generated $\mathcal{O}_L$-submodule $M \subset L^2$ stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and such that this action is continuous
2. $\rho_\mathcal{F}$ is unramified at all $\ell \nmid Np$
3. $\mathrm{trace}(\rho_\mathcal{F}(\mathrm{Frob}_\ell) = c_\ell$ for all $\ell \nmid Np$
4. $\det(\rho_\mathcal{F}(\mathrm{Frob}_\ell) = \chi(\ell)\ell(1+T)^{a_\ell}$ where a_ℓ is defined as before
5. $\rho_\mathcal{F}$ is irreducible and odd ($\det(\rho_\mathcal{F}(complex\ conjugation)) = -1$).

Theorem 5.32. *If $\mathcal{F} \in \mathcal{S}_\chi^0(\mathcal{O}_L)$, then*

$$\rho_\mathcal{F} \mid_{D_p} \simeq \begin{pmatrix} \varepsilon_1 & * \\ 0 & \varepsilon_2 \end{pmatrix}$$

with ε_2 unramified and $\varepsilon_2(\mathrm{Frob}_p) = c_p$.

5.6 Proof of the Main Conjecture (outline)

Our goal in this section is to outline a proof of the fact that for χ an odd character of type S and p an odd prime one has

$$f_\chi(T) = g_{\chi^{-1}\omega}(T).$$

One accomplishes this by showing that if $\wp$ is a prime ideal of Λ_χ, then

$$\mathrm{ord}_\wp(f_\chi(T) = \mathrm{ord}_\wp(g_{\chi^{-1}\omega}(T)).$$

Recalling that all of the prime ideals of Λ_χ are of the form 0, (ϖ), $(P(T))$ for $P(T)$ irreducible and distinguished, or (ϖ, T), we see that we only need to prove the equality of orders for height 1 prime ideals as these constitute all of the possible prime factors of our polynomials. We will make use of the following classical result of Iwasawa which he obtained as an application of the analytic class number formula:

$$\sum_{\substack{\phi\in\Delta^\wedge \\ \phi \text{ odd}}} m_\wp(\phi) = \sum_{\substack{\phi\in\Delta^\wedge \\ \phi \text{ odd}}} n_\wp(\phi)$$

where $m_\wp(\phi) = \mathrm{ord}_\wp(f_\phi(T))$ and $n_\wp(\phi) = \mathrm{ord}_\wp(g_{\phi^{-1}\omega}(T))$. Thus, it is enough to show that $m_\wp(\phi) \geq n_\wp(\phi)$ for every $\wp$ and ϕ. One can accomplish this by constructing a subspace of V^χ on which $\gamma_0 - 1$ has characteristic polynomial $(T-\alpha_\wp)^{n_\wp(\phi)}$ where $\alpha_\wp$ is the root of $f_\chi(T)$ corresponding to $\wp$.

There are two types of primes $\wp$ that must be dealt with separately; $\wp = (T-p)$ and $\wp = (T-(\zeta-1))$ for ζ some p-power root of unity. These are referred to as the exceptional primes. The primes of the form $(T-(\zeta-1))$ can be dealt with using class field theory and we will say nothing more about them here. If $\wp = (T-p)$ and $\phi \neq \omega$, then we obtain that $\mathrm{ord}_\wp(g_{\phi^{-1}\omega}(T)) = 0$ from the fact that $\mathcal{L}_p(1, \phi^{-1}\omega) \neq 0$. If $\wp = (T-p)$ and $\phi = \omega$, then the result follows from the fact that $\mathcal{L}_p(s, 1)$ has a simple pole at $s = 1$. If $G_1(0) = 0$ we would have a contradiction to having a pole at $s = 1$. Thus, in either case we obtain $\mathrm{ord}_\wp(g_{\phi^{-1}\omega}(T)) = 0$.

We now must deal with the non-exceptional primes. Let $\psi = \chi^{-1}\omega^{-1}$. Fix a p-power root of unity τ such that $\hat{G}_\psi(T)$ and $\hat{G}_\psi(\tau^{-1}(1+p)^{-1}(1+T)-1)$ have no zeroes in common where we recall that $\hat{G}_\psi(T)$ is defined by

$$\hat{G}_\psi(T) = G_{\psi\omega^2}((1+p)^2(1+T)-1).$$

This is possible by the Weierstrass preparation theorem. Suppose τ is a p^s-th root of unity and let $\mathcal{O}$ be such that it contains $\mathcal{O}_\psi$ and τ. Recall that $\hat{G}_\psi(T)$ and $\hat{H}_\psi(T)$ are both in $\Lambda_\mathcal{O}$ and $\hat{H}_\psi(T) = 1$ if $\psi \neq \omega^{-2}$. Let $\mathbb{T} \subset \mathrm{End}_{\Lambda_\mathcal{O}} \mathcal{S}^0_\psi(\Lambda_\mathcal{O})$ be the Hecke algebra generated over $\Lambda_\mathcal{O}$ by the T_n's.

Definition 5.33. The *Eisenstein ideal* $I \subset \mathbb{T}$ is the ideal generated by the set

$$\{T_n - c_\psi(n), \hat{G}_\psi(T)\}$$

where n ranges over all positive integers.

We then have the following proposition.

Proposition 5.34. *Suppose* $\psi \neq \omega^{-2}$ *and let* $\wp \subseteq \Lambda_\mathcal{O}$ *be any prime divisor of* $\hat{G}_\psi(T)$ *such that* $p \notin \wp$, $\wp \neq ((1+p)^2(1+T)-1)$, *and* $\wp \neq ((1+p)(1+T)-\zeta)$. *(Note that these last two types correspond to the exceptional primes under this normalization.) Then there exists a* $\Lambda_{\mathcal{O},\wp}$*-isomorphism*

$$\mathbb{T}_\wp/I \xrightarrow{\simeq} \Lambda_{\mathcal{O},\wp}/(\hat{G}_\psi(T)).$$

Moreover, if we define $\mathfrak{P}$ to be the kernel of the map

$$\mathbb{T} \longrightarrow \Lambda_{\mathcal{O},\wp}/(\hat{G}_\psi(T)) \longrightarrow \Lambda_{\mathcal{O},\wp}/\wp$$

then we have the $\Lambda_{\mathcal{O},\wp}$-isomorphism

$$\mathbb{T}_{\mathfrak{P}}/I \xrightarrow{\simeq} \Lambda_{\mathcal{O},\wp}/(\hat{G}_\psi(T)).$$

Before we prove this proposition we need the following lemma.

Lemma 5.35. *Let ζ be a p^{r-1}-th root of unity, $k \geq 2$, and χ a character so that $N|\operatorname{cond}(\chi)$. Define*

$$w = e\prod_{\ell|N} T_\ell(T_\ell^h - \ell^h\psi_\zeta(\ell)(1+p)^{a_\ell h(k-2)})$$

where $h = \varphi(Np)$. If $f \in M_k(Np^r, \chi\omega^{2-k}\psi_\zeta)$ with $a_f(0) = 0$, then wf is a cusp form.

Proof. Write $f = F + E$ where F is a cusp form and E is in the span of the Eisenstein series. We can write

$$E = \sum c(\psi_1,\psi_2)E^{(k)}_{\psi_1,\psi_2}$$

where $\psi_1\psi_2 = \chi\omega^{2-k}\psi_\zeta$ and $\operatorname{cond}(\psi_1)\operatorname{cond}(\psi_2) = Np^r$.
If $p|\operatorname{cond}(\psi_1)$, then $eE^{(k)}_{\psi_1,\psi_2} = 0$ because the p-th Fourier coefficient is $\psi_2(p)p^{k-1}$ and so $E^{(k)}_{\psi_1,\psi_2}$ is not ordinary at p.
If $\ell \neq p$ is a prime with $\ell|\operatorname{cond}(\psi_1)$ and $\ell|\operatorname{cond}(\psi_2)$, then $T_\ell E^{(k)}_{\psi_1,\psi_2} = 0$ because the ℓ-th eigenvalue is 0.
If $\ell \neq p$ is a prime with $\ell|\operatorname{cond}(\psi_1)$ and $\ell \nmid \operatorname{cond}(\psi_2)$, then we have $T_\ell E^{(k)}_{\psi_1,\psi_2} = \psi_2(\ell)\ell^{k-1}E^{(k)}_{\psi_1,\psi_2}$. Thus,

$$\begin{aligned} T_\ell^h E^{(k)}_{\psi_1,\psi_2} &= (\psi_2(\ell)\ell^{k-1})^h E^{(k)}_{\psi_1,\psi_2} \\ &= \psi_2(\ell)^h(\omega(\ell)^{k-1})^h(1+p)^{a_\ell h(k-1)}E^{(k)}_{\psi_1,\psi_2} \end{aligned}$$

where we have used that $\omega(\ell)^h = 1$ since ω has conductor p. Observe that $\psi_2(\ell) = \psi_\zeta(\ell)$ and that $(1+p)^{a_\ell h(k-1)} = \ell^h(1+p)^{a_\ell h(k-2)}$. Thus, we see that

$$T_\ell^h E^{(k)}_{\psi_1,\psi_2} = \ell^h\psi_\zeta(\ell)(1+p)^{a_\ell h(k-2)}E^{(k)}_{\psi_1,\psi_2},$$

in particular we have that $T_\ell^h - \ell^h\psi_\zeta(\ell)(1+p)^{a_\ell h(k-2)}$ kills $E^{(k)}_{\psi_1,\psi_2}$.
From this we can conclude that unless ψ_1 has conductor equal to 1, i.e., ψ_1 is trivial, we must have that $E^{(k)}_{\psi_1,\psi_2}$ is killed by w. Thus we have

$$\begin{aligned} wE &= c(1,\chi\omega^{2-k}\psi_\zeta)wE^{(k)}_{1,\chi\omega^{2-k}\psi_\zeta} \\ &= c'E^{(k)}_{1,\chi\omega^{2-k}\psi_\zeta} \end{aligned}$$

for some constant c'. However, we have that wf and wF both must have constant term 0 and

$$wf = wF + c' E^{(k)}_{1,\chi\omega^{2-k}\psi_\zeta}$$

where $c' E^{(k)}_{1,\chi\omega^{2-k}\psi_\zeta}$ has constant term $c' \frac{L(1-k,\chi\omega^{2-k}\psi_\zeta)}{2}$. Thus, $c' = 0$ and so $wf = wF$ is a cusp form as claimed. □

Proof. (of Proposition 5.34) Set

$$\mathcal{G}(T) = \mathcal{G}_\tau(T) = E^{(1)}_{1,\psi_\tau\omega^{-1}}(z)\, \mathcal{E}_{\psi\psi_\tau^{-1}}((1+p)^{-1}(1+T)-1).$$

Let the Eisenstein series $\mathcal{E}_{\psi\psi_\tau^{-1}}((1+p)^{-1}(1+T)-1)$ be defined by the data $\{c_{\psi\psi_\tau^{-1}}(n)\}$. We claim that $\mathcal{G}$ is a $\Lambda_{\mathcal{O}}$-adic modular form. We show this by looking at specializations. Let ζ be a primitive p^r-th root of unity and $v_{k,\zeta} : \Lambda_{\mathcal{O}} \to \mathcal{O}[\zeta]$ a specialization map. Then we have

$$v_{k,\zeta}\mathcal{G} = E^{(1)}_{1,\psi_\tau\omega^{-1}}(z) E^{(k-1)}_{1,\psi\psi_\tau^{-1}\omega^{3-k}\psi_\zeta}(z) \in M_k(Np^{\max(r,s)+1}, \psi\psi_\zeta\omega^{2-k})$$

as desired. Let $\mathcal{G}$ be defined by the data $\{c(n,\mathcal{G})\}$. We have

$$\begin{aligned} c(0,\mathcal{G}) &= \frac{L(0,\psi_\tau\omega^{-1})}{2}\,\frac{\hat{G}_{\psi\psi_\tau^{-1}}((1+p)^{-1}(1+T)-1)}{2} \\ &= \frac{1}{4}\, L(0,\psi_\tau\omega^{-1})\,\hat{G}_\psi(\tau^{-1}(1+p)^{-1}(1+T)-1). \end{aligned}$$

Set $\mathcal{F}_0 = c(0,\mathcal{G})\mathcal{E}_\psi - c_\psi(0)\mathcal{G}$. This is a $\Lambda_{\mathcal{O}}$-modular form. Write $\mathcal{F}_0 = \{c(n,\mathcal{F}_0)\}$ and observe that by construction we have $c(0,\mathcal{F}_0) = 0$. If we apply the previous lemma we obtain that

$$\mathcal{F} = c(0,\mathcal{G})w\mathcal{E}_\psi - c_\psi(0)w\mathcal{G}$$

is a cusp form. So we obtain

$$\mathcal{F} \equiv c(0,\mathcal{G})w\mathcal{E}_\psi (\operatorname{mod} c_\psi(0)).$$

We would like to show that $c(1,\mathcal{F})$ is a $\wp$-unit as this will allow us to conclude that $\mathcal{F}$ is part of a $\Lambda_{\mathcal{O},\wp}$-basis of $\mathcal{S}^0_\psi(\Lambda_{\mathcal{O}})_\wp$. Observe that we have $c(1,\mathcal{F}) \equiv c(0,\mathcal{G})c(1,w\mathcal{E}_\psi)(\operatorname{mod} c_\psi(0))$. Thus, we need to look at $w\mathcal{E}_\psi$ more closely. Note that $e\mathcal{E}_\psi = \mathcal{E}_\psi$ since $c_\psi(1) = 1$ and this is the eigenvalue when T_p acts on $\mathcal{E}_\psi$.

Exercise 5.36. *For $\ell \mid N = \operatorname{cond}(\psi)$, $T_\ell\mathcal{E}_\psi = \mathcal{E}_\psi$.*

Thus, we have that

$$w\mathcal{E}_\psi = \prod_{\ell \mid N}(1 - \ell^h(1+T)^{a_\ell h})\mathcal{E}_\psi,$$

i.e.,

$$c(1,\mathcal{F}) \equiv c(0,\mathcal{G}) \prod_{\ell \mid N}(1 - \ell^h(1+T)^{a_\ell h})(\operatorname{mod} c_\psi(0)).$$

However, our choice of τ and the fact that $p \notin \wp$ gives that $c(0,\mathcal{G})$ is a unit modulo $\wp$. (The fact that $p \notin \wp$ implies that $\wp$ must be of the form $(P(T))$ for a distinguised polynomial, and hence $\wp \nmid L(0,\psi_\tau\omega^{-1})$.) Since we assumed that $\wp$ is not an exceptional prime we obtain that $\prod_{\ell | N}(1-\ell^h(1+T)^{a_\ell h})$ is a unit modulo $\wp$ as the exceptional primes are the only possible prime divisors of $\prod_{\ell | N}(1-\ell^h(1+T)^{a_\ell h})$.

So we have shown that we can choose $\mathcal{F}$ to be part of a $\Lambda_{\mathcal{O},\wp}$-basis of $S^0_\psi(\Lambda_\mathcal{O})_\wp$. Let $\mathcal{H}_0 = \mathcal{F}, \mathcal{H}_1, \ldots, \mathcal{H}_r$ be a basis of $S^0_\psi(\Lambda_\mathcal{O})_\wp$. Let $t \in \mathbb{T}_\wp$ and write $t\mathcal{F} = \sum \lambda_i(t)\mathcal{H}_i$ for some $\lambda_i(t) \in \Lambda_{\mathcal{O},\wp}$. Consider the map

$$\mathbb{T}_\wp \longrightarrow \Lambda_{\mathcal{O},\wp}/(\hat{G}_\psi)$$

defined by $t \mapsto \lambda_0(t)$. This is a surjective $\Lambda_{\mathcal{O},\wp}$-module map as $1 \mapsto 1$. Observe that $\lambda_0(T_n - c_\psi(n)) = 0$. This is because of the fact that

$$(T_n - c_\psi(n))\mathcal{F} = (T_n - c_\psi(n))c(0,\mathcal{G})w\mathcal{E}_\psi + (T_n - c_\psi(n))c_\psi(0)w\mathcal{G}$$

and $(T_n - c_\psi(n))\mathcal{E}_\psi = 0$ and $c_\psi(0) = \frac{1}{2}\hat{G}_\psi$, which is 0 modulo $\hat{G}_\psi$. Thus we have that $\lambda_0(T_n) = c_\psi(n)$ and so $\lambda_0(T_nT_m) = \lambda_0(T_n)\lambda_0(T_m)$. Hence, λ_0 is a surjective $\Lambda_{\mathcal{O},\wp}$-algebra map. We also have shown that $I \subseteq \ker\lambda_0$ and since I is necessarily a maximal ideal we have the result. □

Recall that $\mathcal{S}^0_\psi(\Lambda_\mathcal{O}) \otimes_{\Lambda_\mathcal{O}} \overline{F}_{\Lambda_\mathcal{O}}$ is spanned by eigenforms where $F_{\Lambda_\mathcal{O}}$ is the fraction field of $\Lambda_\mathcal{O}$. Thus, there exists a finite extension L of $F_{\Lambda_\mathcal{O}}$ so that $\mathcal{S}^0_\psi(\Lambda_\mathcal{O}) \otimes_{\Lambda_\mathcal{O}} L$ is spanned by eigenforms $\mathcal{F}_1, \ldots, \mathcal{F}_r \in \mathcal{S}^0_\psi(\Lambda_\mathcal{O})$. Let $L_i \subseteq L$ be the field extensions of $F_{\Lambda_\mathcal{O}}$ generated by the eigenvalues of $\mathcal{F}_i$. Let $\{\mathcal{F}_i\}_{i\in J}$ be the representatives of conjugacy classes where we say $\mathcal{F}_i \sim \mathcal{F}_j$ if there exists an isomorphism $\sigma : L_i \to L_j$ over $F_{\Lambda_\mathcal{O}}$ taking $\mathcal{F}_i$ to $\mathcal{F}_j$. Set $A = \prod_{i\in J} L_i$. One has that $\mathbb{T}$ is naturally a subring of A via the map

$$t \mapsto \prod_{i \in J} c(1, t\mathcal{F}_i).$$

As in the case of classical modular forms, one obtains an isomorphism of L aglebras

$$\mathbb{T} \otimes_{\Lambda_\mathcal{O}} L \xrightarrow{\simeq} A \otimes_{\Lambda_\mathcal{O}} L \xrightarrow{\simeq} \prod_{i\in J} L.$$

In particular, by counting dimensions one obtains

$$\mathbb{T} \otimes_{\Lambda_\mathcal{O}} F_{\Lambda_\mathcal{O}} \xrightarrow{\simeq} A.$$

Set W to be the $\mathbb{T}$-module $A \oplus A$ and $W_\mathfrak{P}$ to be the $\mathbb{T}_\mathfrak{P}$-module $A_\mathfrak{P} \oplus A_\mathfrak{P}$. Write $A_\mathfrak{P} = \prod_{i \in J_\mathfrak{P} \subseteq J} L_i$.

Let $\rho_{\mathcal{F}_i}$ be the Galois representation associated to $\mathcal{F}_i$. Set $\eta = \det \rho_{F_i}$. As in the classical case, observe that η is independent of i. Fix $\sigma_0 \in I_p$ such that $\eta(\sigma_0) \neq 1 (\mathrm{mod}\, \wp)$. Fix a basis of $\rho_{\mathcal{F}_i}$ such that

1. $\rho_{\mathcal{F}_i}(\sigma_0) = \begin{pmatrix} \alpha_i & 0 \\ 0 & \beta_i \end{pmatrix}$

2. $\rho_{\mathcal{F}_i}|_{D_p} = \begin{pmatrix} \psi_2^{(i)} & 0 \\ * & \psi_1^{(i)} \end{pmatrix}, \quad \psi_2^{(i)}|_{I_p} = 1$

3. $\rho_{\mathcal{F}_i} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathcal{O}_{L_i,\wp_i})$ where $\wp_i$ is some fixed prime over $\wp$.

We put a Galois action on $W_{\mathfrak{P}}$ via $\oplus_{i\in J_{\mathfrak{P}}}\rho_{\mathcal{F}_i}$. This action commutes with the action of $\mathbb{T}_{\mathfrak{P}}$.

Definition 5.37. A submodule $\mathscr{L} \subseteq W_{\mathfrak{P}}$ is a *lattice* if it is a finitely generated $\mathbb{T}_{\mathfrak{P}}$-module such that $\mathscr{L} \otimes_{\Lambda_{\mathcal{O}}} F_{\Lambda_{\mathcal{O}}} = W_{\mathfrak{P}}$. We say the lattice is a *stable lattice* if it is also stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Lemma 5.38. *([Wiles2], Lemma 5.1) Let $\mathscr{L}$ be any stable lattice in $W_{\mathfrak{P}}$. Suppose that V is any irreducible subquotient of $\mathscr{L}/I\mathscr{L}$. Then V has one of the following two types:*
1. $V \xrightarrow{\simeq} \mathbb{T}_{\mathfrak{P}}/\mathfrak{P}\mathbb{T}_{\mathfrak{P}}$ with trivial Galois action (V is of type 1.)
2. $V \xrightarrow{\simeq} \mathbb{T}_{\mathfrak{P}}/\mathfrak{P}\mathbb{T}_{\mathfrak{P}}$ with Galois acting by η (V is of type η.)

Proof. This is essentially an application of the Brauer-Nesbitt theorem. To see this, observe that on $\mathscr{L}$ one has

$$(\mathrm{Frob}_\ell)^2 - T_\ell \,\mathrm{Frob}_\ell + \eta(\ell) = 0$$

as this holds for each $\rho_{\mathcal{F}_i}$ and that on $\mathscr{L}/I\mathscr{L}$ one has $T_\ell = 1 + \eta(\ell)$. Thus

$$(\mathrm{Frob}_\ell - 1)(\mathrm{Frob}_\ell - \eta(\ell)) = 0$$

on $\mathscr{L}/I\mathscr{L}$. □

Definition 5.39. Let M be a $\mathbb{T}_{\mathfrak{P}}[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module. We say M is of *type*-1 (resp. *type*-η) if it has Jordan-Hölder series decomposition with all successive quotients of type-1 (resp. type-η.)

Let

$$\mathscr{L}_0' = \left(\prod_{i\in J_{\mathfrak{P}}} \mathcal{O}_{L_i,\wp_i}\right) \oplus \mathbb{T}_{\mathfrak{P}}.$$

One can show that this is a stable lattice by using the properties used in defining the bases of the $\rho_{\mathcal{F}_i}$. We actually want a slightly different lattice. Note that by our choice of bases above for $\rho_{\mathcal{F}_i}$ that if we write

$$\rho(\sigma) = \bigoplus_{i\in J_{\mathfrak{P}}} \rho_{\mathcal{F}_i} = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix},$$

then a_σ and d_σ lie in $\mathbb{T}_{\mathfrak{P}}$. Using that the Galois representations are continuous, we have that there exists $x \in \Lambda_{\mathcal{O},\wp}$ so that $xc_\sigma \in \mathbb{T}_{\mathfrak{P}}$. If we replace ρ by

$\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix}\rho\begin{pmatrix}1 & 0\\ 0 & x^{-1}\end{pmatrix}$, then the c_σ and d_σ we obtain from this are both in $\mathbb{T}_{\mathfrak{P}}$. Calling this new Galois representation ρ as well, we see that the lattice

$$\mathscr{L}_0 = \left(\prod_{i\in J_{\mathfrak{P}}} \frac{1}{x}\mathcal{O}_{L_i,\wp_i}\right) \oplus \mathbb{T}_{\mathfrak{P}}$$

is a stable lattice. We wish to find a stable lattice $\mathscr{L} \subseteq \mathscr{L}_0$ with filtration

$$\begin{tikzcd} 0 \arrow[r] & (\text{type-1}) \arrow[r] & \mathscr{L}/I\mathscr{L} \arrow[r] & (\text{type-}\eta) \arrow[r] & 0 \end{tikzcd}$$

so that $\mathscr{L}/I\mathscr{L}$ has no type-1 quotient. Note that the filtration is the analogy of finding a lattice so that

$$\overline{\rho}_f = \begin{pmatrix}1 & *\\ 0 & \psi\end{pmatrix}$$

in section 5.4 and the lack of a type-1 quotient is the analogy of $\overline{\rho}_f$ being nonsplit.

Proposition 5.40. *([Wiles2], Proposition 5.2) Let $\mathscr{L}$ be a stable lattice. There exists a stable sublattice $\mathscr{L}' \subseteq \mathscr{L}$ such that*

1. *$\mathscr{L}/\mathscr{L}'$ has type-1*
2. *If $\mathscr{L}'' \subseteq \mathscr{L}$ is a stable sublattice such that $\mathscr{L}/\mathscr{L}''$ has type-1, then $\mathscr{L}' \subseteq \mathscr{L}''$.*

One also has the corresponding statement for type-η.

Proof. We begin by noting that if $\mathscr{L}_1$ and $\mathscr{L}_2$ both satisfy that $\mathscr{L}/\mathscr{L}_1$ and $\mathscr{L}/\mathscr{L}_2$ are of type-1, then so is $\mathscr{L}/\mathscr{L}_1 \cap \mathscr{L}_2$. Suppose we have a collection of stable sublattices $\{\mathscr{L}_i\}_{i\in\mathcal{I}}$ such that $\mathscr{L}/\mathscr{L}_i$ is of type-1 for each $i \in \mathcal{I}$. Set $\mathscr{N} = \bigcap_{i\in\mathcal{I}} \mathscr{L}_i$. We want to be able to set $\mathscr{L}' = \mathscr{N}$. If $\mathscr{N}$ is a lattice we can do this and we will be done.

Suppose $\mathscr{N}$ is not a lattice. We have that $\mathscr{L}/\mathscr{N}$ is finitely generated as a $\Lambda_{\mathcal{O},\wp}$-module and $(\mathscr{L}/\mathscr{N}) \otimes_{\Lambda_{\mathcal{O}}} F_{\Lambda_{\mathcal{O}}} \neq 0$. We know that $(\mathscr{L}/\mathscr{N}) \otimes_{\Lambda_{\mathcal{O}}} F_{\Lambda_{\mathcal{O}}}$ is a quotient of $W_{\mathfrak{P}}$, so as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module its irreducible components come from the $\rho_{\mathcal{F}_i}$'s. Write

$$(\mathscr{L}/\mathscr{N}) \otimes_{\Lambda_{\mathcal{O}}} F_{\Lambda_{\mathcal{O}}} \cong \bigoplus_{i\in J'_{\mathfrak{P}}} \rho_{\mathcal{F}_i}. \tag{5.3}$$

Set

$$(\mathscr{L}/\mathscr{N})^{(\eta)} = \{x \in \mathscr{L}/\mathscr{N} : \sigma_0 x = \eta(\sigma_0)x\}.$$

Equation 5.3 gives that $(\mathscr{L}/\mathscr{N})^{(\eta)} \neq 0$. On the other hand,

$$\mathscr{L}/\mathscr{N} \hookrightarrow \prod_{i\in\mathcal{I}} \mathscr{L}/\mathscr{L}_i$$

where each $\mathscr{L}/\mathscr{L}_i$ is of type-1. Since we have that $\eta(\sigma_0) \not\equiv 1 (\operatorname{mod} \mathfrak{P})$, $(\mathscr{L}/\mathscr{N})^{(\eta)}$ maps to 0 in $\mathscr{L}/\mathscr{L}_i$. Thus, $(\mathscr{L}/\mathscr{N})^{(\eta)} = 0$. This contradiction shows that $\mathscr{N}$ must be a lattice and we are done. □

We apply Proposition 5.40 to teh stable lattice $\mathscr{L}_0$ constructed above and set $\mathscr{L} = \mathscr{L}_0'$. The minimality of the lattice $\mathscr{L}$ shows that $\mathscr{L}/I\mathscr{L}$ has no type-1 quotients. Set $E = \mathscr{L}/I\mathscr{L}$ and let E_1 be the maximal type-1 submodule of E. Set $E_2 = E/E_1$ and observe that $E_2 \neq 0$ as E is not purely type-1 by Proposition 5.40 applied to type-η. Let E_η be the maximal type-η submodule of E_2 and observe that $E_\eta \neq 0$ by the maximality of E_1.

Lemma 5.41. *For E_2 and E_η as above, $E_2 = E_\eta$.*

Proof. Suppose $E_2 \neq E_\eta$. We can use the facts that E_2/E_η has no type-η submodule and E_2 has no type-1 quotient to conclude that there exists E' and E'' so that

1. $E_\eta \subset E' \subsetneq E'' \subset E_2$
2. E'/E_η is type-1 and maximal with respect to this property
3. E''/E' is type-η and irreducible.

Recall that we fixed σ_0 so that $\eta(\sigma_0) \not\equiv 1 (\operatorname{mod} \mathfrak{P})$. Using that E''/E' is irreducible, we have

$$(\sigma_0 - 1)E''/E' = E''/E'.$$

Let $z' \in E''$ be a $\mathbb{T}_{\mathfrak{P}}$-generator of E''/E'. Set $z = (\sigma_0 - 1)z' \in E''$ and observe this is still a generator. Recall that $(\sigma - 1)(\sigma - \eta(\sigma))$ annihilates $E = \mathscr{L}/I\mathscr{L}$ for every $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In particular,

$$(\sigma_0 - \eta(\sigma_0))z = (\sigma_0 - \eta(\sigma_0))(\sigma_0 - 1)z' = 0$$

in E''. Thus,

$$\sigma_0 z = \eta(\sigma_0) z \tag{5.4}$$

in E_2.
Claim: $(\sigma_0 - 1)(\sigma - \eta(\sigma))z = 0$ in E_2 for every $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
Proof: We begin by observing that

$$\begin{aligned}(\sigma_0\sigma - 0)((\sigma - \eta(\sigma)) + (\sigma_0 - 1)(\sigma - \eta(\sigma)))z &= (\sigma_0\sigma - 1)(\sigma_0\sigma - \sigma_0\eta(\sigma))z \\ &= (\sigma_0 - 1)(\sigma_0\sigma - \eta(\sigma_0\sigma)) \\ &= 0\end{aligned}$$

where we have used equation 5.4 and that $(\sigma - 1)(\sigma - \eta(\sigma))$ annihilates E. If we expand the left hand side of the first equation above we obtain

$$(\sigma_0\sigma - 1)(\sigma - \eta(\sigma))z + (\sigma_0\sigma - 1)(\sigma_0 - 1)(\sigma - \eta(\sigma))z = 0.$$

Observe that

$$\begin{aligned}(\sigma_0\sigma - 1)(\sigma - \eta(\sigma))z &= \sigma_0\sigma(\sigma - \eta(\sigma))z - (\sigma - \eta(\sigma))z\\ &= \sigma_0(\sigma - \eta(\sigma))z - (\sigma - \eta(\sigma))z\\ &= (\sigma_0 - 1)(\sigma - \eta(\sigma))z\end{aligned}$$

where we have used that σ acts as 1 on $(\sigma - \eta(\sigma))z$ by virtue of the fact that $(\sigma - 1)(\sigma - \eta(\sigma))$ annihilates E. Thus, we have

$$(\sigma_0 - 1)(\sigma - \eta(\sigma))z + (\sigma_0\sigma - 1)(\sigma_0 - 1)(\sigma - \eta(\sigma))z = 0$$

i.e.,

$$\sigma_0\sigma(\sigma_0 - 1)(\sigma - \eta(\sigma))z = 0.$$

Thus, $(\sigma_0 - 1)(\sigma - \eta(\sigma))z = 0$ (act on each side by $(\sigma_0\sigma)^{-1}$ to see this.) This completes the proof of the claim.

Observe that

$$(\sigma' - \eta(\sigma'))(\sigma - \eta(\sigma)) = (\sigma'\sigma - \eta(\sigma'\sigma)) - \eta(\sigma')(\sigma - \eta(\sigma)) - \eta(\sigma)(\sigma' - \eta(\sigma')).$$

Thus, applying the claim we obtain that

$$(\sigma_0 - 1)(\sigma' - \eta(\sigma'))(\sigma - \eta(\sigma))z = 0 \tag{5.5}$$

for every $\sigma, \sigma' \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let M be the $\mathbb{T}_{\mathfrak{P}}$-span of E_η and the $(\sigma - \eta(\sigma))z$. Note that $M \subseteq E_2$ and M is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. To see that M is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module, observe that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts via 1 on E'/E_η and E_η is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. We also have that $E_\eta \subsetneq M \subset E'$ because if we had $N = E_\eta$, then $E_\eta + \mathbb{T}_{\mathfrak{P}}z$ is a $\mathbb{T}_{\mathfrak{P}}[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module of type η larger then E_η.

Let $H = \ker\eta$. Note that for $h \in H$ we have $(h-1)E_\eta = 0$ and $(h-1)(\sigma - \eta(\sigma))z \in E_\eta$. Thus, equation 5.5 gives that

$$(\sigma_0 - 1)(h-1)(\sigma - \eta(\sigma))z = 0$$

and so

$$(\sigma_0 - 1)(h-1)(\sigma - \eta(\sigma))z = (\eta(\sigma_0) - 1)(h-1)(\sigma - \eta(\sigma))z = 0.$$

Using that $(\eta(\sigma_0) - 1)$ is a unit on E_η, we have that

$$(h-1)(\sigma - \eta(\sigma))z = 0$$

for every $h \in H$. Thus, $(h-1)M = 0$ for every $h \in H$.

Let $U = M \cap \ker(\sigma_0 - 1)$. Note that $U \neq 0$ because $(\sigma_0 - 1)M \subseteq E_\eta \subseteq M$. Let $u \in U$ and $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Observe that

$$\sigma_0 gu = (\sigma_0 g\sigma_0^{-1}g^{-1})(g\sigma_0 u) = g\sigma_0 u = gu.$$

Thus, $gU \subseteq U$ and so U is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. However, any irreducible module in U is of type-1. This is a contradiction as it gives a submodule of E_2 of type-1. Thus, we must have $E_2 = E_\eta$. □

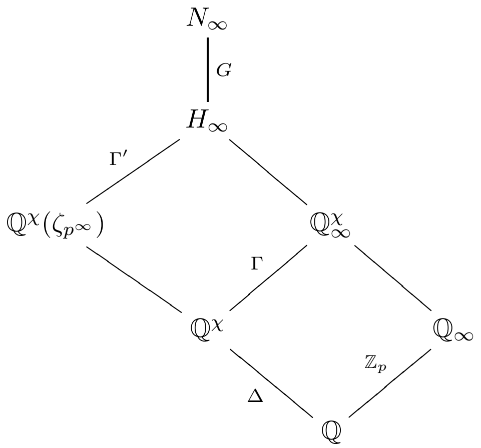
Proposition 5.42. *There is an exact sequence of* $\mathbb{T}_{\mathfrak{P}}[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$*-modules*

$$\begin{tikzcd} 0 \arrow[r] & E_1 \arrow[r] & E \arrow[r] & E_\eta \arrow[r] & 0 \end{tikzcd}$$

such that E_1 *is of type-1 and* $E_\eta \cong \mathbb{T}_{\mathfrak{P}}/I$ *is of type-*η*.*

Proof. The only thing that remains to be shown in this proposition is that $E_\eta \cong \mathbb{T}_{\mathfrak{P}}/I$. Recall from our definition of $\mathscr{L}_0$ that we can write $\mathscr{L}_0 = \mathscr{L}_0^{(1)} \oplus \mathscr{L}_0^{(\eta)}$ where $\mathscr{L}_0^{(1)} = \prod \frac{1}{x}\mathcal{O}_{L_i,\wp_i}$ and $\mathscr{L}_0^{(\eta)} = \mathbb{T}_{\mathfrak{P}}$. Observe that σ_0 acts on $\mathscr{L}_0^{(1)}/I$ by 1 and on $\mathscr{L}_0^{(\eta)}/I$ by $\eta(\sigma_0)$. Using that $\mathscr{L}_0/\mathscr{L}$ is of type-1 we have that $\mathscr{L}_0^{(\eta)} \subseteq \mathscr{L}$. Write $\mathscr{L} = \mathscr{L}^{(1)} \oplus \mathscr{L}^{(\eta)}$ with $\mathscr{L}^{(1)} \subseteq \mathscr{L}_0^{(1)}$ and $\mathscr{L}^{(\eta)} \subseteq \mathscr{L}_0^{(\eta)} \cong \mathbb{T}_{\mathfrak{P}}$. Similarly, we can split E up as $E = E^{(1)} + E^{(\eta)}$. Now just observe that by construction we must have $E^{(\eta)} \cong E_\eta$. Thus, $E_\eta \cong \mathbb{T}_{\mathfrak{P}}/I$ as desired. □

Set $H_\infty = \mathbb{Q}^\chi(\zeta_{p^\infty})\mathbb{Q}_\infty$. Recalling that $\eta(\mathrm{Frob}_\ell) = \psi(\ell)\ell(1+T)^{a_\ell}$, we see that η is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^\chi(\zeta_{p^\infty}))$ as we lose the χ because of the $\mathbb{Q}^\chi$ and we lose the rest by observing that the field $\mathbb{Q}(\zeta_{p^\infty})$ is the fixed field of $\mathbb{Z}_p^\times$. In particular, η is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}/H_\infty)$. Let N_∞ be the splitting field of the lattice E over the field H_∞, i.e., N_∞ is the field extension of H_∞ for which the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/N_\infty)$ on E is trivial. Let $G = \mathrm{Gal}(N_\infty/H_\infty)$ and note that η is trivial on G and so G acts trivially on E_η. We have the following diagram of fields.



where $\Gamma' \cong \Gamma \cong \mathbb{Z}_p$ and we set $\Delta' = \mathrm{Gal}(\mathbb{Q}^\chi(\zeta_{p^\infty})/\mathbb{Q})$.

Observe that we have a map

$$\phi : G \longrightarrow \mathrm{Hom}_{\mathbb{T}_{\mathfrak{P}}/I}(E_\eta, E_1)$$

given by $\phi(\sigma)(e_\eta) = \sigma e - e$ where $e \in E$ is any lift of $e_\eta \in E_\eta$. Using that G acts trivially on E_η, one shows this is well-defined and an injective homomorphism. Recall that $E_\eta \cong \mathbb{T}_{\mathfrak{P}}/I$ and so we get an injection of G into $E_1 \cong \mathrm{Hom}_{\mathbb{T}_{\mathfrak{P}}/I}(\mathbb{T}_{\mathfrak{P}}/I, E_1)$. This shows that G is abelian.

The group $\mathrm{Gal}(H_\infty/\mathbb{Q})$ acts on G by conjugation and acts on $\mathrm{Hom}_{\mathbb{T}_{\mathfrak{P}}/I}(E_\eta, E_1)$ via η^{-1}. To see the action on $\mathrm{Hom}_{\mathbb{T}_{\mathfrak{P}}/I}(E_\eta, E_1)$, observe that for $h \in \mathrm{Gal}(H_\infty/\mathbb{Q})$, $f \in \mathrm{Hom}_{\mathbb{T}_{\mathfrak{P}}/I}(E_\eta, E_1)$, and $e_\eta \in E_\eta$ we have

$$\begin{aligned} h \cdot f(e_\eta) &= hf(h^{-1}e_\eta) \\ &= f(h^{-1}e_\eta) \qquad (f(h^{-1}e_\eta) \in E_1) \\ &= f(\eta(h)^{-1}e_\eta) \qquad (e_\eta \in E_\eta) \\ &= \eta(h)^{-1}f(e_\eta). \end{aligned}$$

Lemma 5.43. *The map ϕ is $\mathrm{Gal}(H_\infty/\mathbb{Q})$-equivariant, i.e., $\phi(h \cdot g)(e_\eta) = \eta(h)^{-1}\phi(g)(e_\eta)$ for all $h \in \mathrm{Gal}(H_\infty/\mathbb{Q})$, $g \in G$, and $e_\eta \in E_\eta$.*

Proof. This is essentially just a long string of equalities:

$$\begin{aligned} \phi(h \cdot g)(e_\eta) &= \phi(hgh^{-1})(e_\eta) \\ &= hgh^{-1}e - e \qquad (e \in E \text{ any lift of } e_\eta) \\ &= hg(\eta(h^{-1})e + e') - e \qquad (\text{for some } e' \in E_1) \\ &= (\eta(h^{-1})h)ge + e' - e \qquad (\text{since } e' \in E_1) \\ &= (\eta(h^{-1})h)(e + e_1) + e' - e \qquad (\text{for some } e_1 \in E_1) \\ &= \eta(h^{-1})he + \eta(h^{-1})e_1 + e' - e \\ &= \eta(h^{-1})\eta(h)e + \eta(h^{-1})e'' + \eta(h^{-1})e_1 + e' - e \qquad (\text{ for some } e'' \in E_1) \\ &= (e + \eta(h^{-1})e'' + e') + \eta(h^{-1})e_1 - e \\ &= h(h^{-1}e) + \eta(h^{-1})e_1 - e \\ &= \eta(h)^{-1}e_1 \\ &= \eta(h)^{-1}(ge - e) \\ &= \eta(h)^{-1}\phi(g)(e). \end{aligned}$$

□

Lemma 5.44. *The extension N_∞/H_∞ is unramified.*

Proof. We begin by noting that N_∞/H_∞ is unramified at all $\ell \nmid Np$ as all the $\rho_{\mathcal{F}_i}$ are unramified at such ℓ and these Galois representations give the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus, it remains to consider the cases $\ell = p$ and $\ell \mid N$.

Let ℓ be a prime so that $\ell \mid N$. Let L_∞ be the maximal unramified abelian p-extension of H_∞, L_∞^N be the maximal abelian p-extension of H_∞ unramified outside of N, and L_∞^ℓ the maximal subextension of L_∞^N which is unramified over H_∞ at ℓ. Let $H_{n,\lambda}$ be the completion of H_n at a prime $\lambda \subset H_n$ dividing ℓ. Using the identification of the inertia at λ with $\mathcal{O}_{H_{n,\lambda}}^\times$ provided by class field theory, we have that $\mathrm{Gal}(L_\infty^N/L_\infty^\ell)$ is isomorphic to a quotient of

$$\varprojlim_n \prod_{\lambda \mid \ell} \mathcal{O}_{H_{n,\lambda}}^\times .$$

We now use that L_∞^N/L_∞^ℓ is a p-extension and $\ell \neq p$ to conclude that in fact we must have that $\mathrm{Gal}(L_\infty^N/L_\infty^\ell)$ is isomorphic to a quotient of

$$k = \varprojlim_n \prod_{\lambda|\ell} k_{n,\lambda}^\times$$

where $k_{n,\lambda}$ is the residue field of $H_{n,\lambda}$. The inertia group I_ℓ acts trivially on k by the definition of inertia and so

$$(\mathrm{Gal}(L_\infty^N/L_\infty^\ell) \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p)^\chi = 0$$

as we assumed χ has conductor divisible by N and so $\chi(I_\ell) \neq 0$. This in turn implies that

$$(\mathrm{Gal}(L_\infty^N/H_\infty) \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p)^\chi \xrightarrow{\simeq} (\mathrm{Gal}(L_\infty^\ell/H_\infty) \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p)^\chi$$

which gives the unramified condition for $\ell \mid N$. Since ℓ was an arbitrary prime dividing N, we have the result for all primes dividing N.

Consider the case where $\ell = p$. Let $N_{\infty,p}$ be the completion of N_∞ at a prime above p and likewise for $H_{\infty,p}$. We have the following sequences of Galois groups:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(N_\infty/H_\infty) \arrow[r] & \mathrm{Gal}(N_\infty/\mathbb{Q}) \arrow[r] & \mathrm{Gal}(H_\infty/\mathbb{Q}) \arrow[r] & 1 \\
1 \arrow[r] & \mathrm{Gal}(N_{\infty,p}/H_{\infty,p}) \arrow[r] \arrow[u, dash, "\cup"] & \mathrm{Gal}(N_{\infty,p}/\mathbb{Q}_p) \arrow[r] \arrow[u, dash, "\cup"] & \mathrm{Gal}(H_{\infty,p}/\mathbb{Q}_p) \arrow[r] \arrow[u, dash, "\cup"] & 1.
\end{tikzcd}$$

We have that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ actions on $\mathrm{Gal}(N_\infty/H_\infty)$ via conjugation as well as through $\mathrm{Gal}(H_\infty/\mathbb{Q})$. We also have a compatible action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $\mathrm{Gal}(N_{\infty,p}/H_{\infty,p})$ that factors through $\mathrm{Gal}(H_{\infty,p}/\mathbb{Q}_p)$. We will compute this action in two different ways to show that we cannot have ramification at p. We have already seen that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\mathrm{Gal}(N_\infty/H_\infty)$ via η^{-1}. We can also compute the local action on $\mathrm{Gal}(N_{\infty,p}/H_{\infty,p})$ by using our information about the restrictions of $\rho_{\mathcal{F}_i}$ restricted to the decomposition group D_p. Recall that since we are working with ordinary forms we have up to equivalence that

$$\rho_{\mathcal{F}_i} |_{D_p} \simeq \begin{pmatrix} \varepsilon_1 & * \\ 0 & \varepsilon_2 \end{pmatrix}$$

where ε_2 is unramified at p and $\varepsilon_2(\mathrm{Frob}_p) = c_p(\mathcal{F}_i)$ (see Theorem 5.32.) Thus, as a D_p-module we must have that E has a filtration as in Proposition 5.42 only with submodule of type-η and quotient of type-1. Thus, we must have that $\sigma x = \eta(\sigma)x$ for $x \in \mathrm{Gal}(N_{\infty,p}/H_{\infty,p})$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. We also know that the inertia group of $\mathrm{Gal}(H_{\infty,p}/\mathbb{Q}_p)$ has finite index in $\mathrm{Gal}(H_\infty, \mathbb{Q})$ (this is true for all number fields, not just $\mathbb{Q}$.) In particular, the inertia group contains $\gamma_0^{p^i}$

for some i. Thus we have two actions for $\gamma_0^{p^i}$ and combining them gives that $\gamma_0^{2p^i}$ must act trivially on $\mathrm{Gal}(N_{\infty,p}/H_{\infty,p})$. This gives that $\mathrm{Gal}(N_{\infty,p}/H_{\infty,p})$ is a torsion $\Lambda_{\mathcal{O}}$-module. Thus, the only zeroes which could possibly be ramified at p are of the form $\zeta - 1$ for ζ some p-power root of unity. But we have already excluded such exceptional zeroes, so we must have that the extension is unramified at p as desired. □

Observe that we have a surjective homomorphism

$$\mathbb{Z}_p[\![\mathrm{Gal}(H_\infty/\mathbb{Q})]\!] \twoheadrightarrow \mathbb{Z}_p[\chi][\![T]\!]$$

via $\sigma \mapsto \eta(\sigma)^{-1}$. This gives that $\phi(G)$ is stable under multiplication by $\mathbb{Z}_p[\chi][\![T]\!]$, i.e., $\phi(G)$ is a $\mathbb{Z}_p[\chi][\![T]\!]$-module. Let M be the $\mathcal{O}$-span of $\phi(G)$. Note this is equivalent to the $\Lambda_{\mathcal{O}}$-span, as well as the $\mathbb{T}_{\mathfrak{P}}$-span. We have that $M_\wp$ is a $\Lambda_{\mathcal{O},\wp}$-module ($M_{\mathfrak{P}}$ is a $\mathbb{T}_{\mathfrak{P}}$-module.) Then $M \subseteq \mathrm{Hom}_{\mathbb{T}_{\mathfrak{P}}/I}(E_\eta, E_1)$ and $M_\wp = M_{\mathfrak{P}}$. In fact, one has that

$$M_\wp = \mathrm{Hom}_{\mathbb{T}_{\mathfrak{P}}/I}(E_\eta, E_1).$$

Suppose not. Then there exists a submodule $E_1' \subsetneq E_1$ so that

$$\phi(G) \subset \mathrm{Hom}_{\mathbb{T}_{\mathfrak{P}}/I}(E_\eta, E_1').$$

We have that the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & E_1/E_1' \arrow[r] & E/E_1' \arrow[r] & E_\eta \arrow[r] & 0 \end{tikzcd}$$

splits over H_∞. Using that $\mathrm{Gal}(H_\infty/\mathbb{Q})$ is abelian, we can write E/E_1' as

$$E/E_1' = \ker(\mathrm{Frob}_\ell - 1) \oplus \ker(\mathrm{Frob}_\ell - \eta(\ell))$$

for any ℓ with $\eta(\ell) \not\equiv 1 (\mathrm{mod}\, \wp)$. This is in fact a splitting of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules and so gives that E has a type-1 quotient, a contradiction. Thus we obtain that $M_\wp \cong E_1$ as a $\mathbb{T}_{\mathfrak{P}}$-module. Looking back at how E, and hence E_1 was constructed, we see that we can write

$$M_\wp \cong \bigoplus_{i=1}^{m} \Lambda_{\mathcal{O},\wp}/\wp^{r_i}$$

for some positive integers m and r_i.

Our goal is to determine $\sum r_i$ in terms of $\mathrm{ord}_\wp(\hat{G}_\psi(T))$. To do this we need to use Fitting ideals, which we now briefly review. For a more substantial treatment of Fitting ideals one should consult [MW] or [Northcott]. Let R be a commutative ring and M a finitely generated R-module. There exists $r \in \mathbb{Z}$, $N \subset R^r$ so that we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\vartheta"] & R^r \arrow[r, "\varrho"] & M \arrow[r] & 0. \end{tikzcd}$$

Definition 5.45. The *Fitting ideal* $\mathrm{Fitt}_R(M)$ is the ideal in R generated by the elements $\det(\Theta)$ for all Θ where Θ is an $r \times r$ matrix of the form

$$\Theta = \begin{pmatrix} \vartheta(x_1) \\ \vdots \\ \vartheta(x_r) \end{pmatrix}$$

where $(x_1, \ldots, x_r)$ runs through all r-tuples of elements in N.

One can show that $\mathrm{Fitt}_R(M)$ is independent of r and ϱ so depends only on the module M. We now state the relevant facts about Fitting ideals.

1. If $M = R/\mathfrak{a}$, where $\mathfrak{a}$ is an ideal of R, then $\mathrm{Fitt}_R(M) = \mathfrak{a}$.

2. If $\mathfrak{a}$ is an ideal of R, then $\mathrm{Fitt}_{R/\mathfrak{a}}(M/\mathfrak{a}M) = \mathrm{Fitt}_R(M)(\mathrm{mod}\,\mathfrak{a})$.

3. If $M \cong M_1 \times M_2$, then $\mathrm{Fitt}_R(M) = \mathrm{Fitt}_R(M_1)\,\mathrm{Fitt}_R(M_2)$.

4. If $\mathfrak{a}$ is a finitely generated ideal of R and M is a faithful R-module, then $\mathrm{Fitt}_R(M/\mathfrak{a}M) \subset \mathfrak{a}$.

Lemma 5.46. *With the set-up as above, we have $\sum r_i \geq \mathrm{ord}_{\wp}(\hat{G}_{\psi}(T))$.*

Proof. Observe that the above properties give us $\mathrm{Fitt}_{\Lambda_{\mathcal{O},\wp}}(M_{\wp}) = \wp^{\sum r_i}$. Thus, if we can show that $\mathrm{Fitt}_{\Lambda_{\mathcal{O},\wp}}(M_{\wp}) \subseteq (\hat{G}_{\psi}(T))$ we will be done. Write $\mathscr{L} = \mathscr{L}^{(1)} \oplus \mathscr{L}^{(\eta)}$ as in the proof of Proposition 5.42. The submodule $\mathscr{L}^{(1)}$ of $\mathscr{L}$ is a faithful$\mathbb{T}_{\mathfrak{P}}$-module and so $\mathrm{Fitt}_{\mathbb{T}_{\mathfrak{P}}}(\mathscr{L}^{(1)}) = 0$ using property 4 above with $\mathfrak{a} = 0$. Applying property 2 we obtain $\mathrm{Fitt}_{\mathbb{T}_{\mathfrak{P}}/I}(\mathscr{L}^{(1)}/I) = 0(\mathrm{mod}\, I)$. We now need to translate this into a statement about $M_{\wp}$. Recall that $\mathbb{T}_{\mathfrak{P}}/I \cong \Lambda_{\mathcal{O},\wp}/(\hat{G}_{\psi}(T))$ as $\Lambda_{\mathcal{O},\wp}$-algebras, $E_1 \cong \mathscr{L}^{(1)}/I$ as a $\mathbb{T}_{\mathfrak{P}}/I$-module, and that $M_{\wp} \cong E_1$ as a $\mathbb{T}_{\mathfrak{P}}/I$-module. Using these isomorphisms, we obtain that

$$\mathrm{Fitt}_{\Lambda_{\mathcal{O},\wp}/(\hat{G}_{\psi}(T))}(\mathscr{L}^{(1)}/(\hat{G}_{\psi}(T))) = 0(\mathrm{mod}\,\hat{G}_{\psi}(T))$$

and

$$\begin{aligned} \mathrm{Fitt}_{\Lambda_{\mathcal{O},\wp}/(\hat{G}_{\psi}(T))}(\mathscr{L}^{(1)}/(\hat{G}_{\psi}(T))) &\cong \mathrm{Fitt}_{\Lambda_{\mathcal{O},\wp}/(\hat{G}_{\psi}(T))}(E_1) \\ &\cong \mathrm{Fitt}_{\Lambda_{\mathcal{O},\wp}/(\hat{G}_{\psi}(T))}(M_{\wp}). \end{aligned}$$

Thus, we have that $\mathrm{Fitt}_{\Lambda_{\mathcal{O},\wp}/(\hat{G}_{\psi}(T))}(M_{\wp}) \subseteq (\hat{G}_{\psi}(T))$. Using that $\mathrm{Fitt}_{\Lambda_{\mathcal{O},\wp}}(M_{\wp}) = \mathrm{Fitt}_{\Lambda_{\mathcal{O},\wp}/(\hat{G}_{\psi}(T))}(M_{\wp})$, we have the result. (Note that this follows from the defintion of the Fitting ideal along with the fact that $(\hat{G}_{\psi}(T)) \subseteq \wp$.) □

Observe that there is an isomorphism $\mathcal{O}[\![x]\!] \cong \Lambda_{\mathcal{O}}$ given by $1+x \mapsto (1+p)^{-1}(1+T)^{-1}$. This allows us to rephrase the lemma as follows.

Corollary 5.47. *With the set-up as above, we have $\sum r_i \geq \operatorname{ord}_{\wp'}(g_{\chi^{-1}\omega}(x))$ where $\wp' \subset \mathcal{O}[\![x]\!]$ is the prime corresponding to $\wp$ under the isomorphism $\mathcal{O}[\![x]\!] \cong \Lambda_{\mathcal{O}}$.*

Proof. To see this, just change variables in the lemma using the given isomorphism and that we assumed $p \notin \wp$ to transfer to a statement about $g_{\chi^{-1}\omega}(x)$. □

We now have a relation between the order of a zero of $g_{\chi^{-1}\omega}$ and the size of M, which in turn measures the size of $G = \operatorname{Gal}(N_\infty/H_\infty)$. One should think of this as saying the order of the zero of $g_{\chi^{-1}\omega}$ gives a lower bound on the size of the extension N_∞/H_∞. The goal is to connect this information back to arithmetic information.

Lemma 5.48. *The group $\operatorname{Gal}(N_\infty/\mathbb{Q}_\infty^\chi)$ is abelian.*

Proof. Observe that $\Delta' \cong \operatorname{Gal}(H_\infty/\mathbb{Q}_\infty)$ acts on G via η^{-1}, which restricts to χ on Δ'. We already know that $\operatorname{Gal}(H_\infty/\mathbb{Q}_\infty^\chi)$ and G are abelian, so it only remains to show that for $\sigma \in \operatorname{Gal}(H_\infty/\mathbb{Q}_\infty^\chi)$ and $g \in G$, we have $\sigma g \sigma^{-1} = g$. However, we know that $\sigma \cdot g = \sigma g \sigma^{-1}$ and this is $\chi(\sigma) g$ since Δ' acts via χ. However, χ restricted to $\operatorname{Gal}(H_\infty/\mathbb{Q}_\infty^\chi)$ is trivial, so we obtain the desired result. □

Exercise 5.49. *Prove there exists an extension $N'_\infty/\mathbb{Q}_\infty^\chi$ so that $G \cong \operatorname{Gal}(N'_\infty/\mathbb{Q}_\infty^\chi)$. (Hint: Use class field theory that the fact that $\operatorname{Gal}(N_\infty/\mathbb{Q}_\infty^\chi)$ is abelian and that G is a subgroup of $\operatorname{Gal}(N_\infty/\mathbb{Q}_\infty^\chi)$.) In particular, $\operatorname{Gal}(N'_\infty/\mathbb{Q}_\infty^\chi)$ is an unramified abelian p-extension on which Δ acts by χ.*

We can now apply the fact that χ is odd to conclude that we have a surjection of Γ-modules

$$X^- \twoheadrightarrow \operatorname{Gal}(N_\infty^-/\mathbb{Q}_\infty^\chi) \cong G.$$

Thus, we have a surjection of $\mathcal{O}[\![x]\!]$-modules

$$X^- \otimes_{\mathbb{Z}_p[\Delta]} \mathcal{O} \twoheadrightarrow G \otimes_{\mathbb{Z}_p[\Delta]} \mathcal{O} = G \otimes_{\mathbb{Z}_p[\Delta']} \mathcal{O} \twoheadrightarrow M.$$

Let f_χ be the characteristic polynomial of $X^- \otimes_{\mathbb{Z}_p[\Delta]} \mathcal{O}$ as a $\mathcal{O}[\![x]\!]$-module and f_M the characteristic polynomial of M as an $\mathcal{O}[\![x]\!]$-module. The above surjection implies that $f_M \mid f_\chi$. Write $f_M = \prod_j f_j$ where f_j are distinguished polynomials as before. Observe that we have

$$\begin{aligned} \bigoplus_j \mathcal{O}[\![x]\!]_{\wp'}/(f_j(x)) &= M_{\wp'} \\ &\cong M_\wp \\ &\cong \bigoplus_j \mathcal{O}[\![x]\!]_{\wp'}/\wp'^{\operatorname{ord}_{\wp'}(f_j)} \\ &\cong \bigoplus_j \mathcal{O}[\![x]\!]_{\wp'}/\wp'^{r_j}. \end{aligned}$$

Thus, we have that

$$\begin{aligned}\mathrm{ord}_{\wp'}(f_\chi) &\geq \mathrm{ord}_{\wp'}(f_M)\\ &= \sum_j r_j\\ &\geq \mathrm{ord}_{\wp'}(g_{\chi^{-1}\omega}(x)).\end{aligned}$$

This completes the proof of the main conjecture in the case of $F = \mathbb{Q}$ using that we know $\mu_\chi = \mu_\chi^{\mathrm{an}} = 0$ in this case. In the case of general totally real number fields, one must make further arguments to deal with the μ-invariants, a topic we do not address here.

Bibliography

[AM] M.F. Atiyah and I.G. MacDonald, *Introduction to Commutative Algebra*, Perseus Books, Cambridge, Mass. (1969).

[CF] J.W.S. Cassels and A. Frohlich, *Algebraic Number Theory*, Academic Press Inc., Washington, D.C. 1967.

[DR] P. Deligne and K. Ribet, *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. 59, 227-286 (1980).

[DS] P. Deligne and J-P Serre, *Formes modulaires de poids 1*, Ann. Scient. Ec. Norm. Sup., 4^{e} serie 7, 507-530 (1974).

[DI] F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem, CMS Conference Proceedings Volume 17, 39-134 (1995).

[DS] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics 228, Springer-Verlag (2000).

[Hida1] H. Hida, *On congruence divisors of cusp forms as factors of the special values of their zeta functions*, Invent. Math. 64, 221-262 (1981).

[Iwas1] K. Iwasawa, *On the μ-invariants of $\mathbb{Z}_\ell$-extensions*, Number theory, Algebraic Geometry, and Commutative Algebra (in honor of Y. Akizuki), Kinokuniya: Tokyo, 1-11 (1973).

[Jan] G. Janusz, *Algebraic Number Fields*, Graduate Studies in Mathematics Vol. 7, AMS (1996).

[Kob] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Graduate Texts in Mathematics 97, Springer-Verlag (1991).

[Lang1] S. Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics 110, Springer-Verlag (1986).

[Lang2] S. Lang, *Cyclotomic Fields I and II*, Graduate Texts in Mathematics 121, Springer-Verlag (1990).

[Mats] H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics 8, (1994).

[Mazur] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Etudes Sci. Publ. Math. 47, 33-186 (1977).

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. 76, 179-330 (1984).

[Milne1] J.S. Milne, *Algebraic Number Theory*, http://www.jmilne.org.

[Milne2] J.S. Milne, *Class Field Theory*, http://www.jmilne.org.

[Milne3] J.S. Milne, *Modular Functions and Modular Forms*, http://www.jmilne.org.

[Miyake] T. Miyake, *Modular Forms*, Spinger-Verlag (1989).

[Northcott] D.G. Northcott, *Finite Free Resolutions*, Cambrdige Univ. Press, Cambridge-New York 1976.

[Skinner] C. Skinner, *Iwasawa theory course notes*, University of Michigan, winter semester (2002).

[Ribet] K. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Invent. Math. 34, 151-162 (1976).

[Rubin] K. Rubin, *Euler Systems*, Hermann Weyl Lectures, The Institute for Advanced Study, Annals of Mathematics Studies 147, Princeton University Press (2000).

[Wash] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics 83, Second Edition, Springer (1991).

[Wiles1] A. Wiles, *On ordinary* λ*-adic representations associated to modular forms*, Invent. Math. 94, 529-573 (1988).

[Wiles2] A. Wiles, *The Iwasawa conjecture for totally real fields*, Annals of Math. (2) 131 no. 3, 493-540 (1990).