Title

A map in Sharifi's conjecture for general non-exceptional characters and tame level

Author
Vu, Frederick

Publication Date
2023

UNIVERSITY OF CALIFORNIA

Los Angeles

A map in Sharifi's conjecture for general non-exceptional characters and tame level

A dissertation submitted in partial satisfaction

of the requirements for the degree

Doctor of Philosophy in Mathematics

by

Frederick Vu

2023

ABSTRACT OF THE DISSERTATION

A map in Sharifi's conjecture for general non-exceptional characters and tame level

by

Frederick Vu
Doctor of Philosophy in Mathematics
University of California, Los Angeles, 2023
Professor Romyar Thomas Sharifi, Chair

This dissertation details the construction of the map Υ of Sharifi's conjecture for a general tame level N and odd prime p satisfying $Np > 3$ and for general non-exceptional characters θ of $(\mathbb{Z}/Np\mathbb{Z})^{\times}$. We then show that, conditioned upon a certain Zariski density result of Hida, the constructed map Υ is in fact surjective and is an isomorphism modulo p-torsion.

The dissertation of Frederick Vu is approved.

Haruzo Hida

Chandrashekhar Khare

Don Blasius

Romyar Thomas Sharifi, Committee Chair

University of California, Los Angeles

2023

To my sister, Jacqueline

TABLE OF CONTENTS

1 Introduction 1

1.1 Overview 5

2 Iwasawa theory 7

2.1 Iwasawa algebras 7

2.2 Iwasawa modules 9

2.2.1 The Iwasawa main conjecture 16

2.3 Iwasawa Cohomology 19

2.4 Iwasawa theory of imaginary quadratic fields 26

2.4.1 Ring class fields and the anticyclotomic $\mathbb{Z}_l$-extension 26

2.4.2 The $\mathfrak{p}$-ramified main conjecture for K 31

3 Modular curves and modular and Λ-adic forms 37

3.1 Modular curves 37

3.1.1 Moduli problems 38

3.1.2 Ihara's model of $X(M)_{\mathbb{F}_{q^2}}$ 46

3.1.3 Degeneracy morphisms 48

3.2 Algebraic theory of Hecke algebras and modular forms 49

3.2.1 Sheaves of differentials and modular forms 50

3.2.2 Cusps and algebraic q-expansions 55

3.2.3 Hecke operators 62

3.2.4 Hecke algebras 70

3.3 Λ-adic forms . . . 75

3.3.1 p-adic L-functions, $\tilde{\Lambda}$-adic Eisenstein series, and the Eisenstein ideal . 82

4 Cohomology of modular curves . . . 90

4.1 Eichler-Shimura cohomology groups . . . 90

4.1.1 The case $p = 3$ for $\tilde{\Lambda}$-adic Eichler-Shimura . . . 93

4.1.2 The $\tilde{\Lambda}$-adic pairing . . . 99

4.1.3 Homology of modular curves and the Drinfeld-Manin splitting . . . 106

4.1.4 The map $(\xi_{\theta_{(0)}} s(c_\theta), -)_{\Lambda_{\mathcal{O}}}$ . . . 107

4.2 Υ . . . 119

4.3 Surjectivity of Υ . . . 127

4.3.1 Modular Jacobians . . . 129

4.3.2 Surjection of CM points . . . 135

4.3.3 Anticyclotomic analog of Washington's theorem . . . 137

References . . . 144

ACKNOWLEDGEMENTS

First and foremost, I express my sincerest gratitude for the guidance and support of my advisor, Romyar Sharifi, throughout my PhD experience.

For our mathematical conversations over the years, I thank Tim Smits, Alex Frederick, Jacob Swenberg, Jas Singh, Rohan Joshi, Tobias Shin, Griffin Pinney, and too many others to name. For distracting me as I worked on my thesis, I would like to thank Ben Major and Robert Miranda, who replaced my previous officemates, Josh Kazdan and Bertrand Stone, whose friendships I deeply appreciate. For making my apartment into a home, I thank my roommates over the years, in particular, Mirian Krystel de Siqueira, Grant Brown, and, I suppose, Griffin Pinney again.

Finally, I must express my gratitude to my family for their love and support. Though I am saddened that I cannot acknowledge everyone who deserves to be named here, I would like to thank all of the individuals I have met along the way, whose influences, no matter how small, have left an indelible mark on my life.

VITA

2016	B.S. in Mathematics, University of Chicago

CHAPTER 1

Introduction

Given the data of an odd prime p, a positive integer N prime to p, and a character θ of $(\mathbb{Z}/Np\mathbb{Z})^\times$, subject to some conditions, the map Υ of Sharifi's conjecture is a morphism of Iwasawa modules from a component of the unramified Iwasawa module X_∞ of the cyclotomic field $\mathbb{Q}(\mu_{Np})$ to the quotient $\mathcal{T}/I_\theta$ of an inverse limit $\mathcal{T}$ of étale cohomology groups of modular curves $X_1(Np^r)$ by the action of the Eisenstein ideal I_θ. The morphism is induced by the restriction of a cocycle appearing in the representation of the absolute Galois group $G_\mathbb{Q}$ on $\mathcal{T}/I_\theta$. A similar cocycle was considered already by M. Ohta in [Oh99, Oh00, Oh03], where he adapted a method of constructing unramified abelian extensions of number fields due to Kurihara in [Ku93] and Harder-Pink in [HP92] to an Iwasawa-theoretic setting in order to give a simpler proof of the main conjecture of Iwasawa theory for the cyclotomic $\mathbb{Z}_p$ extension of (a finite abelian extension of) $\mathbb{Q}$. The thread of ideas going into Ohta's proof, and Sharifi's conjecture, passes through many seminal papers in the field of Iwasawa theory. The main conjecture was proved originally by Mazur-Wiles in [MW84], and its proof was greatly simplified and generalized by Wiles in [Wi90] using the language of Hida theory, then recently developed in [Hi86a, Hi86b]. In both of these works, the main conjecture was proved by demonstrating the existence of appropriate abelian unramified extensions via a study of Galois representations arising from the geometry of modular curves and the arithmetic of modular forms, a method whose key ideas arose from Ribet's insight in [Ri76] and Mazur's influential work on modular curves and the Eisenstein ideal in [Ma77]. Sharifi's conjecture can be seen as a refinement of the Iwasawa main conjecture, which is only concerned with the structure of X_∞ up to pseudo-isomorphism, and in fact only its characteristic ideal (and which has no obvious ties to the geometry of modular curves). Let us introduce some temporary notation in order to speak more precisely about Sharifi's conjecture.

Let F be an abelian number field and S a set of places of F containing those dividing p and any real places. Let $H^i_{\mathrm{Iw},S}(F_\infty/F, \mathbb{Z}_p(i))$ denote the i-th S-ramified Iwasawa cohomology group of the cyclotomic $\mathbb{Z}_p$-extension F_∞/F with coefficients in $\mathbb{Z}_p(i)$. When $i = 1$, we have a canonical identification of this group with the group of norm-compatible systems of S-units of the intermediate fields F_r of F_∞/F, and the cup product in Galois cohomology gives us a map to the Iwasawa cohomology group with $i = 2$. With $F = \mathbb{Q}(\mu_{Np})$ and $S = S_{Np}$, the set of places containing those dividing Np and any real places, Sharifi constructed a map relating the geometry of modular curves to the arithmetic of cyclotomic fields

$$\varpi : H^+ := \varprojlim_r H_1(X_1(Np^r)^{\mathrm{an}}, C_r; \mathbb{Z}_p)^+ \to H^2_{\mathrm{Iw},S_{Np}}(F_\infty/F, \mathbb{Z}_p(2)),$$

defined on the complex-conjugation-fixed part of the inverse limit of singular cohomology groups of the complex analytic curves $X_1(Np^r)^{\mathrm{an}}$ relative to their cusps and which sends a compatible system of Manin symbols, which are roughly homology classes of geodesics between cusps, to a compatible system of cup products of cyclotomic units. This map needs no reference to θ-eigenspaces with respect to the action of $\mathrm{Gal}(F/\mathbb{Q})$ and needs no conditions on N and p in order to be defined, aside from $p > 2$. We are concerned with a map Υ defined in the direction opposite to that of ϖ, but not quite between the two objects given above. The map ϖ was conjectured by Sharifi and shown by Fukaya and Kato in [FK12] to factor through the quotient by the (equivariant) Eisenstein ideal I of the universal p-ordinary cuspidal adjoint Hecke algebra $\mathfrak{h}^*$ of Hida by showing that ϖ arises as the composite of a map which sends a system of Manin symbols to a system of cup products of Siegel units in the second étale cohomology groups of modular curves with the specialization map at the ∞ cusp which takes these cohomology groups to the second Iwasawa cohomology group above. Additionally, Fukaya and Kato showed that the restriction of ϖ to the inverse limit of $H^1_{\text{ét}}(X_1(Np^r)^{\mathrm{an}}; \mathbb{Z}_p)^+$ has image contained in the S_p-ramified Iwasawa cohomology group $H^2_{\mathrm{Iw},S_p}(F_\infty/F, \mathbb{Z}_p(2)) \subset H^2_{\mathrm{Iw},S_{Np}}(F_\infty/F, \mathbb{Z}_p(2))$.

Consider the unramified Iwasawa module X_∞ of F_∞, i.e., the Galois group of the maximal abelian pro-p everywhere unramified extension H_∞ of F_∞, which naturally carries the conjugation action of $\tilde{\Gamma} := \mathrm{Gal}(F_\infty/\mathbb{Q})$ and makes X_∞ into a (continuous) $\tilde{\Lambda} := \mathbb{Z}_p[[\tilde{\Gamma}]]$-module. There is a natural map from $X_\infty(1)$ to $H^2_{\mathrm{Iw},S}(F_\infty/F, \mathbb{Z}_p(2))$ which factors through the Tate twist of the S-split Iwasawa module Y_S of F_∞, the quotient of X_∞ corresponding to the maximal subextension of M_∞/F_∞ in which all places of F_∞ lying above those in S split completely. This map is neither injective nor surjective in general, but for certain p-adic characters χ of the torsion subgroup Δ of the abelian group $\tilde{\Gamma} \cong \Delta \times \Gamma$, we have an isomorphism between the χ-quotients $X_\infty(1)_\chi$ and $H^2_{\mathrm{Iw},S_p}(F_\infty/F, \mathbb{Z}_p(2))_\chi$. When $F = \mathbb{Q}(\mu_{Np})$ so that $\Delta \cong (\mathbb{Z}/Np\mathbb{Z})^\times$, these isomorphisms are had for χ such that $\chi\omega^{-1}$ is nontrivial on the subgroup $(\mathbb{Z}/p\mathbb{Z})^\times \times \langle p \rangle$, where $\langle p \rangle \subset (\mathbb{Z}/N\mathbb{Z})^\times$ is the subgroup generated by p and ω is the Teichmüller character. For such χ, we call χ^{-1} non-exceptional.

Consider next Ohta's p-ordinary Eichler-Shimura cohomology group

$$\mathcal{T} = \varprojlim_r H^1_{\text{ét}}(X_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))^{\mathrm{ord}}$$

which sits in a short exact sequence of $\mathfrak{h}^*[G_{\mathbb{Q}_p}]$-modules

$$0 \to \mathcal{T}_{\mathrm{sub}} \to \mathcal{T} \to \mathcal{T}_{\mathrm{quo}} \to 0,$$

where $\mathcal{T}_{\mathrm{quo}}$ is defined to be the maximal unramified quotient of $\mathcal{T}$. For $p \geq 5$, it was shown by Ohta in [Oh95] that $\mathcal{T}_{\mathrm{sub}}$ is isomorphic to $\mathfrak{h}^*$ and $\mathcal{T}_{\mathrm{quo}}$ is isomorphic to $\mathrm{Hom}_{\tilde{\Lambda}}(\mathfrak{h}^*, \tilde{\Lambda})$, where $\tilde{\Lambda}$ is viewed as the subalgebra of adjoint diamond operators of $\mathfrak{h}^*$. It was also shown by Ohta in [Oh99, Oh00] when $p \nmid \varphi(N)$, where φ denotes Euler's totient function, and for $\theta \neq \omega^{-2}$ a primitive, non-exceptional, even character of $(\mathbb{Z}/Np\mathbb{Z})^\times$ that this sequence splits after localization at the maximal ideal of the Hecke algebra associated with the Eisenstein series associated with θ, and that modulo the corresponding Eisenstein ideal I_θ, one obtains a Galois representation

$$G_{\mathbb{Q}} \ni \sigma \mapsto \begin{pmatrix} 1 & \bar{b}(\sigma) \\ 0 & \bar{d}(\sigma) \end{pmatrix}$$

where one uses an ordered basis corresponding to $(\mathcal{T}_{\text{quo}}, \mathcal{T}_{\text{sub}})$. The cocycle $\bar{b}$ of $G_{\mathbb{Q}}$ restricts to a homomorphism on G_{F_∞} which, under certain technical conditions, factors through X_∞. Fukaya and Kato presented this representation as coming from a short exact sequence of $\mathfrak{h}^*/I_\theta[G_{\mathbb{Q}}]$-modules in the reverse direction, which is split as a sequence of $\mathfrak{h}^*[G_{\mathbb{Q}_p}]$-modules from Ohta's work,

$$0 \to \mathcal{T}_{\text{quo}}/I_\theta \to \mathcal{T}/I_\theta \to \mathcal{T}_{\text{sub}}/I_\theta \to 0.$$

The target of $\bar{b}$ can be canonically identified with H^+/I_θ, and one obtains the morphism of $\tilde{\Lambda}$-modules

$$\Upsilon = \Upsilon_\theta : X_\infty(1)_{\theta^{-1}} \cong H^2_{\text{Iw},S}(F_\infty/F, \mathbb{Z}_p(2))_{\theta^{-1}} \to H^+/I_\theta$$

which is conjecturally inverse to the θ-eigenspace of ϖ. In fact, it was shown recently in [Oh20] that, for certain θ, the map Υ is surjective via a study of multiplicative type subgroup schemes of the Jacobians of modular curves, following the strategy of Vatsal in [Va05]. The proof of this final result relies on an analog of Washington's result on the boundedness of the growth of p-parts of class groups up a cyclotomic $\mathbb{Z}_l$-extension in the setting of the anticyclotomic $\mathbb{Z}_l$-extension of an abelian extension L of an imaginary quadratic field K in which p splits as $\mathfrak{p}\bar{\mathfrak{p}}$, and the proof of this analog result relies on a non-vanishing mod p result of Hida on special values p-adic L-function associated with Hecke characters of K along with an affirmative answer to the $\mathfrak{p}$-ramified main conjectures of the fields along the anticyclotomic $\mathbb{Z}_l$-tower of an abelian extension of K.

In this dissertation, we seek to relax some of the conditions imposed by Sharifi and Ohta in the construction of the map Υ. Specifically, by using results in [La15b] of Lafferty and following the ideas of [FK12] and [Oh03], we define a map $\Upsilon = \Upsilon_\theta$ on the θ^{-1}-eigenspace of $H^2_{\text{Iw},S}(F_\infty/F, \mathbb{Z}_p(2))$ which is induced from a cocycle as in the above account which is conjecturally inverse to the θ-eigenspace of ϖ (modulo the Eisenstein ideal) allowing for θ to be imprimitive and for $p \mid \varphi(N)$, though with the latter condition we are often forced to invert p. We cannot hope to allow for arbitrary characters θ as for exceptional characters, we do not have an isomorphism between $X_{\infty,\theta^{-1}}$ and $H^2_{\text{Iw},S_p}(F_\infty/F, \mathbb{Z}_p(1))_{\theta^{-1}}$, and so the construction of Υ as the restriction of a cocycle in such a case cannot be inverse to the θ-eigenspace of ϖ. We additionally address the case $p = 3$, which was omitted by Ohta due to the lack of citable references of standard results in Hida theory at the time of writing of [Oh95, Oh99, Oh00], and explain how Ohta's proof that Υ is conditionally a surjection carries through to these new cases.

Theorem 1.0.1. *Let p be an odd prime, N be a positive integer prime to p such that $Np > 3$, and θ be an even Dirichlet character of modulus Np. Consider θ as a Galois character via the canonical isomorphism $\mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}) \cong (\mathbb{Z}/Np\mathbb{Z})^{\times}$. Let $\Delta_p \leqslant \mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q})$ be the decomposition subgroup at p and let $\Delta_p' \leq \Delta_p$ be the prime-to-p subgroup of Δ_p. Let $\zeta_{N\varphi(N)}$ be a primitive $N\varphi(N)$-th root of unity, and set $\mathcal{O} = \mathbb{Z}_p[\zeta_{N\varphi(N)}]$.*

If $\omega\theta$ is nontrivial on Δ_p', then there is a morphism of $\tilde{\Lambda}_{\mathcal{O}} = \mathcal{O}[[\mathrm{Gal}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q})]]$-modules

$$\Upsilon : X_\infty(1)_{\theta^{-1}} \otimes_{\mathbb{Z}_p} \mathcal{O} \to (\mathcal{T}_{\mathrm{quo},\mathcal{O}}/I_\theta)^\iota$$

where the $\tilde{\Lambda}_{\mathcal{O}}$-module structure on $(\mathcal{T}_{\mathrm{sub},\mathcal{O}}/I_\theta)^\iota$ is induced by the $\mathfrak{h}^*_{\mathcal{O}}$-module structure on $\mathcal{T}_{\mathrm{sub},\mathcal{O}}/I_\theta$ and the $\mathbb{Z}_p$-algebra map $\tilde{\Lambda}_{\mathcal{O}} \to \mathfrak{h}^*_{\mathcal{O}}$ which sends a group element $[\sigma]$ to the diamond operator $\langle \kappa_{Np}(\sigma)\rangle$, where κ_{Np} is the cyclotomic character valued in $\mathbb{Z}_{p,N}^{\times}$.

If $\omega\theta$ is nontrivial on Δ_p, then there is a morphism of $\tilde{\Lambda}_{\mathcal{O}}$-modules

$$\Upsilon : X_\infty(1)_{\theta^{-1}} \otimes_{\mathbb{Z}_p} \mathcal{O}[1/p] \to (\mathcal{T}_{\mathrm{quo},\mathcal{O}}/I_\theta)^\iota[1/p].$$

In either case, if in addition the restriction $\theta|_{(\mathbb{Z}/p\mathbb{Z})^\times}$ has nontrivial kernel and if the claims of [Hi04, Propositions 2.7, 2.8] are true as stated, then the map Υ is surjective. Conditioned upon this surjectivity, the map Υ is an isomorphism if $p \nmid \varphi(N)$ and is an isomorphism up to p-torsion in general.

1.1 Overview

In Chapter 2, we review the definitions of the unramified, S-split, and S-ramified Iwasawa modules associated with a $\mathbb{Z}_p$-extension of a number field and the definition of the anticyclotomic $\mathbb{Z}_l$-extension of an imaginary quadratic field K. We also define Iwasawa cohomology groups and relate these Iwasawa modules to certain Iwasawa cohomology groups. We additionally state the $\mathfrak{p}$-ramified main conjecture of an abelian extension of K for rational primes p which split as $\mathfrak{p}\overline{\mathfrak{p}}$ in K, to be used in the proof of the surjectivity of Υ in Chapter 4. In Chapter 3, we review the algebraic definitions of modular curves and classical modular forms and Hecke algebras and their Λ-adic variants. In Chapter 4, we recall the statement of Ohta's p-adic Eichler-Shimura isomorphism theorem. We then use the results of [La15b] and a twisted Λ-adic Poincaré duality pairing to construct a short exact sequence of $\mathfrak{h}^*[G_{\mathbb{Q}}]$-modules from which we obtain a cocycle on $G_{\mathbb{Q}}$ which we denote $\bar{b}$. We then study this cocycle in order to define Υ. Finally, we show that Υ is surjective following the argument of [Oh20].

CHAPTER 2

Iwasawa theory

In this chapter, we first establish standard notation to be used throughout the dissertation. We then define the classical unramified, S-split, and S-ramified Iwasawa modules, X_∞, Y_S, and $\mathfrak{X}_S$, associated to a $\mathbb{Z}_p$-extension F_∞/F of a number field F, review known results of their Iwasawa λ- and μ-invariants in certain cases, and relate them to Iwasawa cohomology groups. We additionally review the definition of the anticyclotomic $\mathbb{Z}_l$-extension of an imaginary quadratic field K and state the proven $\mathfrak{p}$-ramified main conjecture of an abelian extension of K for an odd prime p which splits as $\mathfrak{p}\overline{\mathfrak{p}}$ in K.

2.1 Iwasawa algebras

Let p be an odd prime. We fix choices of algebraic closures $\overline{\mathbb{Q}}_p/\mathbb{Q}_p$ and $\overline{\mathbb{Q}}/\mathbb{Q}$, embeddings of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and into $\mathbb{C}_p := \widehat{\overline{\mathbb{Q}}}_p$, and an isomorphism $\mathbb{C} \cong \mathbb{C}_p$ compatible with these embeddings. All algebraic extensions of $\mathbb{Q}$ and of $\mathbb{Q}_p$ considered will be contained in $\mathbb{C}_p$. For any field K, we set $G_K := \mathrm{Gal}(\bar{K}/K)$ and for an algebraic extension K of $\mathbb{Q}$ or $\mathbb{Q}_p$, we denote by $\mathcal{O}_K$ its ring of integers. For a general commutative ring R, we denote by $Q(R)$ its total ring of fractions which is defined as the localization of R at the multiplicative set of non-zero-divisors.

Let N be a positive integer prime to p. Set $\mathbb{Z}_{p,N} = \varprojlim_r \mathbb{Z}/Np^r\mathbb{Z}$. The unit group $\mathbb{Z}_{p,N}^\times$ canonically decomposes as a product

$$\mathbb{Z}_{p,N}^\times \cong (\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times \cong (\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p).$$

Define $\Delta := (\mathbb{Z}/Np\mathbb{Z})^\times$ and $U_r := 1 + p^r\mathbb{Z}_p$ for $1 \leq r$. Fix the topological generator

$\gamma := 1 + p \in U_1$ and define the logarithm homomorphism $i : U_1 \to \mathbb{Z}_p$ by $\gamma^{i(\alpha)} = \alpha$. We denote by Δ' the prime-to-p subgroup of Δ and by $\Delta^{(p)}$ the p-Sylow subgroup of Δ. For any $\mathbb{Z}_p$-algebra $\mathcal{O}$, we denote by $\tilde{\Lambda}_{\mathcal{O}}$ and $\Lambda_{\mathcal{O}}$ the completed group rings

$$\tilde{\Lambda}_{\mathcal{O}} = \mathcal{O}[[\mathbb{Z}_{p,N}^\times]] = \varprojlim_r \mathcal{O}[(\mathbb{Z}/Np^r\mathbb{Z})^\times],$$

$$\Lambda_{\mathcal{O}} = \mathcal{O}[[U_1]] = \varprojlim_r \mathcal{O}[U_1/U_r].$$

If $\mathcal{O} = \mathbb{Z}_p$, we often denote $\tilde{\Lambda}_{\mathbb{Z}_p}$ and $\Lambda_{\mathbb{Z}_p}$ simply by $\tilde{\Lambda}$ and Λ, respectively.

For a general group ring $R[G]$ and $g \in G$, we denote by $[g]$ the corresponding element of $R[G]$. We may identify Λ with the power series ring in one variable $\mathbb{Z}_p[[T]]$ via $[\gamma] \mapsto 1 + T$. Thus, Λ is a complete regular local ring of Krull dimension 2, and so in particular it is a UFD. For any group G, we denote by $\widehat{G}$ the group of finite order characters of G valued in $\mathbb{C}_p^\times$. We have that $\tilde{\Lambda}$ is a complete semi-local ring which decomposes as a direct product of reduced local rings of Krull dimension 2

$$\tilde{\Lambda} \cong \prod_{[\theta]} \mathbb{Z}_p[\theta][\Delta^{(p)}][[U_1]]$$

where the product ranges over $G_{\mathbb{Q}_p}$-conjugacy classes of characters $\theta \in \widehat{\Delta}'$. Moreover, the irreducible components of $\mathrm{Spec}(\tilde{\Lambda})$ correspond bijectively to Galois-conjugacy classes of characters on Δ. Note that when $\Delta^{(p)}$ is nontrivial, the rings $\mathbb{Z}_p[\Delta^{(p)}]$ and $\mathbb{Z}_p[\Delta^{(p)}][[U_1]]$ are not integral domains. For a general integral $\mathbb{Z}_p$-algebra R in place of $\mathbb{Z}_p$, the decomposition as above still holds, but one considers instead $G_{Q(R)}$-conjugacy classes of characters, though the local rings are no longer necessarily so nice. E.g., the power series ring $\mathcal{O}_{\mathbb{C}_p}[[T]]$ has infinite Krull dimension [Ar73].

There is the well-known structure theorem for finitely generated modules over such rings due to Serre [NSW13, 5.1.10].

Proposition 2.1.1. *Let R be a regular local ring of Krull dimension 2, and let M be a finitely generated R-module. There exist an integer r, a finite index set I, height one primes*

$\mathfrak{p}_i \subset R$ and positive integers m_i for $i \in I$, and a morphism of R-modules

$$M \to R^r \oplus \bigoplus_{i \in I} R/\mathfrak{p}_i^{m_i}$$

with finite kernel and cokernel. Moreover, the r and $\mathfrak{p}_i$ are uniquely determined with $r = \dim_{Q(R)}(M \otimes_R Q(R))$ and the $\mathfrak{p}_i$ are those height one primes occurring in the support of M.

We now define the standard invariants attached to finitely generated modules over such rings R. For $\mathcal{O}$ a complete DVR with uniformizer π, we first recall that the Weierstrass preparation theorem states that any power series $f \in \mathcal{O}[[T]]$ may be written uniquely as $f(T) = u\pi^m f_0(T)$ where $u \in \mathcal{O}^\times$ and $f_0(T)$ is a polynomial which is *distinguished* in the sense that it is monic and all non-leading coefficients are divisible by π.

Definition 2.1.2. *In the notation of Proposition 2.1.1, define the characteristic ideal of M to be the ideal in R given by*

$$\mathrm{char}(M) := \prod_i \mathfrak{p}_i^{m_i}$$

If $R = \mathcal{O}[[T]]$ for a complete DVR $\mathcal{O}$ with uniformizer π, then by the Weierstrass preparation theorem, we may specify generators $\mathfrak{p}_i = (f_i)$ for f_i a distinguished polynomial in R or $f_i = \pi$. In this case, we refine the notation of the structure theorem

$$M \to R^r \oplus \bigoplus_{j \in J} R/(\pi_j^m) \oplus \bigoplus_{k \in K} R/(f_k^{n_k})$$

and define the characteristic polynomial of M to be $\pi^{\sum_{j \in J} m_j} \prod_{k \in K} f_k^{n_k}$. We call $\mu = \sum_{j \in J} m_j$ the μ-invariant of M and $\lambda = \sum_{k \in K} \deg(f_k) n_k$ the λ-invariant of M.

Note that the μ-invariant of a finitely generated, torsion $\Lambda_{\mathcal{O}}$-module M is zero if and only if M is finitely generated as an $\mathcal{O}$-module.

2.2 Iwasawa modules

We fix the p-power compatible system of primitive Np^rth roots of unity $\{\zeta_{Np^r} := e^{2\pi i/Np^r}\}_{r \geq 0}$ in $\overline{\mathbb{Q}} \subset \mathbb{C}$ and define $\mu_{Np^r} \subset \overline{\mathbb{Q}}$ as the set of Np^rth roots of unity in $\overline{\mathbb{Q}}$ for $0 \leq r < \infty$ and

μ_{Np^∞} as $\bigcup_{r>0} \mu_{Np^r}$. We set $\zeta_{p^r} = \zeta_{Np^r}^N$ so that $\{\zeta_{p^r}\}_{r\geq 0}$ forms a p-power compatible system of primitive roots of unity. We define the cyclotomic characters

$$\kappa_{Np} : G_{\mathbb{Q}} \to \mathbb{Z}_{p,N}^\times$$
$$\kappa_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$$

by $\sigma(\zeta_{Np^r}) = \zeta_{Np^r}^{\kappa_{Np}(\sigma)}$ for all r, and similarly for κ_p with ζ_{p^r} in place of ζ_{Np^r}. These characters then induce isomorphisms $\mathrm{Gal}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}) \cong \mathbb{Z}_{p,N}^\times$ and $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$.

We recall that there is a unique Galois extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$ such that $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$. This extension is called the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and may be formed by taking the fixed field of $\mathbb{Q}(\mu_{p^\infty})$ under the action of the torsion subgroup of $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$. For a general number field E, we may then form the cyclotomic $\mathbb{Z}_p$-extension $F \cdot \mathbb{Q}_\infty$ of F which will necessarily be Galois with $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$.

For any extension of number fields F/E with corresponding cyclotomic $\mathbb{Z}_p$-extensions F_∞ and E_∞, we take the convention of identifying the groups $\mathrm{Gal}(F_\infty/F)$ and $\mathrm{Gal}(E_\infty/E)$ via restriction and denote this group by Γ without reference to the base field in the notation. Via the cyclotomic character, we then identify $\Gamma \cong U_1$ in the decomposition $\mathrm{Gal}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}) \cong \mathbb{Z}_{p,N}^\times \cong \Delta \times \Gamma$, viewing Γ both as a quotient and a subgroup of the Galois group, and we similarly identify $\mathrm{Gal}(\mathbb{Q}(\mu_{Np})/\mathbb{Q}) \cong \Delta$.

We now define some of the basic Iwasawa modules of interest.

Definition 2.2.1. *Let F_∞/F be a $\mathbb{Z}_p$-extension of a number field F with intermediate extensions F_r/F of degree p^r. Define the p-parts of the class group of F_r*

$$A_r = A_{F_r} := \mathrm{Cl}_{F_r}[p^\infty].$$

For $1 \leq r \leq \infty$, let $H_r = H_{F_r}$ be the maximal abelian pro-p everywhere unramified extension of F_r. Define the unramified Iwasawa module of F_∞/F to be $X_\infty = X_{F,\infty} := \mathrm{Gal}(H_\infty/F_\infty)$.

The maximality of H_{F_r} gives us that H_{F_r}/F is Galois [Wa97, proof of Theorem 13.13], and class field theory tells us that A_r is canonically isomorphic to the $\mathrm{Gal}(H_{F_r}/F_r)$ compatibly with the natural actions of $\mathrm{Gal}(F_r/F)$ on both objects. Restriction gives a map $X_\infty \to A_r$ for each r, and it can be shown also via class field theory that $X_\infty \cong \varprojlim_r A_r$, where the transition maps $A_{r+1} \to A_r$ are induced by the field norm, or by restriction under the identification with $\mathrm{Gal}(H_{F_r}/F_r)$. This gives X_∞ the structure of a $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$-module, and it was first shown by Iwasawa that X_∞ is finitely generated and torsion as a $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$-module [Iw73, Theorem 5]. If F/K is an abelian extension of number fields and F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension, then F_∞/K is abelian and $X_{F,\infty}$ is also a $\Lambda[\mathrm{Gal}(F/K)]$-module. We will later be interested in the case of the cyclotomic $\mathbb{Z}_p$-extension of a subextension F of $\mathbb{Q}(\mu_{Np})/\mathbb{Q}$.

Remark 2.2.2. The notation is a bit imprecise and inaccurate as the group $X_{F,\infty}$ depends on F_∞, and the $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$-module structure of course depends on F_∞/F. We accept these shortcomings, as it should be clear from the context what $\mathbb{Z}_p$-extension of F one is considering.

For a general abelian group G, $\mathbb{Z}_p[G]$-module M, and character $\chi \in \widehat{G}$, we define

$$M_\chi := M \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\chi]$$

where the map $\mathbb{Z}_p[G] \to \mathbb{Z}_p[\chi]$ is induced by $[a] \mapsto \chi(a)$. We refer to M_χ as the χ-eigenspace of M (we always consider quotients and not submodules unless explicitly stated otherwise).

For any algebraic extension E of $\mathbb{Q}$ and set of places S_E of E, we say that an algebraic extension F/E is S_E-split if it is completely split at all places in S_E.

Definition 2.2.3. *Let the notation be as in the previous definition, and let S be a set of places of F including those over p. Define the S-class group $\mathrm{Cl}_{F_r,S}$ of F_r to be the quotient of Cl_{F_r} by the subgroup generated by the classes of primes of F_r corresponding to places over those in S. Set*

$$A_{r,S} = \mathrm{Cl}_{F_r,S}[p^\infty].$$

For $1 \le r \le \infty$, let $L_r = L_{F_r}$ be the maximal abelian pro-p S-split extension of F_r, and define the S-split Iwasawa module to be $Y_S = Y_{F,S} := \mathrm{Gal}(L_\infty/F_\infty)$.

As before, we have that L_∞/F is Galois by maximality giving Y_S the structure of a $\mathbb{Z}_p[\mathrm{Gal}(F_\infty/F)]$-module. This action is moreover continuous, e.g. as $Y_S \cong \varprojlim_r A_{r,S}$ by class field theory, so that in fact Y_S is a $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$-module. We may view Y_S as a quotient of X_∞ by the subgroup generated by the decomposition subgroups of places of F_∞ above those in S. When F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension, then in fact the decompsition subgroups of X_∞ at places of F_∞ not dividing p are trivial so that Y_S is the quotient of X_∞ by the subgroup generated by decomposition subgroups at places over p, and for any set of places $S' \supset S$ of F containing those that divide p, we have that $Y_{F,S'} \cong Y_{F,S}$ via restriction. This can be seen by considering a place w of F_∞ lying over a place $v \in S$ not lying over p and noting that the completion $F_{\infty,w}$ is the maximal abelian pro-p unramified extension of F_v, so that w must split in any abelian pro-p unramified extension of F_∞.

Finally, we define the S-ramified Iwasawa module. For any algebraic extension E of $\mathbb{Q}$ and set of places S_E of E, we say that an algebraic extension F/E is S_E-ramified if it is unramified at all places not in S_E. When S consists of a single prime $\mathfrak{p}$, we often opt to call the extension $\mathfrak{p}$-ramified rather than S-ramified.

Definition 2.2.4. *Let the notation be as in the previous definitions, and let S be a set of places of F. For $1 \leq r \leq \infty$, let $M_r = M_{F_r}$ be the maximal abelian pro-p S-ramified extension of F_r. Define $\mathfrak{X}_{S,r} = \mathrm{Gal}(M_r/F_r)$ for $r < \infty$, and define the S-ramified Iwasawa module to be $\mathfrak{X}_S = \mathfrak{X}_{F,S} := \mathrm{Gal}(M_\infty/F_\infty)$.*

As before, M_∞ is Galois over F by maximality, and $\mathfrak{X}_S \cong \varprojlim_r \mathfrak{X}_{S,r}$ giving $\mathfrak{X}_S$ the structure of a $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$-module. We have that X_∞ is the quotient of $\mathfrak{X}_S$ by the subgroup generated by the inertia subgroups at places lying over those in S.

We have the following lemma comparing Iwasawa modules associated with fields F and E with F/E abelian of degree prime to p.

Lemma 2.2.5. *Let $K \supset F$ be finite abelian extensions of a number field E with $p \nmid [K : F]$. Set $G = \mathrm{Gal}(K/F)$. Let E_∞/E be a $\mathbb{Z}_p$-extension and set $K_\infty = K \cdot E_\infty$ and $F_\infty = F \cdot E_\infty$.*

Let S be a finite set of places of E and view the Iwasawa modules defined above for K_∞/K and F_∞/F as $\mathbb{Z}_p[[\mathrm{Gal}(E_\infty/E)]][G]$-modules. Then the norm maps induce isomorphisms

$$A_{K,G} \cong A_F$$

$$\mathfrak{X}_{K,S,G} \cong \mathfrak{X}_{F,S}$$

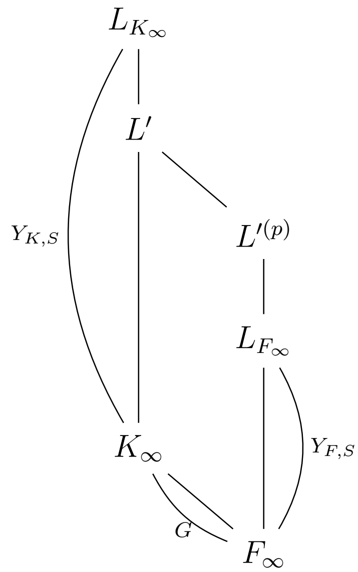
$$X_{K,\infty,G} \cong X_{F,\infty}$$

$$Y_{K,S,G} \cong Y_{F,S},$$

where $(-)_G$ denotes G-coinvariants and where in the last case we assume that $S \supseteq S_p$.

Proof. We give the proof for the S-ramified and S-split Iwasawa modules following the proof of [Oh20, Lemma 2.2.1], where an analogous claim is proved for isotypic components of class groups. Taking S to be empty then gives the claim for the unramified Iwasawa modules as $\mathfrak{X}_\varnothing = X_\infty$. We start with the S-split case.

Let L' denote the maximal abelian subextension of L_{K_∞}/F_∞, and let $L'^{(p)}$ correspond to the maximal pro-p quotient of $\mathrm{Gal}(L'/F_\infty)$. As $p \nmid [K : F]$, we have $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(K_\infty/F_\infty)$ and so $p \nmid [K_\infty : F_\infty]$. Therefore, as L'/K_∞ is S-split, any prime of F_∞ lying over a prime of S can only have ramification index and inertia degree prime to p in L'. We then have that $L'^{(p)}/F_\infty$ is S-split, and therefore we have $L'^{(p)} = L_{F_\infty}$ and $L' = K \cdot L_{F_\infty}$. In terms of Galois groups, this says that the image of $Y_{K,S}$ in the abelianization $\mathrm{Gal}(L_{K_\infty}/F_\infty)^{\mathrm{ab}} \cong G \times Y_{F,S}$ is the factor $Y_{F,S}$.



Consider next the short exact sequence of groups

$$0 \to Y_{K,S} \to \mathrm{Gal}(L_{K_\infty}/F_\infty) \to \mathrm{Gal}(K_\infty/F_\infty) \to 0.$$

As $p \nmid [K_\infty : F_\infty]$, this sequence splits as groups by a profinite version of the Schur-Zassenhaus theorem [RZ10, 2.3.15]. We view $Y_{K,S}$ as a module over $\mathrm{Gal}(K/F)$ and write gx for $g \in \mathrm{Gal}(K/F)$ and $x \in Y_{K,S}$ to mean $\tilde{g}x\tilde{g}^{-1}$, where $\tilde{g} \in \mathrm{Gal}(L_{K_\infty}/F_\infty)$ is any choice of lift of g. As the sequence above is split and as $Y_{K,S}$ and $\mathrm{Gal}(K_\infty/F_\infty)$ are abelian, we find that the commutator subgroup of $\mathrm{Gal}(L_{K_\infty}/F_\infty)$ lies in $Y_{K,S}$ and is generated by the elements $(g-1)x$ for $g \in \mathrm{Gal}(K/F)$ and $x \in Y_{K,S}$. Let D denote the closure of the commutator subgroup of $\mathrm{Gal}(L_{K_\infty}/F_\infty)$. Then $Y_{K,S}/D$ is the module of G-coinvariants of $Y_{K,S}$. On the other hand, by the previous paragraph, we have that $Y_{K,S}/D \cong Y_{F,S}$, proving the claim of the lemma.

For the case of the S-ramified modules, we may argue similarly with M_{K_∞} and M_{F_∞} in place of L_{K_∞} and L_{F_∞}. Letting M' denote the maximal abelian subextension of M_{K_∞}/F_∞ and $M'^{(p)}$ its maximal pro-p subextension, we find that $M'^{(p)}/F_\infty$ is S-ramified as any place of F_∞ not lying over a place of S has ramification index prime-to-p in M' as $p \nmid [K_\infty : F_\infty]$. Thus, we have $M'^{(p)} = M_{F_\infty}$ and $M' = K_\infty \cdot M_{F_\infty}$, and so the image of $\mathfrak{X}_{K,S}$ in $\mathrm{Gal}(M_{K_\infty}/F_\infty)^{\mathrm{ab}} \cong G \times \mathfrak{X}_{F_\infty,S}$

is the factor $\mathfrak{X}_{F_\infty,S}$. We have the split short exact sequence of groups

$$0 \to \mathfrak{X}_{K,S} \to \mathrm{Gal}(M_{K_\infty}/F_\infty) \to \mathrm{Gal}(K_\infty/F_\infty) \to 0,$$

and as before we may conclude that the module of G-coinvariants of $\mathfrak{X}_{K,S}$ is isomorphic to $\mathfrak{X}_{F,X}$. $\square$

Corollary 2.2.6. *In the setting of the lemma above, for any character $\chi \in \widehat{\mathrm{Gal}(F/E)} \subseteq \widehat{\mathrm{Gal}(K/E)}$, we have isomorphisms*

$$A_{K,\chi} \cong A_{F,\chi}$$
$$\mathfrak{X}_{K,S,\chi} \cong \mathfrak{X}_{F,S,\chi}$$
$$X_{K,\infty,\chi} \cong X_{F,\infty,\chi}$$
$$Y_{K,S,\chi} \cong Y_{F,S,\chi}.$$

A similar argument may also be used to demonstrate control of p-class groups up a $\mathbb{Z}_p$-tower in which there is a unique ramified prime above p which is moreover totally ramified.

Lemma 2.2.7 ([Se60, §4])**.** *Let F_∞/F denote a $\mathbb{Z}_p$-extension which is ramified at exactly one prime, and suppose that it totally ramifies. For $n \geq 0$, let F_n/F denote the intermediate extension of degree p^n and let $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$. Then the norm map induces isomorphisms $X_{\infty,\Gamma_n} \cong A_{F_n}$ between the Γ_n-coinvariants of the unramified Iwasawa module $X_\infty = \mathrm{Gal}(H_\infty/F_\infty)$ and the p-class group of F_n.*

Proof. Let L_n denote the maximal abelian subextension of H_∞/F_n. The subextensions H_n and F_∞ of L_n/F_n are linearly disjoint over F_n as the former is unramified while the latter is totally ramified, and the choice of an inertia subgroup in $\mathrm{Gal}(L_n/F_n)$ of a totally ramified prime in F_∞/F_n gives a splitting of $\mathrm{Gal}(L_n/F_n) \twoheadrightarrow \Gamma_n$. As there is only one such prime by assumption, the fixed field corresponding to the image of the inertia subgroup under the splitting must be H_n, and so we have $L_n = F_\infty \cdot H_n$ and an identification $\mathrm{Gal}(L_n/F_\infty) \cong A_{F_n}$.

This says that the image of X_∞ in the abelianization $\mathrm{Gal}(H_\infty/F_n)^{\mathrm{ab}} \cong \Gamma_n \times A_{F_n}$ is the factor A_{F_n}.

$$
\begin{tikzcd}
H_\infty \arrow[d, dash] \arrow[ddd, dash, bend right, "X_\infty"'] & \\
L_n \arrow[dd, dash] \arrow[dr, dash] & \\
& H_n \arrow[dd, dash] \arrow[dd, dash, bend left, "A_{F_n}"] \\
F_\infty \arrow[dr, dash] \arrow[dr, dash, bend right, "\Gamma_n"'] & \\
& F_n
\end{tikzcd}
$$

On the other hand, the exact sequence of groups

$$0 \to \mathrm{Gal}(H_\infty/F_\infty) \to \mathrm{Gal}(H_\infty/F_n) \to \mathrm{Gal}(F_\infty/F_n) \to 0$$

is split as the choice of an inertia subgroup in $\mathrm{Gal}(H_\infty/F_n)$ of a totally ramified prime in F_∞/F_n gives a splitting (this again does not require there to be a unique totally ramified prime). As in the proof of the previous lemma, this splitting implies that the image of $\mathrm{Gal}(H_\infty/F_\infty)$ in $\mathrm{Gal}(H_\infty/F_n)^{\mathrm{ab}}$ is isomorphic to the module of Γ_n-coinvariants of X_∞, and by the previous paragraph, this image is also isomorphic to $\mathrm{Gal}(L_n/F_\infty)$. $\square$

2.2.1 The Iwasawa main conjecture

As Sharifi's conjecture can be viewed as a refinement of the Iwasawa main conjecture, it would be strange not to include a statement of the latter in the dissertation.

Recall that for any Dirichlet character χ of modulus M, there exists the complex analytic Dirichlet L-function in the complex variable s which has a series representation for the real part of s greater than 1

$$L(\chi, s) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

from which one may analytically continue to the whole complex plane, except in the case that χ is trivial where one then has a simple pole at the point $s = 1$. The values of this L-function at nonpositive integers may be written in terms of the generalized Bernoulli numbers $B_{k,\chi} \in \overline{\mathbb{Q}}$ associated with χ

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

for $k \geq 1$, where the Bernoulli numbers are algebraic numbers which may be defined in terms of the Taylor expansion

$$\sum_{a=1}^{N} \frac{\chi(a)te^{at}}{e^{Nt}-1} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}.$$

One may construct a function $L_p(\chi, s)$ on $\mathbb{Z}_p$ which takes on the values

$$L_p(\chi, 1-k) = (1 - (\chi\omega^{-k})_{(0)}(p)p^{k-1})L(\chi\omega^{-k}, 1-k)$$

for integers $k \geq 1$, where ω denotes the Teichmüller character and where for a general Dirichlet character θ we denote by $\theta_{(0)}$ its associated primitive Dirichlet character. In this sense, the function $L_p(\chi, s)$ p-adically interpolates the values of complex analytic L-functions associated to twists of the character χ at the nonpositive integers. Below, in Section 3.3.1, we give a detailed construction of these p-adic L-functions as elements of $\Lambda_{\mathbb{Z}_p[\chi]} \cong \mathbb{Z}_p[\chi][[T]]$ following Iwasawa [Iw69]. Write $f_\chi(T)$ for the power series satisfying

$$f_\chi(\gamma^s - 1) = L_p(\chi^{-1}\omega, s),$$

where we remind the reader that $[\gamma] = [1+p] \in \Lambda_{\mathbb{Z}_p}$ is sent to $1 + T \in \mathbb{Z}_p[[T]]$ under the isomorphism $\Lambda_{\mathbb{Z}_p} \cong \mathbb{Z}_p[[T]]$.

We can now state the Iwasawa main conjecture for the cyclotomic $\mathbb{Z}_p$-extension of an abelian number field over $\mathbb{Q}$. Let χ be an odd Dirichlet character of modulus M where $p^2 \nmid M$, and view χ as a character of $\mathrm{Gal}(\mathbb{Q}(\mu_M)/\mathbb{Q}) \cong (\mathbb{Z}/M\mathbb{Z})^\times$. Set $F = \mathbb{Q}(\mu_M)^{\ker(\chi)}$ and continue to denote by χ the character of $\mathrm{Gal}(F/\mathbb{Q})$ induced by χ.

Theorem 2.2.8 ([MW84, p. 214]). *The characteristic ideal of $X_{F,\infty,\chi}$ in $\Lambda_{\mathbb{Z}_p[\chi]}$ is generated by $f_\chi(T)$.*

Remark 2.2.9. Recall that for even characters θ, the p-adic L-function $L_p(\theta^{-1}\omega, s)$ is identically 0, and the component $X_{F,\infty,\theta}$ is conjectured to be finite by Greenberg [Gr71].

As mentioned in the introduction, the main conjecture was originally proved in 1984 by Mazur and Wiles [MW84] through a careful study of the geometry of certain abelian variety quotients with good reduction at p of the Jacobians $J_1(Np^r)$ of the modular curves $X_1(Np^r)$ for $r \geq 1$. Their proof can be viewed to be in a similar line of thought as that of Ribet's proof in [Ri76] of the converse to Herbrand's theorem in that Mazur and Wiles constructed unramified abelian extensions of the fields $\mathbb{Q}(\mu_{Np^r})$ as the splitting fields of Galois representations, from which a Fitting ideal argument led to the conclusion that $f_\chi(T)$ divides $\mathrm{char}((X_\infty)_\chi)$. These divisibilities for all such χ together with the analytic class number formula, and Ferrero and Washington's result on the vanishing of the μ-invariant of X_∞ [FW79], imply equality of ideals. However, rather than directly studying congruences between Eisenstein series and cusp forms as Ribet did, Mazur and Wiles studied the cuspidal divisor class subgroups of the Jacobians $J_1(Np^r)$, which lie inside the part of the aforementioned quotient abelian varieties killed by the Eisenstein ideals of the cuspidal Hecke algebras of each level $\Gamma_1(Np^r)$.

In [Wi86], Wiles revisited the ideas of Ribet and streamlined the proof of the main conjecture over $\mathbb{Q}$ while additionally generalizing the results to cover the analogous main conjecture for totally real fields of odd degree over $\mathbb{Q}$. The argument eschewed the analysis of the cuspidal group and proceeded instead by establishing congruences between sequences of (Hilbert) cusp forms and (Hilbert) Eisenstein series with coefficients in the group rings $\mathbb{Z}_p[(\mathbb{Z}/Np^r\mathbb{Z})^\times]$ for $r \geq 1$ and then showing the existence of lattices with prescribed properties inside the representation spaces of the Galois representations associated with the cusp forms coming from the cohomology of (Hilbert) modular varieties (cf. [Wi86, §3] or [Wi90, §5]). The splitting field of the representations on the lattices modulo the Eisenstein ideal then produce unramified extensions of $\mathbb{Q}(\mu_{Np^\infty})$ in the appropriate components of X_∞, and again a Fitting ideal argument gives divisibility of the characteristic polynomial by the p-adic L-function. The restriction on the degree of the totally real field over $\mathbb{Q}$ was due to the lack of knowledge at the time of the existence of representations associated with Hilbert cusp forms in general – the odd degree case being due to work of Hida and of Carayol building off the work of Shimura. These obstacles were overcome in [Wi88] and [MW86], now using the language of the recently developed Hida theory, and led to a proof of the cyclotomic main conjecture for all totally real fields in [Wi90] up to μ-invariants, following the same strategy as that in [Wi86].

One shortcoming of Wiles' arguments in [Wi90] in the case of $\mathbb{Q}$ is that the lattices that he used are inexplicit – he showed that starting with any Galois stable lattice inside the representation associated with a cusp form, one can find a stable sublattice such that its reduction modulo the Eisenstein ideal has the desired optimality property in the sense that it is "type 1 deprived" in the terminology of [Wi90, Proposition 5.2] and the discussion following. Any optimal lattice can then be used to prove the main conjecture via the process described above. In the case of $\mathbb{Q}$, there is of course a natural lattice that one is led to consider in the representation space: that given by the integral étale cohomology of the modular curve. In short, the part of Sharifi's conjecture with which we concern ourselves in this dissertation is the claim that this canonical lattice is optimal; the map Υ comes from a cocycle associated with the extension class of the Galois representation associated with this lattice, and its surjectivity is equivalent to this claim of optimality.

2.3 Iwasawa Cohomology

In this section, we define Iwasawa cohomology groups as inverse limits of continuous Galois cohomology groups along a tower of fields in a $\mathbb{Z}_p$-extension of a number field. We then relate the Iwasawa modules defined in the previous section to these cohomology groups and describe their compatibilities along extensions of number fields.

Let E be an algebraic extension of $\mathbb{Q}$ and let S_E be a set of places E. Set $G_{E,S_E} = \mathrm{Gal}(E_{S_E}/E)$ the Galois group of the maximal S_E-ramified extension E_{S_E} of E. We will often write S_E simply as S when it is clear with which field it is that we are concerned. We also often take the convention that when considering an extension of fields L/K and a set of places S_K of K, the notation S_L will denote the set of places of L that lie over those in S_K, and in some instances, we will use S to denote either of S_K or S_L when it is clear from context which is meant. For any set of places S, we denote by S_f its subset of finite places, and for an extension of fields E/F, we indicate that the extension is finite by the use of the notation $E \supseteq_f F$.

Definition 2.3.1. *Let p be an odd prime and R the ring of integers of a finite extension of $\mathbb{Q}_p$. Let F be a number field, S a set of places of F containing those over p and any real places, and F_∞/F a $\mathbb{Z}_p$-extension. For a finitely generated, continuous $R[[G_{F,S}]]$-module T, define the ith S-ramified Iwasawa cohomology group of T to be*

$$H^i_{\mathrm{Iw},S}(F_\infty/F, T) = \varprojlim_{F_\infty \supset E \supseteq_f F} H^i(G_{E,S}, T),$$

where we take the convention that all group cohomology groups considered will be of continuous group cohomology, and where the limit is with respect to the corestriction maps running over all finite subextensions of F_∞/F. If F/K is a Galois extension, then $H^i_{\mathrm{Iw},S}(F_\infty/F, T)$ is naturally an $R[[\mathrm{Gal}(F_\infty/K)]]$-module induced from the usual action on conjugation on group cohomology.

Set $\mathbb{Q}_{N_r} = \mathbb{Q}(\mu_{Np^r})$ for $1 \leq r \leq \infty$. Recall from the introduction that the group $H^2_{\mathrm{Iw},S_{Np}}(\mathbb{Q}_{N_\infty}/\mathbb{Q}_{N_1}, \mathbb{Z}_p(2))$ is the target of the morphism ϖ in Sharifi's conjecture and that its image is contained in the submodule of S_p-ramified Iwasawa cohomology. As Υ is meant to be the inverse to ϖ, we review in this section some general properties of this group for use in Chapter 4.

Note that if E/F is an S-ramified extension, then $F_S = E_S$ so that $G_{E,S}$ is a subgroup of $G_{F,S}$. We then have an identification of Iwasawa cohomology groups of E and of F when E/F is in addition finite and Galois.

Lemma 2.3.2. *Let the notation be as in the definition above, and let E/F be an S_F-ramified Galois extension of number fields. Set $E_\infty = E \cdot F_\infty$, and let S_E denote the corresponding set of places of E. Then the inverse limit of corestriction maps induces an isomorphism*

$$\mathrm{cor} : H^2_{\mathrm{Iw},S_E}(E_\infty/E, T)_{\mathrm{Gal}(E/F)} \xrightarrow{\cong} H^2_{\mathrm{Iw},S_F}(F_\infty/F, T).$$

Proof. By [NSW13, 3.3.11], corestriction gives an isomorphism at finite level for each r

$$\mathrm{cor}_r : H^2(G_{E_r,S_{E_r}}, T)_{\mathrm{Gal}(E/F)} \xrightarrow{\cong} H^2(G_{F_r,S_{F_r}}, T)$$

as $G_{E_r,S_{E_r}}$ is an open normal subgroup of $G_{F_r,S_{F_r}}$ and both have p-cohomological dimension 2 [NSW13, 10.11.3]. $\square$

For any algebraic extension $E/\mathbb{Q}$ and set of places S_E of E, we let $\mathcal{O}_{E,S_E}$ denote the ring of S_E-integers of E, i.e., those elements of E which have non-negative valuation at finite places not in S_E. We have the following lemma relating the S-split Iwasawa module Y_S and Iwasawa cohomology groups.

Lemma 2.3.3. *Let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension of a number field F, and let F/K be an abelian extension of number fields. Let S be a set of places of F containing those dividing p and any real places. Then there is an exact sequence of $\Lambda[\mathrm{Gal}(F/K)]$-modules.*

$$0 \to Y_{F,S} \to H^2_{\mathrm{Iw},S}(F_\infty/F, \mathbb{Z}_p(1)) \to \bigoplus_{w \in S_{F_\infty,f}} \mathbb{Z}_p \xrightarrow{\Sigma} \mathbb{Z}_p \to 0 \tag{2.3.1}$$

where the $\Lambda[\mathrm{Gal}(F/K)]$-module structure on the direct sum is induced by the natural action of $\mathrm{Gal}(F_\infty/K)$ permuting the places of F_∞.

Proof. We give a sketch of the proof and refer the reader to [NSW13, §8.3] for more details on Galois cohomology with restricted ramification. For a finite intermediate extension E of F_∞/F, the Kummer sequence

$$0 \to \mu_{p^n} \to \mathcal{O}_{E_S,S}^\times \xrightarrow{(-)^{p^n}} \mathcal{O}_{E_S,S}^\times \to 0$$

gives rise to the exact sequence

$$0 \to A_{E,S}/p^n A_{E,S} \to H^1(G_{E,S}, \mu_{p^n}) \to H^2(G_{E,S}, \mathcal{O}_{E_S,S}^\times)[p^n] \to 0, \tag{2.3.2}$$

where $A_{E,S}$ is the p-part of the S-class group of E. We can then consider the long exact sequence associated with the short exact sequence

$$0 \to \mathcal{O}_{E_S,S}^\times \to I_S \to C_S \to 0$$

where $I_S = \varinjlim_K I_{K,S}$ is the filtered colimit of the S-idèles $I_{K,S} = \prod_{w \in S_K} K_w^\times$ of finite intermediate extensions K of E_S/E and C_S is the filtered colimit along the same indexing set of S-idèle class groups. By [NSW13, 8.3.11, 8.3.8], we have isomorphisms of $\mathrm{Gal}(E/F)$-modules

$$H^2(G_{E,S}, I_S)[p^n] \cong \bigoplus_{v \in S_{E,f}} H^2(\mathrm{Gal}((E_S)_{\widetilde{w}}/E_v), (E_S)_{\widetilde{w}}^\times)[p^n] \cong \bigoplus_{v \in S_{E,f}} \mathbb{Z}/p^n\mathbb{Z}$$

where $\widetilde{w}|v$ is any place of E_S lying over v and where the action of $\mathrm{Gal}(E/F)$ on the direct sum is given by permutation of the summands corresponding to the natural conjugation action on decomposition groups D_v, and a short exact sequence of $\mathrm{Gal}(E/F)$-modules,

$$0 \to H^2(G_{E,S}, \mathcal{O}_{E_S,S}^\times)[p^n] \to \bigoplus_{v \in S_{E,f}} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\Sigma} H^2(G_{E,S}, C_S)[p^n] \cong \mathbb{Z}/p^n\mathbb{Z} \to 0. \tag{2.3.3}$$

We see that

$$H^2(\mathrm{Gal}((E_S)_{\widetilde{w}}/E_v), (E_S)_{\widetilde{w}}^\times)[p^n] \cong H^2(\mathrm{Gal}((E_S)_{\widetilde{w}}/E_v), \mu_{p^n})$$

by considering the long exact sequence associated with

$$0 \to \mu_{p^r} \to (E_S)_{\widetilde{w}}^\times \xrightarrow{(-)^{p^n}} (E_S)_{\widetilde{w}}^\times \to 0$$

and using Hilbert's Theorem 90. Splicing the two short exact sequences 2.3.2 and 2.3.3 into a four-term exact sequence and taking an inverse limit over n gives

$$0 \to A_{E,S} \to H^2(G_{E,S}, \mathbb{Z}_p(1)) \to \bigoplus_{v \in S_{E_f}} \mathbb{Z}_p \xrightarrow{\Sigma} \mathbb{Z}_p \to 0.$$

Taking an inverse limit over finite intermediate extensions $F_\infty \supset E \supseteq_f F$ gives the exact sequence of the lemma. $\square$

It may be useful to think of the third term of sequence 2.3.1 in the following manner. For the remainder of this chapter, we use the notation $\tilde{\Gamma} = \mathrm{Gal}(F_\infty/K)$ and for each $v \in S_{F,f}$, we pick a place $w \mid v$ of F_∞ and let $\tilde{\Gamma}_v$ be the corresponding decomposition subgroup. We may then define a bijection of $\mathbb{Z}_p[[\tilde{\Gamma}]]$-modules

$$\bigoplus_{w \in S_{F_\infty,f}} \mathbb{Z}_p \cong \bigoplus_{v \in S_{F,f}} \mathbb{Z}_p[[\tilde{\Gamma}/\tilde{\Gamma}_v]],$$

where a coset $\sigma\tilde{\Gamma}_v$ corresponds to the place $\sigma(w)$. The direct sum on the right is of $\mathbb{Z}_p[[\tilde{\Gamma}]]$-modules, and the action of $[\sigma] \in \mathbb{Z}_p[[\tilde{\Gamma}]]$ for $\sigma \in \tilde{\Gamma}$ on each summand is given by multiplication by $[\sigma]$.

Recall from the discussion after Definition 2.2.3 that the canonical quotient map of Iwasawa modules $Y_{F,S'} \to Y_{F,S}$ is an isomorphism for any subset $S' \subseteq S$ containing the places over p when F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension. This quotient map fits into a diagram of exact sequences

$$\begin{array}{ccccccccc} 0 \longrightarrow & Y_{F,S'}(1) & \longrightarrow & H^2_{\mathrm{Iw},S'}(F_\infty/F, \mathbb{Z}_p(2)) & \longrightarrow & \bigoplus_{S'} \mathbb{Z}_p[[\tilde{\Gamma}/\tilde{\Gamma}_l]](1) & \longrightarrow & \mathbb{Z}_p(1) & \longrightarrow 0 \\ & \downarrow{\cong} & & \downarrow{\mathrm{inf}} & & \downarrow & & \| & \\ 0 \longrightarrow & Y_{F,S}(1) & \longrightarrow & H^2_{\mathrm{Iw},S}(F_\infty/F, \mathbb{Z}_p(2)) & \longrightarrow & \bigoplus_{S} \mathbb{Z}_p[[\tilde{\Gamma}/\tilde{\Gamma}_l]](1) & \longrightarrow & \mathbb{Z}_p(1) & \longrightarrow 0 \end{array} \qquad (2.3.4)$$

where the map "inf" is an inverse limit of inflation maps and the third vertical morphism corresponds to the inclusion $S' \subseteq S$. Note that the horizontal sequences are Tate twists of sequence!2.3.1 as in general one has

$$H^j_{\mathrm{Iw},S}(F_\infty/F, \mathbb{Z}_p)(i) \cong H^j_{\mathrm{Iw},S}(F_\infty/F, \mathbb{Z}_p(i)).$$

This can be seen by first reducing to the case that $\mu_p \subset F$ as in general $F(\mu_p)/F$ is S-ramified, and we may apply Lemma 2.3.2. Then, by viewing the Iwasawa cohomology group as a "diagonal" inverse limit

$$H^j_{\mathrm{Iw},S}(F_\infty/F, \mathbb{Z}_p(i)) \cong \varprojlim_n H^j(G_{F_n,S}, \mu_{p^n}^{\otimes i}),$$

we see we may pull the twists out of the cohomology groups in the inverse limit as $\mu_{p^n} \subset F_n$.

To conclude this section, we point out that while the injectivity of the "inf" map of diagram 2.3.4 follows from a diagram chase, granting that the inflation maps on the adelic Brauer groups do indeed correspond to the inclusion of direct summands, we opt to give a second explanation of this injectivity via a more geometric route as it also gives us a chance to introduce the Gysin sequence in étale cohomology, which will be brought up again in Chapter 4. In fact, we will end up proving a stronger statement.

We recall that for a number field K and a set of places S of K including all real places, there is a natural isomorphism between the Galois cohomology of K with S-restricted ramification of a continuous profinite $G_{K,S}$-module M whose finite quotients have order invertible in $\mathcal{O}_{K,S}$ and the étale cohomology of $\mathrm{Spec}(\mathcal{O}_{K,S})$

$$H^i(G_{K,S}, M) \cong H^i_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_{K,S}), \mathcal{F}_M)$$

for $i \geq 0$, where $\mathcal{F}_M$ is the inverse system of sheaves on the étale site $(\mathrm{Spec}(\mathcal{O}_{K,S}))_{\text{ét}}$ associated with M. This follows from the degeneration of the Hochschild-Serre spectral sequence as in [Mi06, Prop. II.2.9].

For a general closed immersion of schemes $i\colon Z \to X$ with corresponding open complement $j\colon U \to X$ and any sheaf of abelian groups $\mathcal{F}$ on $X_{\text{ét}}$, we have a short exact sequence of sheaves on $X_{\text{ét}}$ [SP, Tag 095L]

$$0 \to j_!j^*\mathcal{F} \to \mathcal{F} \to i_*i^*\mathcal{F} \to 0.$$

Taking $\mathcal{F}$ to be the constant sheaf $\underline{\mathbb{Z}}_X$ and taking the long exact sequence associated with the short exact sequence of the functor $\mathrm{Hom}(-, \mathcal{G})$, we obtain

$$\cdots \to H^i_{\text{ét},Z}(X, \mathcal{G}) \to H^i_{\text{ét}}(X, \mathcal{G}) \to H^i_{\text{ét}}(U, \mathcal{G}|_U) \to H^{i+1}_{\text{ét},Z}(X, \mathcal{G}) \to \cdots$$

where $H^i_{\text{ét},Z}(X, \mathcal{G})$ is the ith étale cohomology group with support in Z, i.e., the ith right derived functor of global sections with support in Z functor - see e.g. the introduction of [SP, Tag 09XP]. In the sequence above, the morphism between the middle two cohomology groups corresponds to the inclusion j, and in the situation that $X = \mathrm{Spec}(\mathcal{O}_{K,S'})$ and $U = \mathrm{Spec}(\mathcal{O}_{K,S})$ for a subset of places $S' \subset S$ (with finite complement $S \backslash S'$), the corresponding map on Galois cohomology is the inflation morphism corresponding to the natural quotient $G_{K,S} \to G_{K,S'}$. The purity theorem due to Thomason and Gabber relates cohomology with support in Z to cohomology on Z.

Lemma 2.3.4. *Let $i\colon Z \to X$ be a closed immersion of regular schemes of pure codimension c. For any locally constant sheaf of $\mathbb{Z}/n\mathbb{Z}$-modules $\mathcal{G}$ on $X_{\text{ét}}$ with n invertible on X, there is a natural isomorphism*

$$H^i_{\text{ét},Z}(X, \mathcal{G}) \xrightarrow{\cong} H^{i-2c}_{\text{ét}}(Z, \mathcal{G}(-c)).$$

The result was conjectured originally in [SGA5, Exposé I 3.1.4] at the level of generality stated here, though in the case that $\dim(X) = 1$, it was proved in [SGA5, Exposé I 5.1]. Applying this to the case $\mathcal{G} = \mu_{p^n}^{\otimes i}$ for $i \in \mathbb{Z}$, we obtain the exact sequence

$$\begin{aligned} 0 \to H^1_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_{K,S'}), \mu_{p^n}^{\otimes i}) \to H^1_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_{K,S}), \mu_{p^n}^{\otimes i}) \to \\ \bigoplus_{v \in S \backslash S'} H^0_{\text{ét}}(\mathrm{Spec}(\kappa(v)), \mu_{p^n}^{\otimes i-1}) \to H^2_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_{K,S'}), \mu_{p^n}^{\otimes i}) \to H^2_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_{K,S}), \mu_{p^n}^{\otimes i}) \\ \to \bigoplus_{v \in S \backslash S'} H^1_{\text{ét}}(\mathrm{Spec}(\kappa(v)), \mu_{p^n}^{\otimes i-1}) \to 0 \end{aligned}$$

where $\kappa(v)$ is the residue field of a prime v of $\mathcal{O}_K$. Taking an inverse limit along n gives

$$\varprojlim_n H^0_{\text{ét}}(\mathrm{Spec}(\kappa(v)), \mu_{p^n}^{\otimes i-1}) = 0$$

when $i \neq 1$, so that the inflation map on $H^2(G_{K,S'}, \mathbb{Z}_p(i))$ is injective when $i \neq 1$.[1] Taking an inverse limit along finite subextensions $F_\infty \supset K \supseteq_f F$ gives injectivity of inf on Iwasawa cohomology.[2] Note also that the Gysin sequence shows that $Y_{F,S'} \cong Y_{F,S}$.

2.4 Iwasawa theory of imaginary quadratic fields

In this section, we provide some background on the Iwasawa theory of imaginary quadratic fields for use in Chapter 4. We first review the definition and basic properties of the anticyclotomic $\mathbb{Z}_l$-extension of a finite abelian extension of an imaginary quadratic $K/\mathbb{Q}$ for a rational prime l. Additionally, for a rational prime p split in K, we state the single variable $\mathfrak{p}$-ramified main conjecture for an abelian extension of K. Our choice of notation for the primes used here reflects our intended application of the statements of this section.

2.4.1 Ring class fields and the anticyclotomic $\mathbb{Z}_l$-extension

Recall that an order R of an algebraic number field F of degree n over $\mathbb{Q}$ is a subring of $\mathcal{O}_F$ which is finite over $\mathbb{Z}$ of rank n. For any order R of F, we define the conductor $\mathfrak{f}_R$ of R to be the annihilator in R of the R-module quotient $\mathcal{O}_F/R$, which necessarily is also an ideal of $\mathcal{O}_F$. This may also be viewed as the colon-quotient ideal

$$(R : \mathcal{O}_F) = \{x \in F \mid x\mathcal{O}_F \subseteq R\},$$

or alternatively the module $\mathrm{Hom}_R(\mathcal{O}_F, R)(\subset F)$. When F is a quadratic extension of $\mathbb{Q}$, then in fact the conductor as an ideal of $\mathcal{O}_F$ is generated by a positive integer, which we also call the conductor of R, and this integer then agrees with the index $[\mathcal{O}_F : R]$. For any positive integer n, there is a unique order $\mathcal{O}_n := \mathbb{Z} + n\mathcal{O}_K$ in $\mathcal{O}_K$ of conductor n [Co13, Lemma 7.2].

[1] Note that on Iwasawa cohomology groups for a cyclotomic $\mathbb{Z}_p$-extension, the map "inf" is injective regardless of the twist of the coefficients, as the twists may be pulled out of the cohomology groups.

[2] For general $S' \subseteq S$, we may cofilter by $S' \subseteq S'' \subseteq S$ for cofinite $S'' \subseteq S$.

For an integral domain R with fraction field F, we define a fractional ideal of R to be a nonzero finitely generated R-submodule of F. There is a clear structure of a monoid on the set of fractional ideals of R, and we may consider the unit group of invertible fractional ideals $I(R)$ of this monoid along with the subgroup of principal fractional ideals $P(R) \cong F^\times/R^\times$, i.e., those which are free of rank 1 as R-modules. The quotient group of invertible fractional ideals modulo principal fractional ideals is called the class group of R. We remark that often in the literature, invertible fractional ideals of $\mathcal{O}_n$ (that is, in the quadratic case) are referred to as proper fractional ideals. Proper fractional ideals are defined generally for an order R of a number field F as those fractional ideals $\mathfrak{a}$ satisfying

$$(\mathfrak{a} : \mathfrak{a}) = R.$$

Every invertible fractional ideal is proper, and for quadratic fields, the converse is also true [Co13, Proposition 7.4]. We may also consider the set of isomorphism classes of R-modules with a monoid structure given by tensor product over R. The unit group of isomorphism classes of invertible R-modules of this monoid is called the Picard group $\mathrm{Pic}(R)$ of R. We have that an invertible R-module M is always isomorphic as an R-module to an invertible fractional ideal of R, as $M \hookrightarrow M \otimes_R F \cong F$ so that in fact the class group and Picard group of R coincide.

Remark 2.4.1. It is perhaps worth pointing out that the class group considered here is precisely the group of Cartier divisors of R up to linear equivalence. One may also consider the group of Weil divisors, viewed either as the group of formal (finite) linear combinations over $\mathbb{Z}$ of height 1 primes of R or equivalently as the group of formal linear combinations over $\mathbb{Z}$ of codimension 1 integral subschemes of $\mathrm{Spec}(R)$. Its subgroup of principal divisors is defined to be the subgroup generated by those linear combinations of the form

$$\sum_{\mathfrak{p}} l_{\mathfrak{p}}(R/(f))\mathfrak{p}$$

for some $f \in F^\times$, where $l_{\mathfrak{p}}$ is the length of the $R_{\mathfrak{p}}$-module $R_{\mathfrak{p}}/(f)$. One may then define the Weil divisor class group as the group of Weil divisors modulo the subgroup of principal divisors. There is a canonical map from the group of Cartier divisors to the group of Weil divisors which then induces a map of class groups which is neither injective nor surjective in general. When R is Noetherian and normal, then the map of class groups is injective [SP, Tag 0BE8], and if R is additionally factorial, meaning its local rings are all UFDs, then the map is surjective [SP, 0BE9]. For instance, when R is the ring of integers of a number field, the isomorphism of Cartier and Weil divisor class groups is reflected in the unique factorization of fractional ideals of R into a product of prime ideals. In the context of subrings of number fields, the Picard group is the more arithmetically interesting group to consider, and though focusing only on the Weil divisors of $\mathrm{Spec}(R)$ is too crude to deduce properties of the Picard group when R is an order (so not necessarily normal), we do have that the group of invertible fractional ideals of an order R is isomorphic to the direct sum over all nonzero prime ideals of R of the groups of principal fractional ideals of the local rings [Ne99, Proposition 12.6]

$$I(R) \cong \bigoplus_{\mathfrak{p} \neq (0)} P(R_{\mathfrak{p}}).$$

This fact features in the proof of the following formula for the order of $\mathrm{Pic}(R)$ in terms of $\mathrm{Pic}(\mathcal{O}_F)$.

Lemma 2.4.2. *Let R be an order of a number field F. The order of* $\mathrm{Pic}(R)$ *is given by*

$$|\mathrm{Pic}(R)| = \frac{|\mathrm{Pic}(\mathcal{O}_F)|}{[\mathcal{O}_F^\times : R^\times]} \frac{(\mathcal{O}_F/\mathfrak{f}_R)^\times}{(R/\mathfrak{f})^\times}.$$

In particular, if K is an imaginary quadratic field with $\mathcal{O}_K^\times = \{\pm 1\}$ and l is an odd prime, then for $r \geq 1$,

$$|\mathrm{Pic}(\mathcal{O}_{l^r})| = \begin{cases} |\mathrm{Pic}(\mathcal{O}_K)| l^{r-1}(l-1) & \textit{if } l \textit{ is split in } K, \\ |\mathrm{Pic}(\mathcal{O}_K)| l^{r-1}(l+1) & \textit{if } l \textit{ is inert in } K, \\ |\mathrm{Pic}(\mathcal{O}_K)| l^{r} & \textit{if } l \textit{ is ramified in } K. \end{cases}$$

Proof. By the isomorphism of the above remark, we have that

$$\mathrm{Pic}(R) \cong (\bigoplus_{\mathfrak{p} \neq (0)} P(R_{\mathfrak{p}}))/P(R) \quad \text{and} \quad \mathrm{Pic}(\mathcal{O}_F) \cong (\bigoplus_{\widetilde{\mathfrak{p}} \neq (0)} P(\mathcal{O}_{F,\widetilde{\mathfrak{p}}}))/P(\mathcal{O}_F).$$

For a nonzero prime ideal $\mathfrak{p}$ of R, we have that $\mathcal{O}_{F,\mathfrak{p}}$ is a PID so that $P(\mathcal{O}_{F,\mathfrak{p}}) \cong \bigoplus_{\mathrm{Spec}(\mathcal{O}_F)\ni\widetilde{\mathfrak{p}}\supset\mathfrak{p}} P(\mathcal{O}_{F,\widetilde{\mathfrak{p}}})$. Therefore, we may write

$$\mathrm{Pic}(\mathcal{O}_F) \cong \left(\bigoplus_{\mathrm{Spec}(R)\ni\mathfrak{p}\neq(0)} P(\mathcal{O}_{F,\mathfrak{p}}) \right) / P(\mathcal{O}_F).$$

The inclusion $R \subset \mathcal{O}_F$ induces a morphism of short exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & F^\times/R^\times & \longrightarrow & \bigoplus_{\mathfrak{p}\neq(0)} F^\times/R_\mathfrak{p}^\times & \longrightarrow & \mathrm{Pic}(R) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & F^\times/\mathcal{O}_F^\times & \longrightarrow & \bigoplus_{\mathfrak{p}\neq(0)} F^\times/\mathcal{O}_{F,\mathfrak{p}}^\times & \longrightarrow & \mathrm{Pic}(\mathcal{O}_F) & \longrightarrow & 0.
\end{array}$$

The first two vertical arrows are quotient maps, so that the third vertical arrow is also surjective. We obtain then the exact sequence

$$0 \to \mathcal{O}_F^\times/R^\times \to \bigoplus_{\mathfrak{p}\neq(0)} \mathcal{O}_{F,\mathfrak{p}}^\times/R_\mathfrak{p}^\times \to \mathrm{Pic}(R) \to \mathrm{Pic}(\mathcal{O}_F) \to 0.$$

We have that $\bigoplus_{\mathfrak{p}\neq(0)} \mathcal{O}_{F,\mathfrak{p}}^\times/R_\mathfrak{p}^\times \cong (\mathcal{O}_F/\mathfrak{f}_R)^\times/(R/\mathfrak{f}_R)^\times$, giving the general formula in the statement of the lemma.

For the specific case of $F = K$ an imaginary quadratic field and $R = \mathcal{O}_{l^r}$, we have that $\mathfrak{f}_R = l^r\mathcal{O}_K \subset R$ so that $\mathcal{O}_{l^r}/(l^r\mathcal{O}_K) \cong \mathbb{Z}/l^r\mathbb{Z}$ has unit group of order $(l-1)l^{r-1}$. If l is split in K, the unit group of $\mathcal{O}_K/(l^k) \cong (\mathbb{Z}/l^r\mathbb{Z})^2$ has order $((l-1)l^{r-1})^2$. If l is inert or ramified in K, then we may use the standard decomposition of $(\mathcal{O}_K/(l^r))^\times$ into $(\mathcal{O}_K/(l))^\times \times (1+l\mathcal{O}_K)/l^r\mathcal{O}_K$ to find that $|(\mathcal{O}_K/(l^r))^\times|$ is $(l^2-1)l^{2r-2}$ if l is inert and $(l-1)l^{2r-1}$ if l is ramified. The formula for the order of $\mathrm{Pic}(\mathcal{O}_{l^r})$ in the statement of the lemma then follows as $[\mathcal{O}_K^\times : \mathcal{O}_{l^r}^\times] = 1$ by assumption.

$\square$

One may show that $\mathrm{Pic}(\mathcal{O}_n)$ is isomorphic to the idelic group

$$K^\times \backslash \mathbb{I}_{K,f}/\widehat{\mathcal{O}}_n^\times$$

where $\widehat{\mathcal{O}}_n$ is the profinite completion of $\mathcal{O}_n$ and $\mathbb{I}_{K,f}$ is the group of finite ideles of K [Co13, 15.35]. The corresponding abelian extension of K coming from class field theory is called the ring class field L_n of $\mathcal{O}_n$ or of conductor n. When $n = 1$, the ring class field is the Hilbert class field of K, and for each $n \geq 1$, the ring class field L_n contains the Hilbert class field of K and is contained in the ray class field of modulus $n\mathcal{O}_K$. Naturality of Artin reciprocity, in the sense that the reciprocity map is compatible with isomorphisms of fields, and stability of $\mathcal{O}_n$ under complex conjugation shows that $L_n/\mathbb{Q}$ is Galois and that the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathrm{Gal}(L_n/K)$ by inversion [Co13, Lemma 9.3]. Such extensions are called generalized dihedral extensions of $\mathbb{Q}$, and in fact all generalized dihedral finite extensions of $\mathbb{Q}$ which are abelian over K are contained in some ring class field of K [Co13, Theorem 19.18].

We now consider $\mathbb{Z}_l$-extensions of K for l an odd prime. Recall from class field theory that the $\mathbb{Z}_l$-rank of K is 2, i.e., that the Galois group of the maximal pro-l abelian extension of K has rank 2 as a $\mathbb{Z}_l$-module. The cyclotomic $\mathbb{Z}_l$-extension K_{cyc} arises as the fixed field of $K(\mu_{l^\infty})$ under the action of the torsion subgroup of $\mathrm{Gal}(K(\mu_{l^\infty})/K)$. Note that K_{cyc} is Galois and abelian over $\mathbb{Q}$ so that the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$ acts trivially on $\mathrm{Gal}(K_{\mathrm{cyc}}/K)$. On the other hand, we have the complementary so-called anticyclotomic $\mathbb{Z}_l$-extension of K.

Definition 2.4.3. *The anticyclotomic $\mathbb{Z}_l$-extension K_{ac} of K is the unique $\mathbb{Z}_l$-extension contained in the union $H_\infty = \bigcup_n L_{l^n}$ of ring class fields of K of l-power conductor. That is, it is the fixed field of H_∞ under the action of the torsion part of* $\mathrm{Gal}(H_\infty/K)$.

We see that K_{cyc} and K_{ac} are the only two $\mathbb{Z}_l$-extensions of K which are Galois over $\mathbb{Q}$ using the classifications of generalized dihedral extensions and of abelian extensions over $\mathbb{Q}$. Note also that consideration of the effects of the action of $\mathrm{Gal}(K/\mathbb{Q})$ on their respective Galois groups shows that K_{cyc} and K_{ac} are linearly disjoint over K.

In section 4.3, we will consider the growth of p-parts of class groups up the tower $K_{\mathrm{ac}}F/F$ for F/K a finite abelian extension satisfying certain ramification conditions and an odd prime

$p \neq l$ which is split in K.

2.4.2 The $\mathfrak{p}$-ramified main conjecture for K

Let p be an odd prime which splits into distinct primes $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in K, where $\mathfrak{p}$ corresponds to our chosen embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. In addition to the cyclotomic and anticyclotomic $\mathbb{Z}_p$-extensions of K, we may consider the union of ray class fields $K(\mathfrak{p}^n)$ and $K(\overline{\mathfrak{p}}^n)$ to obtain the following $\mathbb{Z}_p$-extensions of K.

Definition 2.4.4. *The $\mathfrak{p}$-ramified $\mathbb{Z}_p$-extension $K^{\mathfrak{p}}$ of K is the unique $\mathbb{Z}_p$-extension of K which is unramified outside of $\mathfrak{p}$. Similarly, the $\overline{\mathfrak{p}}$-ramified $\mathbb{Z}_p$-extension $K^{\overline{\mathfrak{p}}}$ of K is the unique $\mathbb{Z}_p$-extension of K unramified outside of $\overline{\mathfrak{p}}$.*

Note that in general, the intersection of $K^{\mathfrak{p}}$ with the Hilbert class field H_0 of K is not necessarily equal to K. That is, $\mathfrak{p}$ is not necessarily totally ramified in $K^{\mathfrak{p}}/K$ (but of course it is eventually totally ramified). Similarly, $K^{\mathfrak{p}}$ may be not linearly disjoint from $K^{\overline{\mathfrak{p}}}$ over K.

Definition 2.4.5. *Let F/K be a finite abelian extension of number fields, and set $F_\infty = F \cdot K^{\mathfrak{p}}$. The $\mathfrak{p}$-ramified Iwasawa module $\mathfrak{X}_{\mathfrak{p}} = \mathfrak{X}_{\mathfrak{p}}(F)$ of F is the Galois group of the maximal abelian pro-p extension of F_∞ unramified outside of the places dividing $\mathfrak{p}$.*

Let $F_\infty/K^{\mathfrak{p}}$ be a finite extension which is abelian over K. Choose a decomposition

$$\mathrm{Gal}(F_\infty/K) \cong H \times G$$

where $G \cong \mathbb{Z}_p$ and H is a finite abelian group, and define $F_n = F_\infty^{G_n}$ where G_n is the subgroup of G corresponding to $p^n\mathbb{Z}_p$.

Let $\mathfrak{X}_{\mathfrak{p}}$ be the $\mathfrak{p}$-ramified Iwasawa module of F_∞/F_0, and let X_∞ be the unramified Iwasawa module of F_∞/F_0.

For $n \geq 0$, let

$$\mathcal{E}_{F_n} = (\mathcal{O}_{F_n}^\times)_p^\wedge$$

be the p-completion of the global units of F_n, and let

$$\mathcal{U}_{F_n} = \prod_{S_{F_n} \ni v | \mathfrak{p}} \mathcal{O}_{F_n,v}^{\times} \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

be the product of the principal units of $F_{n,v}$ at places $v \mid \mathfrak{p}$, which we call the semi-local principal units of F_n at $\mathfrak{p}$. We define the subgroup of elliptic units $\mathcal{C}_{F_n}$ of $\mathcal{E}_{F_n}$ as in [Ru91, §1], which are roughly special values of certain theta functions at torsion points on an elliptic curve with CM by $\mathcal{O}_K$, and set $\mathcal{E}_\infty = \varprojlim_n \mathcal{E}_{F_n}$, $\mathcal{U}_\infty = \varprojlim_n \mathcal{U}_{F_n}$, and $\mathcal{C}_\infty = \varprojlim_n \mathcal{C}_{F_n}$ where the inverse limits are along norm maps. Class field theory then gives us the well-known sequence of finitely generated $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F_0)]] \cong \Lambda$-modules

$$0 \to \mathcal{E}_\infty/\mathcal{C}_\infty \to \mathcal{U}_\infty/\mathcal{C}_\infty \to \mathfrak{X}_{\mathfrak{p}} \to X_\infty \to 0.$$

Exactness except at the term $\mathcal{E}_\infty/\mathcal{C}_\infty$ is true generally, and that Leopoldt's conjecture holds for abelian extensions of imaginary quadratic fields, proved by Brumer [Br67, Theorem 2'], gives us exactness of the full sequence. Greenberg has shown that Leopoldt's conjecture tells us that $\mathfrak{X}_{\mathfrak{p}}$ is a torsion Λ-module [Gr78, §4], while Λ-torsionness of $\mathcal{E}_\infty/\mathcal{C}_\infty$ and of $\mathcal{U}_\infty/\mathcal{C}_\infty$, which are equivalent, was shown by Rubin in [Ru91] under the hypothesis that $p \nmid [F_0 : K]$ and F_0 contains the Hilbert class field of K, by de Shalit in [dS87, III.1.5] for the case that $F_0 = K(\mathfrak{f})$ is a ray class field of modulus $\mathfrak{f}$, and by Viguié in general in [Vi16, §3]. We now state the $\mathfrak{p}$-ramified main conjecture at the level of generality that we will later need.

Theorem 2.4.6 ([Vi16], [OV16])**.** *Let $\chi \in \widehat{H}$. Then we have an equality of characteristic ideals in $\mathbb{Z}_p[\chi][[T]]$*

$$\mathrm{char}(X_{\infty,\chi}) = \mathrm{char}((\mathcal{E}_\infty/\mathcal{C}_\infty)_\chi) \text{ and } \mathrm{char}(\mathfrak{X}_{\mathfrak{p},\chi}) = \mathrm{char}((\mathcal{U}_\infty/\mathcal{C}_\infty)_\chi).$$

The theorem was proved for $p > 3$ in [Vi16], and the vanishing of the μ-invariant of $\mathfrak{X}_{\mathfrak{p}}$ in the case $p = 3$ proved in [OV16] gives the claim for $p = 3$ as well, as we explain below. We first provide some history of the proof of the theorem. The first steps toward the proof of the main conjecture were made independently by Gillard [Gi85, Théorème 3.4] and Schneps

[Sc85, Theorem IV] in their proofs of the vanishing of the μ-invariant of $\mathfrak{X}_\mathfrak{p}$ for $p \geq 5$. The main conjecture was first proved under the condition that F_0 contains the Hilbert class field H_0 of K and $p \nmid [F_0 : K]$ by Rubin in [Ru91], where he utilized the machinery of Euler systems to obtain the divisibility for each character χ

$$\mathrm{char}(X_{\infty,\chi}) \mid p^k \mathrm{char}((\mathcal{E}_\infty/\mathcal{C}_\infty)_\chi), \tag{2.4.1}$$

for some $k \geq 0$ [Ru91, Theorem 8.3] and used the vanishing of the μ-invariant to conclude

$$\mathrm{char}(X_{\infty,\chi}) \mid \mathrm{char}((\mathcal{E}_\infty/\mathcal{C}_\infty)_\chi).$$

Equality of these divisibilities was then made by appealing to an analytic class number formula proved by Gillard as stated in [Ru91, Theorem 1.3], which made use of the hypothesis that $p \nmid [F_0 : K]$.

Various authors then chipped away at the technical hypotheses made by Rubin by modifying the proofs at the technical core of the Euler system machinery. The first advance was made by Rubin himself in [Ru94], where the condition that $F_0 \supseteq H_0$ was removed. In another direction, Bley in [Bl05], following Greither's treatment of the cyclotomic case over $\mathbb{Q}$, gave a proof of the main conjecture for $p \geq 3$ with $F_0 = K(\mathfrak{f})$ a ray class field and assuming that $p \nmid |\mathrm{Pic}(\mathcal{O}_K)|$, but without the assumption that $p \nmid [F_0 : K]$. In addition to modifying the Euler system machinery, Bley used a result of de Shalit as an alternative to Gillard's class number formula. Precisely, for $F_0 = K(\mathfrak{f})$, de Shalit showed that the sums of the Iwasawa invariants of eigenspaces of $\mathfrak{X}_\mathfrak{p}$ and $\mathcal{U}_\infty/\mathcal{C}_\infty$ coincide [dS87, III.2.1] by using the vanishing of the μ-invariant as proved by Gillard and Schneps [dS87, III.2.12]:

$$\begin{aligned} \sum_\chi \mu(\mathfrak{X}_{\mathfrak{p},\chi}) &= \sum_\chi \mu((\mathcal{U}_\infty/\mathcal{C}_\infty)_\chi), \\ \sum_\chi \lambda(\mathfrak{X}_{\mathfrak{p},\chi}) &= \sum_\chi \lambda((\mathcal{U}_\infty/\mathcal{C}_\infty)_\chi). \end{aligned} \tag{2.4.2}$$

Finally, Viguié in [Vi16] combined the adaptations of [Ru94] and [Bl05] in the general Euler system argument to obtain the divisibility as in equation 2.4.1

$$\mathrm{char}(X_{\infty,\chi}) \mid p^k \mathrm{char}((\mathcal{E}_\infty/\mathcal{C}_\infty)_\chi)$$

for all primes p with $k > 0$ [Vi16, eq. 7.10] and from there used the vanishing of μ-invariants of the Galois-theoretic Iwasawa modules to deduce the main conjecture for primes $p > 3$. For $p = 3$, the vanishing of μ-invariants was later proved by Viguié and Oukhaba in [OV16], and so the main conjecture in that case follows as well.

Remark 2.4.7. There are a few instances in the literature where it seems some authors have invoked Gillard's and Schneps's result on the vanishing of the μ-invariant of $\mathfrak{X}_\mathfrak{p}$ for $p \geq 5$ but yet do not exclude the case $p = 3$ from their discussions. De Shalit's result on the equality of sums of Iwasawa invariants for instance uses this vanishing result in the last step of his argument, yet [dS87, Chapter II] works with $p > 2$ throughout with no further restrictions. This impacts Bley's proof of the main conjecture as well, and in addition Bley cites the vanishing of the μ-invariant [Bl05, Page 78] despite working throughout with $p > 2$.

Rubin also uses Gillard's and Schneps's result in [Ru91, Corollary 9.1] while working generally with $p > 2$, he only needs the result for irreducible $\mathbb{Z}_p$-representations χ which are of "type II" in the sense of [Ru91, §8], which means that $\mu_p \subset F_0$ and $\chi = \widehat{\chi} \otimes \omega$ where ω is the Teichmüller character on $\mathrm{Gal}(F_0/K)$ and $\widehat{\chi}$ is the contragredient representation of χ. The Euler system argument for such representations produces a divisibility as in equation 2.4.1 with $k > 0$, and one relies on the vanishing of μ-invariants to achieve the divisibility desired for the proof of the main conjecture. Additionally, in [Ru94], in modifying the statement and proof of Theorem 8.3 of [Ru91], Rubin classifies also ω as a type II representation. In both cases, it is not clear how to conclude the main theorem without the knowing the vanishing of the μ-invariant for $p = 3$. These issues are of course all resolved by the result of [OV16].

To end this section, we recall the result of de Shalit identifying the characteristic ideal of $(\mathcal{U}_\infty/\mathcal{C}_\infty)_\chi$ with the ideal generated by a p-adic Hecke L-function, the analog of a theorem of Iwasawa for the cyclotomic case over $\mathbb{Q}$.

We continue to work with an odd prime p which splits in an imaginary quadratic K. Recall that a Hecke character of K is a continuous homomorphism η of the idele class group of K

$$\eta : K^\times \backslash \mathbb{I}_K \to \mathbb{C}^\times.$$

The infinity type (k, l) of η is the pair of integers such that for elements $x \in K_\infty^\times \cong \mathbb{C}^\times$ of the archimedean component, one has $\eta(x) = x^{-k}\overline{x}^{-l}$, where the bar indicates complex conjugation, and the conductor $\mathrm{cond}(\eta)$ of η is the smallest modulus of K for which η factors through the associated ray class group. Note that any character of a ray class group may be viewed as a Hecke character of infinity type $(0, 0)$. One may translate from this idelic definition of a Hecke character to an ideal-theoretic definition to obtain a character η^{id} on the group of fractional ideals of $\mathcal{O}_K$ prime to $\mathrm{cond}(\eta)$. Extending η^{id} to be 0 on all ideals not prime to $\mathrm{cond}(\eta)$, we may define the series in the complex variable s whose real part is greater than 1

$$L(\eta, s) = \sum_{\mathfrak{a}} \eta^{\mathrm{id}}(\mathfrak{a})/N(\mathfrak{a})^s,$$

where the sum ranges over all nonzero integral ideals of $\mathcal{O}_K$ and N denotes the ideal norm, and via analytic continuation obtain the Hecke L-function associated with η. We write $L^{(\mathfrak{g})}(\eta, s)$ when we wish to remove Euler factors at primes dividing an integral ideal $\mathfrak{g}$ of $\mathcal{O}_K$. Additionally, when $\mathrm{cond}(\eta)$ divides $\mathfrak{f}\mathfrak{p}^\infty$ for an integral ideal $\mathfrak{f}$ of $\mathcal{O}_K$ which is prime to $\mathfrak{p}$, we denote by $\eta^{\mathfrak{p}} : \mathrm{Gal}(K(\mathfrak{f}\mathfrak{p}^\infty)/K) \to \overline{\mathbb{Q}}_p^\times$ the character satisfying $\eta^{\mathfrak{p}}(\mathrm{Frob}_{\mathfrak{q}}) = \eta^{\mathrm{id}}(\mathfrak{q})$ for any integral ideal $\mathfrak{q}$ prime to $\mathrm{cond}(\eta)\mathfrak{p}$.

Theorem 2.4.8 ([dS87, II.4.12], [Oh20, 1.1.5])**.** *Let $\mathfrak{f}$ be a nontrivial integral ideal of $\mathcal{O}_K$ prime to $\mathfrak{p}$. Then there exist periods $\Omega \in \mathbb{C}^\times$ and $\Omega_p \in \mathbb{C}_p^\times$ and a unique p-adic $\mathcal{O}_{\mathbb{C}_p}$-valued measure $\mu(\mathfrak{f})$ on $\mathrm{Gal}(K(\mathfrak{f}\mathfrak{p}^\infty)/K)$ such that for any Hecke character η of infinity type $(k, 0)$ for some $k \geq 1$ and of conductor dividing $\mathfrak{f}\mathfrak{p}^\infty$, we have*

$$\Omega_p^{-k} \int_{\mathrm{Gal}(K(\mathfrak{f}\mathfrak{p}^\infty)/K)} \eta^{\mathfrak{p}}(\sigma) d\mu(\mathfrak{f}; \sigma) = \Omega^{-k} G(\eta) \left(1 - \frac{\eta^{\mathrm{id}}(\mathfrak{p})}{N(\mathfrak{p})}\right) (k-1)! L^{(\mathfrak{f})}(\eta^{-1}, 0),$$

where $G(\eta)$ is the "like Gauss sum" defined in [dS87, II.2.11].

The measure $\mu(\mathfrak{f})$ is in fact valued in the completion $\widehat{\mathbb{Z}}_p^{\mathrm{ur}}$ of the integer ring of the maximal unramified extension $\mathbb{Q}_p^{\mathrm{ur}}$ of $\mathbb{Q}_p$. We now fix a nontrivial integral ideal $\mathfrak{f}$ prime to $\mathfrak{p}$ and relate the above measure to the $\mathfrak{p}$-ramified main conjecture. We fix a decomposition

$$\mathcal{G}(\mathfrak{f}) := \mathrm{Gal}(K(\mathfrak{f}\mathfrak{p}^\infty)/K) \cong \mathcal{H}(\mathfrak{f}) \times G \tag{2.4.3}$$

where as before, $G \cong \mathbb{Z}_p$ via a fixed choice of topological generator $\gamma_0 \in G$. Let R denote the finite extension of $\widehat{\mathbb{Z}}_p^{\mathrm{ur}}$ given by adjoining the $|\mathcal{H}(\mathfrak{f})|$th roots of unity. For a Hecke character $\chi \in \widehat{\mathcal{H}(\mathfrak{f})}$, let $f_\chi \in R[[T]]$ be the power series corresponding to the image of the measure $\mu(\mathfrak{f})$ along the projection $R[[\mathcal{G}(\mathfrak{f})]] \to R[[G]] \cong R[[T]]$, where the isomorphism is via the usual correspondence $[\gamma_0] - 1 \leftrightarrow T$. As in [dS87, II.4.17], we have:

Corollary 2.4.9 ([Oh20, Corollary 1.1.7])**.** *For a Hecke character η as in Theorem 2.4.8 such that $\eta^{\mathfrak{p}} = \chi \times \eta_\Gamma^{\mathfrak{p}}$ according to the decomposition 2.4.3, we have*

$$f_\eta(\eta_\Gamma^{\mathfrak{p}}(\gamma_0) - 1) = \Omega_p^k \Omega^{-k} G(\eta) \left(1 - \frac{\eta^{\mathrm{id}}(\mathfrak{p})}{N(\mathfrak{p})}\right) (k-1)! L^{(\mathfrak{f})}(\eta^{-1}, 0).$$

Writing $\mathcal{F}_n = K(\mathfrak{f}\mathfrak{p}^n)$, we let $U(\mathcal{F}_n)$ be the semi-local principal units of $\mathcal{F}_n$ at $\mathfrak{p}$ and $C(\mathcal{F}_n)$ the subgroup of elliptic units, and we set $U(\mathcal{F}_\infty) = \varprojlim_n U(\mathcal{F}_n)$ and $C(\mathcal{F}_\infty) = \varprojlim_n C(\mathcal{F}_n)$.

Theorem 2.4.10 ([dS87, III.1.10])**.** *Let $\chi \in \widehat{H}$ be a character with conductor $\mathfrak{g}$ or $\mathfrak{g}\mathfrak{p}$ with $\mathfrak{g}$ prime to $\mathfrak{p}$ and nontrivial. Then we have an equality of ideals in $R[[T]]$*

$$\mathrm{char}(((U(\mathcal{F}_\infty)/C(\mathcal{F}_\infty)) \otimes_{\mathbb{Z}_p} R)_\chi) = (f_\chi).$$

Recall our set-up F_∞/K_∞ in the discussion of the $\mathfrak{p}$-ramified main conjecture, and suppose that $F_0 \subseteq K(\mathfrak{f}\mathfrak{p})$, i.e., that the conductor of F_0/K divides $\mathfrak{f}\mathfrak{p}$. For a character $\chi \in \widehat{H}$ viewed also as a character of $\mathrm{Gal}(K(\mathfrak{f}\mathfrak{p})/K)$ by inflation, we have a map induced by the norm map from $K(\mathfrak{f}\mathfrak{p})$ to F_0

$$((U(\mathcal{F}_\infty)/C(\mathcal{F}_\infty)) \otimes_{\mathbb{Z}_p} R)_\chi \to ((\mathcal{U}_\infty/\mathcal{C}_\infty) \otimes_{\mathbb{Z}_p} R)_\chi$$

which is a pseudo-isomorphism as we know the μ-invariants of both items vanish. The following corollary follows from the above theorem and Theorem 2.4.6.

Corollary 2.4.11. *Let $\chi \in \widehat{H}$ be a character with conductor $\mathfrak{g}$ or $\mathfrak{g}\mathfrak{p}$ with $\mathfrak{g}$ prime to $\mathfrak{p}$ and nontrivial. Then the characteristic ideal in $R[[T]]$ of $(\mathfrak{X}_{\mathfrak{p}} \otimes_{\mathbb{Z}_p} R)_\chi$ is generated by f_χ.*

CHAPTER 3

Modular curves and modular and Λ-adic forms

In this chapter, we first define the modular curves $X_1(M)$ and $X_1^{\mu}(M)$ as schemes representing moduli problems on the category of (generalized) elliptic curves. We go into more detail than is truly needed for our intended applications, but as conventions seem to vary from paper to paper in the literature surrounding Sharifi's conjecture, we opt to be fastidious for our own sake and for posterity. We also give a short description of Ihara's twist of the modular curve $X(M)_{\mathbb{F}_{q^2}}$ and state Ihara's theorem characterizing the family of such twists for varying M and a fixed prime q, which is Theorem 3.1.5 below. This theorem is used to prove surjectivity of Υ in Chapter 4.

We then define modular forms as sections of certain invertible sheaves on these modular curves and define Hecke operators and algebras via algebraic correspondences on these modular curves. Finally, we define Λ-adic forms as certain power series that specialize to classical modular forms and relate spaces of Λ-adic forms to inverse limits of spaces of classical forms, following [Oh95].

3.1 Modular curves

In this section, we define modular curves as representing objects for certain moduli problems of generalized elliptic curves with level structure. The theory has been thoroughly developed in the standard references [DR73], [KM85], and [Co07], and we summarize the needed results and references here while making an attempt to follow their notation and terminology for ease of reference. However, while [DR73] and [Co07] freely use the language of stacks, we will avoid doing so here, though it is arguably the more natural setting in which to work.

3.1.1 Moduli problems

The classical theory of moduli spaces of elliptic curves typically starts with the consideration of quotients of the upper half complex plane $\mathcal{H}$ by the action of a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ by fractional linear transformations to produce a non-compact Riemann surface which admits an analytic compactification, and proceeds by demonstrating that the moduli space of elliptic curves with level M level structure for large enough M can in fact be represented by a smooth affine scheme over $\mathbb{Q}$, or even over $\mathbb{Z}[1/M]$. From here, there are two directions for improvement in the algebraic story: one is to "compactify" the affine moduli scheme over $\mathbb{Z}[1/M]$ to a proper moduli scheme (i.e., a proper scheme with a moduli theoretic interpretation of its points) which recovers the compact Riemann surface upon analytification, and the other is to extend the moduli scheme to one over $\mathbb{Z}$. The three texts above each make progress in realizing these goals.

The book [DR73] introduced the notion of Néron polygons and generalized elliptic curves, which can be viewed as certain "stable" degenerations (or "semistable" in modern terminology) of genuine elliptic curves, and showed that there exist proper moduli schemes over $\mathbb{Z}[1/M]$ extending the affine schemes from the paragraph above. Additionally, they showed these schemes admit finite flat maps to the localization away from M of the moduli stack $\mathcal{M}_{1,1}$ over $\mathbb{Z}$ of genus 1 curves with a marked point, and so by normalization produced proper schemes over $\mathbb{Z}$, but with no modular interpretation in bad characteristics. In the other direction, the book [KM85] developed the notion of Drinfeld level structures on elliptic curves, which was originally considered by Serre, which essentially tracks the data of the Cartier divisor associated with a subgroup scheme rather than the subgroup scheme itself, and showed that one could produce normal affine moduli schemes over $\mathbb{Z}$. These schemes also admit finite flat morphisms to the j-line $\mathbb{A}^1_{\mathbb{Z}}$, and so by normalization of $\mathbb{P}^1_{\mathbb{Z}}$, one obtains proper flat schemes over $\mathbb{Z}$, but with no modular interpretation of the cusps. Finally, Conrad in [Co07] combined the two approaches and considered Drinfeld level structures on generalized elliptic curves and produced proper flat moduli schemes over $\mathbb{Z}$ and showed that for large enough M, they agreed with the proper $\mathbb{Z}$-schemes of [DR73] and [KM85]. Below, we introduce some of the moduli problems and modular curves that will be used in this dissertation combining the terminology and notation of each of the three standard references, though we do not attempt to be completely thorough; this section is meant to record basic facts that are scattered throughout the literature.

Recall that an elliptic curve over a scheme S is the data of a smooth, proper scheme $E \to S$ of pure relative dimension 1 whose geometric fibers are connected genus 1 curves, together with a section $0 \in E(S)$. There is then a unique commutative group scheme structure on E/S in which 0 is the identity element [KM85, Ch. 2].

A Néron n-gon $C_{n,S}$ over S for a positive integer n is the quotient of n copies of $\mathbb{P}^1_S$ indexed by $i \in \mathbb{Z}/n\mathbb{Z}$, which we may denote $\mathbb{P}^1_S \times \underline{\mathbb{Z}/n\mathbb{Z}}_S$, given by identifying the 0 section of the ith copy of $\mathbb{P}^1_S$ with the ∞ section of the $(i+1)$th copy. The smooth locus $C^{\mathrm{sm}}_{n,S}$ is then isomorphic to $\mathbb{G}_{m,S} \times \underline{\mathbb{Z}/n\mathbb{Z}}_S$, which we give its usual S-group scheme structure $+$. Consider $S = \mathrm{Spec}(\mathbb{Z})$, and write C_n for $C_{n,\mathrm{Spec}(\mathbb{Z})}$. The functor $\mathrm{Aut}(C_n, +)$ of $+$-preserving automorphisms of C_n which sends a scheme S to the group $\mathrm{Aut}(C_{n,S}, +)$ can be identified with the $\mathbb{Z}$-group scheme $\underline{\mathbb{Z}/2\mathbb{Z}}_{\mathbb{Z}} \times \mu_{n,\mathbb{Z}}$ where the involution $1 \in \mathbb{Z}/2\mathbb{Z}$ sends $(x, i) \in C^{\mathrm{sm}}_{n,S}(S)$ to $(x^{-1}, -i)$ and an element $\zeta \in \mu_{n,\mathbb{Z}}(S)$ sends (x, i) to $(\zeta^i x, i)$ [DR73, II.1.10], [Ce17, 2.1.6].

A generalized elliptic curve over S is the data of a flat, proper, finitely presented scheme $E \to S$ whose smooth geometric fibers are elliptic curves and whose non-smooth geometric fibers are Néron polygons, together with a section $0 \in E(S)$ and an S-morphism

$$+ : E^{\mathrm{sm}} \times_S E \to E$$

that restricts to give a commutative S-group scheme structure on the smooth locus E^{sm} such that on any non-smooth geometric fiber $C_{\overline{s}}$ of E, for any given rational point $x \in C^{\mathrm{sm}}_{\overline{s}}(\overline{s})$, the translation action on $C_{\overline{s}}^{\mathrm{sm}}(\overline{s})$ given by $y \mapsto y + x$ induced by $+$ induces a rotation on the irreducible components of $C_{\overline{s}}^{\mathrm{sm}}$. See [DR73, II.1] for a thorough discussion on generalized elliptic curves.

We begin with a definition of certain "Drinfeldian" level structures on generalized elliptic curves, following [Co07].

Definition 3.1.1. *Let $E \to S$ be a generalized elliptic curve, and let M be a positive integer.*

(i) A $\Gamma(M)$-structure on E is a homomorphism

$$\phi : (\mathbb{Z}/M\mathbb{Z})^2 \to E^{\mathrm{sm}}[M]$$

which induces an equality of relative effective Cartier divisors of E^{sm}/S

$$E^{\mathrm{sm}}[M] = \sum_{(a,b)\in(\mathbb{Z}/M\mathbb{Z})^2} [\phi(a,b)]$$

such that the divisor intersects each irreducible component of each geometric fiber nontrivially.

(ii) A $\Gamma_1(M)$-structure on E is a homomorphism

$$\phi : \mathbb{Z}/M\mathbb{Z} \to E^{\mathrm{sm}}[M]$$

such that the relative effective Cartier divisor of E^{sm}/S it generates

$$\sum_{a\in\mathbb{Z}/M\mathbb{Z}} [\phi(a)]$$

is a subgroup scheme of $E^{\mathrm{sm}}[M]$ such that the divisor intersects each irreducible component of each geometric fiber nontrivially.

(iii) A $\Gamma_1^{\mu}(M)$-structure on E is a closed immersion of S-group schemes

$$\phi : \mu_{M,S} \to E^{\mathrm{sm}}[M]$$

which intersects every irreducible component of each geometric fiber nontrivially.

If S is a $\mathbb{Z}[1/M]$-scheme, then a $\Gamma(M)$-structure on E is the same as an isomorphism of S-group schemes $\underline{(\mathbb{Z}/M\mathbb{Z})^2}_S \xrightarrow{\cong} E^{\mathrm{sm}}[M]$, and a $\Gamma_1(M)$-structure is closed immersion of S-group schemes $\underline{\mathbb{Z}/M\mathbb{Z}}_S \hookrightarrow E^{\mathrm{sm}}[M]$ [KM85, 1.5.3]. Additionally, if E is a genuine elliptic curve, then the condition of intersecting each irreducible component of each geometric fiber is automatically satisfied, and these definitions then agree with those of [KM85, Ch.3] and [KM85, 4.9].

Let (GEll) be the category whose objects are generalized elliptic curves $E \to S$ and whose morphisms are Cartesian squares

$$\begin{array}{ccc} E' & \longrightarrow & E \\ \downarrow & & \downarrow \\ S' & \longrightarrow & S \end{array}$$

which induce isomorphisms of generalized elliptic curves $E' \cong E \times_S S'$ over S', and let (Ell) be the full subcategory whose objects are elliptic curves $E \to S$. For any scheme T, let (GEll/T) denote the full subcategory of (GEll) whose objects are E/S where S is a T-scheme. If R is a commutative ring, we write (GEll/R) in place of (GEll/Spec(R)). We define (Ell/T) and (Ell/R) similarly.

Definition 3.1.2. *Let M be a positive integer. Let $[\Gamma_*^?(M)] : (\mathrm{GEll}) \to Set$ denote the moduli problem which assigns to each generalized elliptic curve $E \to S$ the set of $\Gamma_*^?(M)$-structures of E/S, where "$*$" is either empty or 1, and "?" is empty if $*$ is empty, and is empty or μ otherwise.*

Let *Sch* denote the category of schemes (we do not worry about set-theoretic issues). We may alternatively consider the moduli problem $X_*^?(M)$ (resp. $Y_*^?(M)$) which assigns to $S \in Sch$ the set of S-isomorphism classes of pairs (E, ϕ) where E/S is a generalized elliptic curve (resp. elliptic curve) and ϕ is a $\Gamma_*^?(M)$-level structure on E/S. If $[\Gamma_*^?(M)]$ is represented by $\mathcal{E}/\mathcal{M}$, then $\mathcal{M}$ represents the corresponding moduli problem on *Sch* and vice versa if $[\Gamma_*^?(M)]$ is rigid, i.e., if there are no nontrivial S-automorphisms of (E, ϕ) for E/S a generalized elliptic curve (resp. elliptic curve) and ϕ a $\Gamma_*^?(M)$-level structure for all such

(E, ϕ) and S [KM85, 4.4, A.4.1.2].

We have the following representability results, where in what follows we take a curve over a base scheme to mean an integral scheme which is flat, separated, and finitely presented of pure relative dimension 1 over the base.

Theorem 3.1.3 ([DR73, KM85, Co07, Ce17])**.**

(i) If $d \mid M$ and $d \geq 3$, then $[\Gamma(M)]$ on $(\mathrm{GEll}/\mathbb{Z}[1/d])$ and its restriction to $(\mathrm{Ell}/\mathbb{Z}[1/d])$ are represented respectively by

$$\overline{E}(M)_{\mathbb{Z}[1/d]}/X(M)_{\mathbb{Z}[1/d]} \quad \text{and} \quad E(M)_{\mathbb{Z}[1/d]}/Y(M)_{\mathbb{Z}[1/d]}$$

where $X(M)_{\mathbb{Z}[1/d]}$ is a projective, regular curve over $\mathbb{Z}[1/d]$ which is smooth over $\mathbb{Z}[1/M]$ and $Y(M)_{\mathbb{Z}[1/d]}$ is an affine, regular curve over $\mathbb{Z}[1/d]$ which is an open subscheme of $X(M)_{\mathbb{Z}[1/d]}$. In particular, if M is not of the form p^s or $2p^s$ for some prime p and $s \in \mathbb{Z}_{\geq 0}$, then $X(M)$ exists as a projective, regular curve over $\mathbb{Z}$.

(ii) If $d \mid M$, then $[\Gamma_1(M)]$ on $(\mathrm{GEll}/\mathbb{Z}[1/d])$ for $d \geq 5$ and its restriction to $(\mathrm{Ell}/\mathbb{Z}[1/d])$ for $d \geq 4$ are represented respectively by

$$\overline{E}_1(M)_{\mathbb{Z}[1/d]}/X_1(M)_{\mathbb{Z}[1/d]} \quad \text{and} \quad E_1(M)_{\mathbb{Z}[1/d]}/Y_1(M)_{\mathbb{Z}[1/d]},$$

where $X_1(M)_{\mathbb{Z}[1/d]}$ is a proper, regular curve over $\mathbb{Z}[1/d]$ which is smooth over $\mathbb{Z}[1/M]$, and $Y_1(M)_{\mathbb{Z}[1/d]}$ is an affine, regular curve over $\mathbb{Z}[1/d]$, which is an open subscheme of $X_1(M)_{\mathbb{Z}[1/d]}$. In particular, if M is not of the form p^s, $2p^s$, or $3p^s$ for p a prime and $s \in \mathbb{Z}_{\geq 0}$, then $Y_1(M)$ exists as a affine, regular curve over $\mathbb{Z}$, and if additionally M is not of the form $4p^s$, then $X_1(M)$ exists as a proper, regular curve over $\mathbb{Z}$.

(iii) The moduli problem $[\Gamma_1^\mu(M)]$ on (GEll) for $M \geq 5$ and its restriction to (Ell) for $M \geq 4$ is represented by $\overline{E}_1^\mu(M)/X_1^\mu(M)$ and $E_1^\mu(M)/Y_1^\mu(M)$, where $X_1^\mu(M)$ is a smooth curve over $\mathbb{Z}$ with geometrically irreducible fibers which is moreover proper over $\mathbb{Z}[1/M]$, and $Y_1^\mu(M)$ is a smooth curve over $\mathbb{Z}$ which is an affine open subscheme of $X_1^\mu(M)$.

Proof. We of course only indicate where to locate these statements in the standard references.

(i) The claim of regularity of $X(M)_{\mathbb{Z}[1/d]}$ is [Ce17, Theorems 4.3.5, 4.5.1] or [Co07, Theorem 4.1.1]. The claim of smoothness away from M is [Co07, Theorem 3.2.7] or [Ce17, Proposition 4.3.2, Theorem 4.5.1]. The representability and projectivity claims are in [Co07, Theorem 4.2.1] and [Ce17, Proposition 4.3.6], though the statement in the latter has a typo as it fails to exclude the exponent $s = 0$. We remark that for the moduli problem on (GEll/$\mathbb{Z}[1/M]$), representability, smoothness, and projectivity is given in [DR73, IV.2.9].

We additionally indicate how the proof of representability goes for the moduli problem on (Ell), as it follows from results in the more classical reference [KM85]. First, on the elliptic curve locus, the moduli problem factors into corresponding moduli problems for the prime factors of M [KM85, 3.5.1] (this is not true for the full problem on (GEll) [Ce17, Example 4.5.3]). For a general M, the problem $[\Gamma(M)]$ on (Ell/$\mathbb{Z}[1/M]$) is relatively representable, finite, and étale [KM85, 5.1.1], and if $M \geq 3$, then it is rigid by [KM85, 2.7.2] (using that Drinfeldian level structures reduce to the classical level structures of [KM85, 2.7] if M is invertible). Thus, by [KM85, 4.7.0], it is representable, and by [KM85, 4.7.1], $Y(M)_{\mathbb{Z}[1/M]}$ has the claimed properties (the proof there works with (Ell/$\mathbb{Z}[1/M]$) in place of (Ell)). Finally, looking at prime factorizations and using that the product of a representable moduli problem with a relatively representable moduli problem is representable [KM85, 4.3.4] gives the claim of the theorem. In the cases $M = p^s$ and $M = 2p^s$, for a supersingular elliptic curve E over $\mathbb{F}_p$, one has the nontrivial automorphism -1 of (E, ϕ).

(ii) The representability claim follows from [Co07, 4.2.1], and the result for $Y_1(M)$ can be deduced from [KM85, 5.1.1, 2.7.4, 4.7.0, 4.7.1, 4.3.4, 3.5.1] just as above. Regularity and smoothness away from M are again [Co07, 3.2.7, 4.1.1], and projectivity follows from [Ce17, 4.1.3, 4.5.1]. Additionally, that $[\Gamma_1(4)]$ is not representable over $\mathbb{Z}[1/2]$ is due to [Co07, 2.2.5] and the fact that the data $(C_{2,\mathbb{Z}[\mu_4,1/2]}, \phi)$ of a Néron 2-gon $C_{2,\mathbb{Z}[\mu_4,1/2]}$ with any $\Gamma_1(4)$-structure ϕ admits a nontrivial involution.

(iii) The affine case follows from [KM85, 4.9, 4.10, 2.7.4]. The moduli problem on (GEll) has trivial automorphism groups for $M \geq 5$ by [KM85, 2.7.4] and [Ce17, 2.1.6], but there seems to be no prominent reference in the literature which gives details on the geometric properties of $X_1^{\mu}(M)$, though $\mathbb{Z}$-smoothness and $\mathbb{Z}[1/M]$-properness is claimed in [DI95, 9.3.7], which cites [Ka76, II.2.5], where such properties are only claimed for the affine curve $Y_1^{\mu}(M)$.

□

For the case of problematic M, one can still form so-called coarse moduli schemes as the moduli problems above are relatively representable and affine: in [KM85, 8.1], it is explained that any relatively representable affine moduli problem has an associated coarse moduli scheme; in [DR73, I.8, Ch 8], it is explained that any algebraic stack (with quasicompact and separated diagonal) that is separated and finite type over a Noetherian base admits a coarse moduli algebraic space, and that if the stack is Deligne-Mumford, then the coarse algebraic space is a scheme (see [Co05] for a proof and removal of the Noetherian hypothesis). Both the "fine" moduli schemes representing the moduli problems in the above theorem and the coarse moduli schemes will be referred to as modular curves.

The modular curves of primary interest for us are the curves $X_1^?(M)$, where ? is either empty or μ, and where we have dropped the subscript indicating the base ring of definition. For the purposes of Sharifi's conjecture, the differences between the two curves are essentially cosmetic - there are only slight differences in the description of the Hecke actions and Galois actions on the étale cohomology groups of these modular curves. We explain now the two ways in which these curves are isomorphic after a possible extension of scalars.

Suppose M is such that the fine moduli scheme $X_1(M)$ exists, and let $R = \mathbb{Z}[1/M, \zeta_M]$. As M is invertible in R, we then interpret the moduli problem $[\Gamma_1(M)]$ on Sch as parametrizing pairs $(E/S, \beta)$ where β is the morphism of group schemes associated with the data $(E/S, \phi)$ as in the discussion after Definition 3.1.2. We have an isomorphism $f : \mu_{M,R} \to \underline{\mathbb{Z}/M\mathbb{Z}}_R$ over R given by sending ζ_M to 1, and so we obtain an isomorphism $v_M : X_1^\mu(M)_R \to X_1(M)_R$ induced by the map of moduli problems described by

$$(E/S, \beta : \mu_S \hookrightarrow E^{\mathrm{sm}}[M]) \mapsto (E/S, \beta \circ f_{/S}).$$

If we instead work over $R = \mathbb{Z}[1/M]$, we have the Atkin-Lehner isomorphism $w_M : X_1^\mu(M)_R \to X_1(M)_R$ defined via the morphism of moduli problems on the elliptic curve locus

$$(E/S, \alpha : \mu_{M,S} \hookrightarrow E) \mapsto (\overline{E} := E/\mathrm{im}(\alpha), \beta : \underline{\mathbb{Z}/M\mathbb{Z}}_S \hookrightarrow \overline{E})$$

where β is the unique inclusion such that, over any ring containing a primitive Mth root of unity, $\beta(1)$ and $\alpha(\zeta)$ pair to ζ under the Weil pairing for all Mth roots of unity ζ. A description of this scheme-theoretic Weil pairing is given in [KM85, 2.8] and [KM85, IV.3.21]. We then have that $v_M^{-1} \circ w_M$ and $w_M \circ v_M^{-1}$ are involutions over $\mathbb{Z}[\mu_M, 1/M]$, which we will refer to as Atkin-Lehner involutions.

Remark 3.1.4. There is a mistake in [FK12, 1.4.2] as they claim w_M defines an isomorphism over $\mathbb{Z}$; this is impossible as $X_1^\mu(M)$ is smooth over $\mathbb{Z}$, while if $M = p^k M'$ for p an odd prime, $k \geq 1$, $M' \geq 5$, and $p \nmid M'$ then the fibers over p of $Y_1(M)_{\mathbb{Z}_{(p)}}$ are known to be singular [KM85, 13.5].

It will also be useful to relate these isomorphisms to the analytic theory of modular curves. Recall that $\mathcal{H}$ denotes the complex upper half plane, and let $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1_{\mathbb{Q}}$ be the extended upper half plane. Let $M \geq 5$, let $\Gamma_1(M)$ denote the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of matrices that are unipotent modulo M, and consider the compact Riemann surface $\Gamma_1(M)\backslash\mathcal{H}^*$. Recall that a model of $\Gamma_1(M)\backslash\mathcal{H}^*$ in the sense of [Sh59, 16.7] is the data (V, φ) of a smooth projective curve V over a number field, together with an isomorphism $\varphi : \Gamma_1(M)\backslash\mathcal{H}^* \to V(\mathbb{C})^{\mathrm{an}}$ where $(-)^{\mathrm{an}}$ denotes the analytification functor of Serre's GAGA. For the curves $X_1(M)_{\mathbb{Q}}$ and $X_1^\mu(M)_{\mathbb{Q}}$, we have the two models of $\Gamma_1(M)\backslash\mathcal{H}^*$ induced by

$$\varphi_M : \Gamma_1(M)\backslash\mathcal{H} \ni z \mapsto (\mathcal{H}/(\mathbb{Z}+z\mathbb{Z}), 1 \mapsto 1/M)$$
$$\varphi_M^\mu : \Gamma_1(M)\backslash\mathcal{H} \ni z \mapsto (\mathcal{H}/(\mathbb{Z}+z\mathbb{Z}), \zeta_M \mapsto 1/M).$$

The isomorphism v_M then induces an isomorphism of models over $\mathbb{Q}(\zeta_M)$, while w_M does not induce an isomorphism of models but instead corresponds to the involution $z \mapsto \frac{-1}{Mz}$ of $\mathcal{H}^*$. This may be seen from calculating that for the elliptic curve $\mathcal{H}/(\mathbb{Z}+z\mathbb{Z})$, the M-torsion point $1/M$ pairs with the point z/M of $\mathcal{H}/(\frac{1}{M}\mathbb{Z}+z\mathbb{Z})$ to $e^{2\pi i/M}$ under the Weil pairing and using that $\frac{1}{M}\mathbb{Z}+z\mathbb{Z}$ is homothetic to $\mathbb{Z}+\frac{-1}{Mz}\mathbb{Z}$, where the minus sign is introduced so that $\frac{-1}{Mz}$ is in $\mathcal{H}$. The points $\infty, 0 \in \mathbb{P}^1_{\mathbb{Q}}$ give rise to distinct points in $X_1^\mu(M)_{\mathbb{Q}}$ and in $X_1(M)_{\mathbb{Q}}$, which are respectively referred to as the ∞ and 0 cusps, and which are swapped by the map w_M. We have that in the $X_1(M)$ model, the ∞ cusp has residue field $\mathbb{Q}(\mu_M)^+$, while in the $X_1^\mu(M)$ model, the ∞ cusp has residue field $\mathbb{Q}$; these claims follow from Proposition 3.2.10 below. After introducing Hecke and diamond operators in the next section, we will explain how these isomorphisms interact with the Galois and Hecke actions on the cohomology groups of the two models of modular curves.

3.1.2 Ihara's model of $X(M)_{\mathbb{F}_{q^2}}$

We describe a particular twist $X(M)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}}$ of the curve $X(M)_{\mathbb{F}_{q^2}}$, where q is a prime not dividing M and $\mathbb{F}_{q^2}$ is the finite field of order q^2. For a fixed q, the family of curves $\{X(M)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}}\}_M$ was studied in the paper [Ih75] of Ihara in which he used the congruence subgroup property of $\mathrm{PSL}_2(\mathbb{Z}_{(q)})$ to describe the ramification and splitting behavior of this family of coverings. Though this paper is well-known for being the source of what is now called Ihara's Lemma, which was named by Ribet is his study of level-raising congruences of modular forms, we will only need to use the following formulation of the main theorem of the paper.

Theorem 3.1.5 ([Ih75, MT 2]). *There is no nontrivial finite abelian covering $Y \to X(M)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}}$ by a geometrically irreducible, smooth, proper curve Y over $\mathbb{F}_{q^2}$ in which all supersingular* *points of* $X(M)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}}$ *are completely split.*

Here, we say that a point x of $X(M)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}}$ is completely split if the fiber of x along the covering map $Y \to X(M)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}}$ is a disjoint union of copies of the residue field of x.[1] We also point out that for a smooth curve, connectedness is equivalent to irreducibility; this assumption is to rule out uninteresting covers which on the function field side correspond to extensions $K(Y)/K(X(M)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}})$ such that $\mathbb{F}_{q^2}$ is not algebraically closed in $K(Y)$.

The curves $X(M)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}}$ are essentially constructed by forcing the q^2-power Frobenius to act rationally as $\pm p$ on the universal elliptic curve so that the corresponding supersingular elliptic points are defined over $\mathbb{F}_{q^2}$. We do this as follows.

The curve $X(M)_{\mathbb{Z}[1/M]}$ admits a map via the Weil pairing to the scheme of primitive M-roots of unity $\mu^{\mathrm{prim}}_{N,\mathbb{Z}[1/M]} = \mathrm{Spec}(\mathbb{Z}[1/M][X]/(\Phi_M(X))) \subset \mathrm{Spec}(\mathbb{Z}[1/M][X]/(X^M - 1)) = \mu_{M,\mathbb{Z}[1/M]}$ where $\Phi_M(X)$ is the Mth cyclotomic polynomial, over which the curve $X(M)_{\mathbb{Z}[1/M]}$ is fiberwise geometrically connected. There is a natural left action of $\mathrm{PGL}_2(\mathbb{Z}/M\mathbb{Z})$ on $X(M)_{\mathbb{Z}[1/M]}$ over $\mathbb{Z}[1/M]$ which on points (E, P, Q) corresponds to left matrix multiplication on $\binom{P}{Q}$. The action of a $\gamma \in \mathrm{PGL}_2(\mathbb{Z}/M\mathbb{Z})$ on $X(M)_{\mathbb{Z}[1/M]}$ commutes with the action of $\det(\gamma) \in (\mathbb{Z}/M\mathbb{Z})^\times \cong \mathrm{Aut}(\mu^{\mathrm{prim}}_{M,\mathbb{Z}[1/M]})$ on $\mu^{\mathrm{prim}}_{M,\mathbb{Z}[1/M]}$:

$$\begin{tikzcd} X(M)_{\mathbb{Z}[1/M]} \arrow[r, "\gamma"] \arrow[d] & X(M)_{\mathbb{Z}[1/M]} \arrow[d] \\ \mu^{\mathrm{prim}}_{M,\mathbb{Z}[1/M]} \arrow[r, "\det(\gamma)"] & \mu^{\mathrm{prim}}_{M,\mathbb{Z}[1/M]}. \end{tikzcd}$$

Fixing a choice ζ_M of a primitive Mth root of unity, we have an isomorphism

$$\mathrm{Spec}(\mathbb{Z}[1/M, \zeta_M]) \cong \mu^{\mathrm{prim}}_{N,\mathbb{Z}[1/M]}$$

along which we pull back $X(M)_{\mathbb{Z}[1/M]}$ to obtain the curve $X(M)^{(\zeta_M)}_{\mathbb{Z}[1/M,\zeta_M]}$. We fix a choice of

[1]The terminology Ihara uses is "decomposed completely", not to be confused with the notion of "completely decomposed" as used by Nisnevich in a different but similar sense.

prime of $\mathbb{Z}[1/M, \zeta_M]$ lying over q and consider the reduction

$$X(M)^{(\zeta_M)}_{\mathbb{F}_{q^f}} \to \mathrm{Spec}(\mathbb{F}_{q^f}) = \mathrm{Spec}(\mathbb{F}_q(\zeta_M))$$

where the integer f is the smallest positive integer such that $M \mid q^f - 1$. The subgroup of matrices $G \leqslant \mathrm{PGL}_2(\mathbb{Z}/M\mathbb{Z})$ with determinant a power of q mod N then act on $X(M)^{(\zeta_M)}_{\mathbb{F}_{q^f}}$ over $\mathbb{F}_q$. Let σ_{q^2} denote the arithmetic q^2-power Frobenius of $\mathbb{F}_{q^{2f}}$ and let $g = \left(\begin{smallmatrix} q & 0 \\ 0 & q \end{smallmatrix}\right) \in G$. Then $g \times \mathrm{Spec}(\sigma q^2)$ acts on $X(M)^{(\zeta_M)}_{\mathbb{F}_{q^f}} \times_{\mathrm{Spec}(\mathbb{F}_{q^f})} \mathrm{Spec}(\mathbb{F}_{q^{2f}})$ over $\mathrm{Spec}(\mathbb{F}_{q^2})$ with order f.

Definition 3.1.6. *Define Ihara's curve of level M over $\mathbb{F}_{q^2}$ to be the quotient*

$$X(M)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}} = (X(M)^{(\zeta_M)}_{\mathbb{F}_{q^f}} \times_{\mathrm{Spec}(\mathbb{F}_{q^f})} \mathrm{Spec}(\mathbb{F}_{q^{2f}}))/\langle(g, \mathrm{Spec}(\sigma_{q^2}))\rangle.$$

One important feature of the curves is that the supersingular points of $X(M)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}}$ (i.e., those that are in the image of the supersingular points of $X(M)^{(\zeta_M)}_{\mathbb{F}_{q^{2f}}}$ under the defining quotient map) are all defined over $\mathbb{F}_{q^2}$ [Ih75, 1.3.1]. We will use both this property and Theorem 3.1.5 with $q \equiv \pm 1 \pmod{M}$, so that $X(M)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}} = X(M)^{(\zeta_M)}_{\mathbb{F}_{q^2}}$, in our analysis of the map Υ to be defined in the next chapter.

3.1.3 Degeneracy morphisms

For future use, we also define degeneracy maps $\pi_d : X_1(M) \to X_1(M')$ for each divisor $d \mid M$ such that $dM' \mid M$ which on $Y_1(M)$ are given by

$$\pi_d : (E/S, \alpha : \underline{\mathbb{Z}/M\mathbb{Z}}_S \to E[M]) \mapsto (E', \alpha' : \underline{\mathbb{Z}/M'\mathbb{Z}}_S \to E'[M/d])$$

where $E' := E/\alpha(\frac{M}{d}\mathbb{Z}/M\mathbb{Z})$ and α' is the composition

$$\alpha' := \underline{\mathbb{Z}/M'\mathbb{Z}}_S \hookrightarrow \underline{\mathbb{Z}/(M/d)\mathbb{Z}}_S \xrightarrow{\alpha \bmod \alpha(\frac{M}{d}\mathbb{Z}/M\mathbb{Z})} E'[M/d].$$

We may also define $\pi^\mu_d : X^\mu_1(M) \to X^\mu_1(M')$ which on $Y^\mu_1(M)$ is given by

$$\pi^\mu_d : (E/S, \beta : \mu_{M,S} \hookrightarrow E[M]) \mapsto (E' := E/\beta(\mu_{d,S}), \beta' : \mu_{M',S} \hookrightarrow E'[M'])$$

where

$$\beta' := \mu_{M',S} \hookrightarrow \mu_{M/d,S} \xrightarrow{\beta \bmod \beta(\mu_d)} E'[M'].$$

Over the appropriate extension of scalars, we then have that $\pi_d \circ w_M = w_{M'} \circ \pi^{\mu}_{M/dM'}$, and if we define v_M and $v_{M'}$ as above using a primitive Mth root of unity ζ_M and set $\zeta_{M'} := \zeta_M^{M/M'}$, then we have $\pi_d \circ v_M = v_{M'} \circ \pi^{\mu}_d$. Combining these, we have $\pi^{\mu}_d \circ v_M^{-1} \circ w_M = v_{M'}^{-1} \circ w_{M'} \circ \pi^{\mu}_{M/dM'}$.

3.2 Algebraic theory of Hecke algebras and modular forms

In this section, we set up the algebraic theory of Hecke operators and modular forms due to Igusa and Deligne, following roughly the presentations of [De69] and [Co07]. We start with defining Hecke correspondences, which will enable us to describe Hecke operators as associated endomorphisms of cohomology groups of certain sheaves on modular curves. We then define modular forms as global sections of certain line bundles on modular curves and compare this definition with another algebraic definition of modular forms due to Katz in [Ka72] and the analytic theory of modular forms. We will see that there are some subtleties in the algebraic theory over $\mathbb{Z}$ that arise from the difference in properties of the two models $X_1(M)$ and $X_1^{\mu}(M)$. We assume throughout that the level M is large enough so that we work with moduli problems representable by schemes.

We start with a definition.

Definition 3.2.1. *For a regular proper curve X over an affine scheme $S = \operatorname{Spec}(R)$, a correspondence $T := (\pi_1, \pi_2)$ on X is a pair of finite morphisms $\pi_1, \pi_2 : Y \rightrightarrows X$ from a regular proper curve Y over S. The dual correspondence of T is the correspondence $T^* := (\pi_2, \pi_1)$.*

To define our Hecke correspondences, we first need the modular curve $X_1(M, l)$ defined via another moduli problem on (GEll). Due to the number of technical details needed to define the moduli problem, we only summarize the most pertinent parts of the definition and refer to [Co07, 2.4.3] and [Ce17, 4.6] for more precise definitions.

For M a positive integer and l any prime, let $[\Gamma_1(M,l)]$ be the moduli problem on (GEll) which assigns to E/S the set of data $(E/S, \alpha : \underline{\mathbb{Z}/M\mathbb{Z}} \to E^{\mathrm{sm}}[M], C)$ where α is in $[\Gamma_1(M)](E/S)$ and C is a finite, locally free rank l cyclic S-subgroup scheme of $E^{\mathrm{sm}}[l]$ such that when $l \mid M$, there is an equality of closed subschemes

$$\sum_{a \in \mathbb{Z}/l\mathbb{Z}} (\alpha(aM/l) + C) = E^{\mathrm{sm}}[l]$$

in E. By [Co07, 4.2.1], we have criteria on M for representability of $[\Gamma_1(M,l)]$ which agree with that for $[\Gamma_1(M)]$ in Theorem 3.1.3. In such cases, we denote the corresponding proper modular curve by $X_1(M,l)/\mathbb{Z}$, which is smooth over $\mathbb{Z}[1/Ml]$ by [Co07, 3.2.7].

Let $M \geq 1$ be such that $X_1(M)$ exists as a fine moduli scheme over $\mathbb{Z}$, and let l be any prime. Let $\pi_1^{(l)}, \pi_2^{(l)} : X_1(M,l) \rightrightarrows X_1(M)$ be the morphisms induced by the maps of moduli problems

$$\pi_1^{(l)} \colon (E/S, \alpha : \underline{\mathbb{Z}/M\mathbb{Z}}_S \to E[M], C) \mapsto (E/S, \alpha : \underline{\mathbb{Z}/M\mathbb{Z}}_S \to E[M])$$
$$\pi_2^{(l)} \colon (E/S, \alpha : \underline{\mathbb{Z}/M\mathbb{Z}}_S \to E[M], C) \mapsto (\overline{E} := (E/C)/S, \alpha \bmod C : \underline{\mathbb{Z}/M\mathbb{Z}}_S \to \overline{E}[M]).$$

By [Ce17, 4.7.1], the morphisms are finite and flat.

Definition 3.2.2. *Define the lth Hecke correspondence on $X_1(M)$ to be the correspondence $(\pi_1^{(l)}, \pi_2^{(l)})$. We often denote this by T_l if $l \nmid M$ and by U_l if $l \mid M$.*

We can also analogously define a moduli problem $[\Gamma_1^\mu(M,l)]$, yielding a curve $X_1^\mu(M,l)$ over $\mathbb{Z}$ which is smooth over $\mathbb{Z}[1/l]$, proper over $\mathbb{Z}[1/Ml]$, and which admits finite flat morphisms $\pi_i^{(l),\mu}$ to $X_1^\mu(M)$ and Atkin-Lehner isomorphisms $v_{M,l}, w_{M,l}$ defined over $\mathbb{Z}[1/M, \mu_M]$ and $\mathbb{Z}[1/M]$, respectively. We have then that $w_M \circ \pi_i^{(l)} = \pi_{3-i}^{(l),\mu} \circ w_{M,l}$ and $v_M \circ \pi_i^{(l)} = \pi_i^{(l),\mu} \circ v_{M,l}$. Thus, the correspondences T_l and U_l correspond to the similarly defined $T_l^{\mu *}$, $U_l^{\mu *}$ under w_M.

3.2.1 Sheaves of differentials and modular forms

We introduce the sheaves which will be used to algebraically define spaces of modular forms following [DI95, §12]. Recall that a morphism of schemes $f \colon X \to S$ is called Cohen-Macaulay (respectively syntomic) if it is flat, locally of finite presentation, and has Cohen-Macaulay (resp. local complete intersection) fibers.

Definitions 3.2.3. *Let $f\colon E \to S$ be a Cohen-Macaulay morphism of schemes of pure relative dimension d.*

(i) Let $\Omega_{E/S}$ be the relative dualizing sheaf over E of f of [DR73, I.2].

(ii) Let $\Omega^1_{E/S}$ be the sheaf over E of relative Kahler differentials of [SP, Tag 01UM].

(iii) Suppose that f is a generalized elliptic curve with identity section $e : S \to E$. Then f is syntomic, and we let

$$\omega_{E/S} := e^*\Omega_{E/S}.$$

We remark that in [DR73], the notation $\omega_{X/S}$ is used for our $\Omega_{E/S}$ and they refer to the sheaf as the sheaf of regular differentials. The first two items in the above definition are related by a canonical map

$$c_{E/S} : \Omega^d_{E/S} \to \Omega_{E/S}$$

which is an isomorphism over the smooth locus of f [Li02, 6.4.13], where $\Omega^d_{E/S} = (\Omega^1_{E/S})^{\otimes d}$. As the identity section e has image in the smooth locus, we see then that $\omega_{E/S}$ is canonically isomorphic to $e^*\Omega^1_{E/S}$. We record some useful results.

Lemma 3.2.4.

(i) Let

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ \downarrow{\scriptstyle h'} & & \downarrow{\scriptstyle h} \\ S' & \xrightarrow{g} & S \end{array}$$

be a commutative diagram of schemes. Then there is a canonical map of sheaves $g'^*\Omega^1_{X'/S'} \to \Omega^1_{X/S}$ which is an isomorphism if the diagram is Cartesian.

(ii) The construction $\omega_{X/S}$ is stable under base change of S, i.e., $g^*\omega_{X/S} = \omega_{X'/S'}$.

(iii) The sheaves $\Omega_{E/S}$ and $\omega_{E/S}$ are line bundles.

(iv) There is a canonical isomorphism $\omega_{E/S} \to f_*\Omega_{E/S}$

Proof. The first claim is [SP, Tag 01UV], while the second claim follows from the first claim. The last two claims are [DR73, II.1.6]. $\square$

In the analytic setting, the sheaf $\omega = \omega_{\overline{E}_1^\mu(M)/X_1^\mu(M)}$ can be described rather concretely. We give a summary of the exposition in [DI95, 12.3] here. We first start with a concrete description of the universal analytic family of elliptic curves $E_1(M)^{\mathrm{an}}$ over $Y_1(M)^{\mathrm{an}}$ as the quotient of the trivial bundle $\mathcal{H} \times \mathbb{C}$ over $\mathcal{H}$ by the right action of $\Gamma_1(M)$ on $\mathbb{Z} \times \mathbb{Z}$ given by

$$(z, \zeta) \cdot (m, n) = (z, \zeta + mz + n).$$

This produces a family of elliptic curves over the upper half plane $\mathcal{E} \to \mathcal{H}$ with a canonical family of points of order M described by the section $z \mapsto (z, 1/M)$. We may define on the left an action of $\mathrm{SL}_2(\mathbb{Z})$ given by $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ acting as

$$[(z, \zeta)] \mapsto [(\gamma(z), (cz + d)^{-1}\zeta)].$$

The quotient of the universal family of elliptic curves by the action of $\Gamma_1(M) \leqslant \mathrm{SL}_2(\mathbb{Z})$ then gives the universal elliptic curve over the modular curve of level $\Gamma_1(M)$. The analytic sheaf ω^{an} can then be identified with the sheaf of sections of the line bundle

$$\Gamma_1(M)\backslash(\mathcal{H} \times \mathrm{Cot}(\mathbb{C})),$$

where $\mathrm{Cot}(\mathbb{C})$ is the 1-dimensional cotangent space of $\mathbb{C}$ at the origin. This line bundle can be identified with the bundle

$$\Gamma_1(M)\backslash(\mathcal{H} \times \mathbb{C})$$

over $Y_1(M)^{\mathrm{an}}$ where the action is given by $\gamma \cdot (z, \xi) = (\gamma(z), (cz + d)\xi)$, with the identification given by

$$(z, \xi) \leftrightarrow (z, 2\pi i \xi d\zeta).$$

The analytic description can also be extended to the universal generalized elliptic curve over the projective modular curve $X_1^\mu(N)$ as in [DR73, VII.4]. In this way, we have an identification of the classical space of modular forms $M_k(N;\mathbb{C})^{\mathrm{class}}$ with the space $H^0(X_1^\mu(M)^{\mathrm{an}},\omega^{\otimes k,\mathrm{an}})$ where a modular form $f(z)$ produces a global section $f(z)(d\zeta)^{\otimes k}$ of the tensor power of the pushforward of the relative cotangent bundle invariant under pullback by elements of $\Gamma_1(M)$. This suggests that we should algebraically define the space of modular forms as $H^0(X_1^{(\mu)}(M),\omega^{\otimes k})$, where the superscript (μ) indicates we are considering both the regular and the μ-variant of the modular curve.

Definition 3.2.5. *Write ω for $\omega_{\overline{E}_1^{(\mu)}(M)/X_1^{(\mu)}(M)}$. Let $D = X_1^{(\mu)}(M) - Y_1^{(\mu)}(M)$ be the cuspidal divisor. For an arbitrary ring A for which $[\Gamma_1^{(\mu)}(M)]$ is representable, define a modular form over A on $X_1^{(\mu)}(M)$ and weight $k \geq 2$ to be an element of*

$$H^0(X_1^{(\mu)}(M)_A,(\omega^{\otimes k})_A),$$

and a cusp form over A to be an element of the subspace

$$H^0(X_1^{(\mu)}(M)_A,(\omega^{\otimes k}(-D))_A).$$

We write $M_k^{(\mu)}(M;A)$ for the space of such modular forms, and we write $S_k^{(\mu)}(M;A)$ for the subspace of such cusp forms.

We see that $M_k^{(\mu)}(M;A)$ and $S_k^{(\mu)}(M;A)$ are finitely generated and torsion-free as A-modules, being spaces of global sections of torsion-free sheaves on integral schemes flat over $\mathrm{Spec}(A)$. Recall the degeneracy maps $\pi_d^{(\mu)} : X_1^{(\mu)}(M) \to X_1^{(\mu)}(M')$ for a positive integer d such that $dM' \mid M$ of section 3.1.3. These induce injective degeneracy operators $i_d^{(\mu)} : M_k^{(\mu)}(M';A) \hookrightarrow M_k^{(\mu)}(M;A)$, induced by the counit $\mathrm{id} \to \pi_{d*}\pi_d^*$ of the adjunction $(\pi_d^* \dashv \pi_{d*})$ evaluated at $(\omega^{\otimes k})_A$, that take $S_k^{(\mu)}(M';A)$ into $S_k^{(\mu)}(M;A)$. To see that these maps are injective, note that the sheaves ω are locally free, being invertible sheaves, that injectivity may be checked on an affine cover of $X_1^{(\mu)}(M')$, that $\pi_d^{(\mu)}$ are surjective, and that $X_1^{(\mu)}(M)$ are integral schemes.

Remark 3.2.6. In the above definition, the assumption that the moduli problem is representable may be removed if we allow discussion of relative dualizing sheaves on algebraic stacks as in [Co07].

Lemma 3.2.7. *For any flat R-algebra S, we have canonical isomorphisms*

$$M_k^{(\mu)}(N;R)\otimes_R S \xrightarrow{\cong} M_k^{(\mu)}(N;S), \quad S_k^{(\mu)}(N;R)\otimes_R S \xrightarrow{\cong} S_k^{(\mu)}(N;S).$$

Proof. This follows as cohomology of quasicoherent sheaves commutes with flat base change for relatively quasicompact and separated schemes [SP, Tag 02KH]. □

When $A=\mathbb{C}$, we recover the classical space of homolorphic modular forms of weight k and level $\Gamma_1(M)$ via the analytification map of Serre's GAGA

$$H^0(X_1^{(\mu)}(M)_{\mathbb{C}}, \omega_{\mathbb{C}}^{\otimes k}) \xrightarrow{\cong} H^0(X_1^{(\mu)}(M)_{\mathbb{C}}^{\mathrm{an}}, (\omega^{\mathrm{an}})^{\otimes k}) = M_k(\Gamma_1(M),\mathbb{C})^{\mathrm{class}}$$

as $\omega_{\Gamma_1(M),\mathbb{C}}$ is a coherent sheaf and $X_1^{(\mu)}(M)_{\mathbb{C}}$ is smooth and proper over $\mathbb{C}$. We in particular have a canonical $\mathbb{Z}$-structure on the space of classical modular forms using the model $X_1^{\mu}(M)$, along with a $\mathbb{Z}$-structure coming from using the model $X_1(M)$. The former $\mathbb{Z}$-structure agrees with that coming from q-expansions at infinity, while the latter in general does not, as we will indicate below. Over any $\mathbb{Z}[1/M,\mu_M]$-algebra, we may identify the two spaces of algebraic modular forms associated with the two models using the isomorphism v_M of modular curves, and as this isomorphism induces the identity map on the analytic curves, it also induces the identity map on the corresponding spaces of analytic forms. The two integral theories generally differ, however, and we maintain the distinction in notation through the next few sections as we set up the Hecke theory.

We now relate this to the notion of so-called geometric modular forms due to Katz [Ka72], which is used in the first part of [Oh20]. This presentation of ideas also allows one to define modular forms without worrying about issues of representability of moduli functors [Ka76, II.2.5]. Recall that for a morphism of schemes $g: X\to Y$ and a quasicoherent sheaf $\mathcal{G}$ on Y, there is a natural morphism of global sections $\Gamma(Y, \mathcal{G}) \to \Gamma(X, g^*\mathcal{G})$, where $g^*\mathcal{G} := g^{-1}\mathcal{G} \otimes_{g^{-1}\mathcal{O}_Y} \mathcal{O}_X$, inducing a map on cohomology

$$H^i(Y, \mathcal{G}) \to H^i(X, g^*\mathcal{G}).$$

Taking $g : \overline{E}_1^{(\mu)}(M) \to X_1^{(\mu)}(M)$ to be the structure morphism and $\mathcal{G} = \omega^{\otimes k} = \omega_{E/X}^{\otimes k}$, we then see that a modular form $f \in M_k^{(\mu)}(M; A)$ gives for any generalized elliptic curve with level structure $(E/S, \alpha)$ corresponding to a morphism $\varphi : S \to X_1^{(\mu)}(M)$ an element $f_{E/S} \in H^0(S, \omega_{E/S}^{\otimes k})$ and that this assignment is compatible with composition/base change. As any scheme is determined by its morphisms from affine schemes, we find that a modular form f on $X_1^{(\mu)}$ is equivalent to a "rule" which assigns to every triple $(E/\mathrm{Spec}(R), \alpha, \xi)$, where $(E/\mathrm{Spec}(R), \alpha)$ is a generalized elliptic curve with level structure and ξ is a nowhere vanishing global section of $\omega_{E/\mathrm{Spec}(R)}^{\otimes k}$ (so that we have an isomorphism $H^0(\mathrm{Spec}(R), \omega_{E/\mathrm{Spec}(R)}^{\otimes k}) \cong R$), an element $f(E/\mathrm{Spec}(R), \alpha, \xi) \in R$ which depends only on the isomorphism class of $(E/\mathrm{Spec}(R), \alpha, \xi)$, which commutes with arbitrary base change, and which satisfies for any $\lambda \in R^\times$ that $f(E/R, \alpha, \lambda\xi) = \lambda^{-k} f(E/R, \alpha, \xi)$.

3.2.2 Cusps and algebraic q-expansions

We may apply the geometric viewpoint on modular forms above to Tate curves over $\mathbb{Z}[[q]]$ in order to obtain q-expansions of modular forms. The construction of Tate curves is carried out in [DR73, Ch. VII] and [Co07, §2.5] following Raynaud's construction via formal schemes and algebraization. We summarize the results below in the notation of [Co07].

Definition 3.2.8.

(i) For all $n \geq 1$, there exist generalized elliptic curves $\underline{\mathrm{Tate}}_n \to \mathrm{Spec}(\mathbb{Z}[[q^{1/n}]])$ whose fibers over $q^{1/n} = 0$ are standard Néron n-gons and whose restriction to $\mathbb{Z}((q^{1/n}))$ are elliptic curves.

(ii) There is a canonical element ω_{can} of $H^0(\mathrm{Spec}(\mathbb{Z}_p[[q]]), \omega_{\underline{\mathrm{Tate}}_n})$ given by the differential

$\frac{dq^{1/n}}{q^{1/n}}$ *on* Tate_n.

Lemma 3.2.9. *(i)* $\underline{\mathrm{Tate}}_n$ *admits a free action by the group* $\mathbb{Z}/n\mathbb{Z}$ *which lifts the standard rotation action on the standard* n*-gon over* $\mathrm{Spec}(\mathbb{Z})$.

(ii) For $m \mid n$*, there is a finite étale map* $\underline{\mathrm{Tate}}_n \to \underline{\mathrm{Tate}}_m$ *over* $\mathrm{Spec}(\mathbb{Z}[[q^{1/m}]])$ *of degree* n/m *given by the quotient of the action of* $m\mathbb{Z}/n\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z}$.

(iii) The curves $\underline{\mathrm{Tate}}_n$ *are the unique generalized elliptic curves up to unique isomorphism over* $\mathbb{Z}[[q^{1/n}]]$ *which have standard* n*-gon fibers and which have fiber over* $\mathbb{Z}((q^{1/n}))$ *isomorphic to* $\underline{\mathrm{Tate}}_1 \otimes_{\mathbb{Z}[[q]]} \mathbb{Z}((q^{1/n}))$.

(iv) There is a unique isomorphism of group schemes over $\mathbb{Z}[[q^{1/n}]]$

$$\underline{\mathrm{Tate}}_n^{\mathrm{sm}}[n] \cong \mu_n \times \underline{\mathbb{Z}/n\mathbb{Z}}$$

lifting the canonical isomorphism on the standard n*-gon fiber over* $q^{1/n} = 0$.

As generalized elliptic curves over algebraically closed fields are all isomorphic to standard n-gons C_n, the study of the residue fields of the cusps of $X_1^{(\mu)}(M)$ amounts to the study of $[\Gamma_1^{(\mu)}(M)]$ structures on C_n for $n \geq 1$. Tate curves are then universal deformations of n-gons and can be used to identify the universal deformation rings at the cusps of the modular curves $X_1^{(\mu)}(M)$. The identification of the cusps of $X_1(M)$ is carried out in [Co07, Theorem 4.3.4]; however, the theorem statement there contains errors. We give a description of the cusps of $X_1^{\mu}(M)$ in the following proposition.

Proposition 3.2.10. *Let* $M \geq 5$*. For* $d > 0$*, let* $\mathcal{C}(M)_d$ *be the locus of points on* $X_1^{\mu}(M)$ *corresponding to* $\Gamma_1^{\mu}(M)$*-structures on generalized elliptic curves with* d*-gon geometric fibers. For* $d \mid M, d < M/2$*, we have that* $\mathcal{C}(M)_{d,\mathbb{Z}[1/M]}$ *is a disjoint union of* $\varphi(M/d)/2$ *copies of* $\mathrm{Spec}(\mathbb{Z}[\mu_d, 1/M])$ *corresponding to elements of* $(\mathbb{Z}/\frac{M}{d}\mathbb{Z})^{\times}/\pm$*, while if* $d = M$ *or* $M/2$*, then* $\mathcal{C}(M)_{d,\mathbb{Z}[1/M]} = \mathrm{Spec}(\mathbb{Z}[\mu_d, 1/M]^+)$.

Proof. As in the proof of [Co07, Theorem 4.3.4], we study the cusps of the generic fiber $X_1^\mu(M)_{\mathbb{Q}}$. Note first that as we require $\Gamma_1^\mu(M)$-structures on a generalized elliptic curve to contact each irreducible component of each geometric fiber, any such structure can only exist on a d-gon for $d \mid M$. To find the residue fields of points of $\mathcal{C}(M)_{d,\mathbb{Q}}$, we pass to $\overline{\mathbb{Q}}$ and consider Galois orbits of isomorphism classes of the data of the standard d-gon C_d equipped with a $\Gamma_1^\mu(M)$-structure over $\overline{\mathbb{Q}}$. These are all of the form $(C_d, \zeta_M \mapsto (\zeta_M^r, b))$ where $b \in (\mathbb{Z}/d\mathbb{Z})^\times$, so that the $\mathbb{Z}$-span of (ζ_M^r, b) intersects each irreducible component of C_d, and where $r \in \mathbb{Z}/M\mathbb{Z}$ maps to a unit in $\mathbb{Z}/\frac{M}{d}\mathbb{Z}$, so that (ζ_M^r, b) has order M.

We now consider one such pair (ζ_M^r, b) describing an isomorphism class of $\Gamma_1^\mu(M)$-structures on C_d. Recall that $\mathrm{Aut}(C_d, +) = \mathbb{Z}/2\mathbb{Z} \times \mu_d$, where $\zeta = \zeta_M^{sM/d} \in \mu_d(\overline{\mathbb{Q}})$ acts by sending (ζ_M^r, b) to $(\zeta_M^{r+bsM/d}, b)$ and where the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ acts by inversion. Thus, we may assume that $0 < r \leq M/d$. The Galois action by a $\sigma \in G_{\mathbb{Q}}$ mapping to $a \in (\mathbb{Z}/M\mathbb{Z})^\times$ via the cyclotomic character sends $\zeta_M \mapsto (\zeta_M^r, b)$ to $\zeta_M^a \mapsto (\zeta_M^{ar}, b)$, which is equivalent to the level structure $\zeta_M \mapsto (\zeta_M^r, a^{-1}b)$, where we view $a \in (\mathbb{Z}/d\mathbb{Z})^\times$.

Suppose that we are in the case $d = M$ or $M/2$. As M/d is then 1 or 2, the automorphisms of the previous paragraph produce isomorphisms of level structures between $\zeta_M \mapsto (\zeta_M, b)$, $\zeta_M \mapsto (\zeta_M^{-1}, -b)$, and $\zeta_M \mapsto (\zeta_M, -b)$, where the first isomorphism comes from the inversion automorphism and the second isomorphism comes from the μ_d part of $\mathrm{Aut}(C_d, +)$. Thus, we have an equality of isomorphism classes $[(C_d, \zeta_M \mapsto (\zeta_M, b))] = [(C_d, \zeta_M \mapsto (\zeta_M, -b))]$, and we see that $G_{\mathbb{Q}}$ acts transitively on all isomorphism classes of $\Gamma_1^\mu(M)$-structures. Thus, the Galois stabilizer for the class is $G_{\mathbb{Q}(\zeta_M)^+}$, which gives the residue field $\mathbb{Q}(\zeta_M)^+$ of the corresponding point of $X_1^\mu(M)$.

In the remaining case that $d < M/2$, we have that r and $-r$ are distinct modulo M/d, and so we get $\varphi(M/d)/2$ distinct Galois orbits, each with corresponding stabilizer $G_{\mathbb{Q}(\mu_d)}$ and residue field $\mathbb{Q}(\mu_d)$.

To obtain the integral results as in the proposition statement, we appeal to the regularity and properness of $X_1^\mu(M)_{\mathbb{Z}[1/M]}$ as in the proof of [Co07, 4.3.4]. $\square$

We now point out the error in the statement of [Co07, Theorem 4.3.4]. There it is claimed that the d-gon cusps of $X_1(M)$, assuming that the moduli problem is representable over $\mathbb{Z}$, when $d > 2$ form a disjoint union of copies of $\mathrm{Spec}(\mathbb{Z}[\mu_{M/d}])$ indexed by pairs (b, r) where $b \in (\mathbb{Z}/d\mathbb{Z})^\times$ and r is a positive divisor of d that reduces to a unit in $(\mathbb{Z}/(M/d)\mathbb{Z})^\times$. This cannot be true, as the number of cusps of $X_1(M)_{\overline{\mathbb{Q}}}$ is known to be $1/2 \sum_{d|M} \varphi(d)\varphi(M/d)$ [DS05, pg. 102], and Conrad's description yields an overcount.

Describing the cusps of $X_1^\mu(M)$ over $\mathbb{Z}$ involves considering closed immersions of group schemes $\mu_{M,\mathbb{Z}} \to \mathbb{G}_{m,\mathbb{Z}} \times \underline{\mathbb{Z}/d\mathbb{Z}}_{\mathbb{Z}}$ which are surjective upon composing with the projection to the constant group scheme factor. As there are no nontrivial maps from the local group scheme $\mu_{p^k,\mathbb{F}_p}$ to an étale group scheme over $\mathbb{F}_p$, we see that some of the cusps over $\mathbb{Z}[1/M]$ described above will not extend over $\mathbb{Z}$. In the case $d = 1$, we always have the $\Gamma_1^\mu(M)$-structures $\mathrm{Spec}(\mathbb{Z}) \to X_1^\mu(M)$ coming from the usual inclusions $\mu_{M,\mathbb{Z}} \hookrightarrow C_1^{\mathrm{sm}} = \mathbb{G}_{m,\mathbb{Z}}$. We are particularly interested in the cusp corresponding to the canonical inclusion as it corresponds to the infinity cusp from the analytic theory, as we now explain.

Recall that we have an identification of curves $X_1(M)^{\mathrm{an}} = X_1^\mu(M)^{\mathrm{an}}$ via the algebraic isomorphism v_M. Viewing $X_1^{(\mu)}(M)^{\mathrm{an}}$ as $\Gamma_1(M)\backslash(\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}))$, we have an identification of cusps $\Gamma_1(M)\backslash\mathbb{P}^1(\mathbb{Q}) = \Gamma_1(M)\backslash PSL_2(\mathbb{Z})/\left(\begin{smallmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right)$ where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ corresponds to $\gamma \cdot \infty = a/c \in \mathbb{P}^1(\mathbb{Q})$. We may also set

$$P_M := \{(c, d) \in (\mathbb{Z}/M\mathbb{Z})^2 \mid (c, d) = \mathbb{Z}/M\mathbb{Z}\}$$

and identify the set of cusps of $X_1^{(\mu)}(M)^{\mathrm{an}}$ with $P_M/\!\sim$ where $(c, d) \sim (c', d')$ if $c = \epsilon c'$ and $d \equiv \epsilon d' \bmod c(\mathbb{Z}/M\mathbb{Z})$ where $\epsilon = \pm 1$. A cusp $a/c \in \mathbb{P}^1(\mathbb{Q})$ corresponds to $(c, d) \in P_M/\!\sim$ when $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, and in terms of the algebraic description of cusps, $(c, d) \in P_M/\!\sim$ corresponds to the level structure $1 \mapsto (\zeta_M^d, \frac{c}{\gcd(c,M)})$ (or $\zeta_M \mapsto (\zeta_M^d, \frac{c}{\gcd(c,M)})$), where we use notation as in the proof of Proposition 3.2.10.

For later use, we would like to record the action of $G_{\mathbb{Q}}$ on the cusps, which depends on which algebraic model of the modular curve one uses. In [FK12], they opt for the presentation

$P_M/{\sim}$ for the curve $X_1(M)$, while in [Oh03] and [Oh99, §4.3], the cusps $a/c \in \mathbb{P}^1(\mathbb{Q})$ of $X_1^{\mu}(M)$ are represented as $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \in A_M/{\sim}$ where

$$A_M := \{\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \in (\mathbb{Z}/M\mathbb{Z})^2 \mid (a,c) = \mathbb{Z}/M\mathbb{Z}\}$$

and $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right]$ if $c = \epsilon c'$ and $a \equiv \epsilon a' \bmod c(\mathbb{Z}/M\mathbb{Z})$ where $\epsilon = \pm 1$. We remark that we may use either of the presentations, $P_M/{\sim}$ or $A_M/{\sim}$, when discussing the cusps of either model of the modular curve, and we will later do so when referring to results in the literature.

Lemma 3.2.11. *For $\sigma \in G_{\mathbb{Q}}$, let $\alpha \in (\mathbb{Z}/M\mathbb{Z})^{\times}$ be such that $\sigma(\zeta_M) = \zeta_M^{\alpha}$. Then*

$$\sigma \cdot \begin{bmatrix} a \\ c \end{bmatrix} = \begin{bmatrix} a \\ \alpha^{-1}c \end{bmatrix}$$

as a cusp of $X_1^{\mu}(M)$, and

$$\sigma \cdot (c,d) = (c, \alpha d)$$

as a cusp of $X_1(M)$.

Proof. The cusp (c,d) of $X_1(M)$ corresponds to the level structure $(\zeta_M^d, \frac{c}{\gcd(c,M)})$, and so the action of $G_{\mathbb{Q}}$ on (c,d) is apparent. The cusp $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$ corresponds to (c,d), and so as a cusp of $X_1(M)$, an element $\sigma \in G_{\mathbb{Q}}$ corresponding to α maps the cusp to $\left[\begin{smallmatrix} \alpha^{-1}a \\ c \end{smallmatrix}\right]$. Via the equality $\sigma \circ v_M = v_M \circ \langle \kappa_{Np}(\sigma)\rangle \circ \sigma$ as morphisms $X_1^{\mu}(M) \to X_1(M)$, we see that σ sends $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$ to $\left[\begin{smallmatrix} a \\ \alpha^{-1}c \end{smallmatrix}\right]$ as a cusp of $X_1^{\mu}(M)$. □

We have two particular cusps of interest. The cusp $(1,0) \in P_M$ is called the 0-cusp and corresponds an M-gon cusp of $X_1^{(\mu)}(M)_{\overline{\mathbb{Q}}}$. The cusp $(0,1)$ is the so-called infinity cusp and corresponds to a 1-gon cusp of $X_1^{(\mu)}(M)_{\overline{\mathbb{Q}}}$, and which in the case of $X_1^{\mu}(M)$ is defined over $\mathbb{Z}$ as indicated above.

For the model $X_1^{\mu}(M)$, the canonical inclusion $\mu_{M,\mathbb{Z}} \hookrightarrow C_1$ lifts to an embedding $\mu_{M,\mathbb{Z}} \hookrightarrow \underline{\mathrm{Tate}}_1$ corresponding to a morphism

$$\infty : \mathrm{Spec}(\mathbb{Z}[[q]]) \to X_1^{\mu}(M).$$

The 1-gon cusp of $X_1(M)$ over $\mathbb{Z}$ admits a twisted Tate curve as a universal deformation over $\mathbb{Z}[\mu_M]^+$, which is denoted by $\underline{\mathrm{Tate}}'_1$ in [Co07, 4.3.7]. For our purposes, this is not quite the curve we wish to use in order to define algebraic q-expansions. Instead, we pass up to $X_1(M)_{\mathbb{Z}[\mu_M]}$ and use the Tate curve $\underline{\mathrm{Tate}}_{1,\mathbb{Z}[[q]]\otimes\mathbb{Z}[\mu_M]}$ with $\Gamma_1(M)$-structure corresponding to ζ_M, which will correspond in the analytic theory to the infinity cusp, and which corresponds to a map

$$\mathrm{Spec}(\mathbb{Z}[[q]] \otimes \mathbb{Z}[\mu_M]) \to X_1(M)_{\mathbb{Z}[\mu_M]}.$$

Definition 3.2.12. *For any modular form f on $X_1^\mu(M)$ of weight k over a commutative ring R, we define the q-expansion of f at infinity to be the image under the pullback morphism*

$$H^0(X_1^\mu(M)_R, \omega_R) \to H^0(\mathrm{Spec}(R \otimes \mathbb{Z}[[q]]), \infty^*\omega_R) \cong R \otimes \mathbb{Z}[[q]],$$

where the last isomorphism comes from the canonical element ω_{Tate}. For any $\mathbb{Z}[\mu_M]$-algebra R and any modular form f on $X_1(M)_R$, we similarly define the q-expansion of f to be the pullback along the morphism induced by $\underline{\mathrm{Tate}}_{1,R\otimes\mathbb{Z}[[q]]}$ composed with the isomorphism with $R \otimes \mathbb{Z}[[q]]$.

The above construction agrees with the Fourier expansion at infinity of the associated analytic modular form for $R = \mathbb{C}$ for either model $X_1(M)$ or $X_1^\mu(M)$, and as such we may refer to the q-expansion (at infinity) of a form simply as its Fourier expansion.

We now state the q-expansion principle, which allows us to identify modular forms with formal power series.

Proposition 3.2.13 (Katz)**.**

(i) For any commutative ring A the map

$$M_k^\mu(M; A) \to A \otimes_{\mathbb{Z}} \mathbb{Z}[[q]] \hookrightarrow A[[q]]$$

is injective.

(ii) If A is a subring of B, then the commutative diagram

$$\begin{array}{ccc} M_k^{\mu}(M;A) & \longrightarrow & A \otimes_{\mathbb{Z}} \mathbb{Z}[[q]] \\ \downarrow & & \downarrow \\ M_k^{\mu}(M;B) & \longrightarrow & B \otimes_{\mathbb{Z}} \mathbb{Z}[[q]] \end{array}$$

is Cartesian.

The analogous statement for cusp forms, and the corresponding statements using the model $X_1(M)$ in place of $X_1^{\mu}(M)$ if restricting to $\mathbb{Z}[1/M, \mu_M]$-algebras, hold as well.[2]

The formulation above is as in [DI95, 12.3.4, 12.3.5], though they work over $\mathbb{Z}[1/M, \mu_M]$-algebras for the model $X_1(M)$. The original result is [Ka72, 1.6.1], where it is stated only for the curve $X(M)$ over $\mathbb{Z}[1/M]$. The point of commonality in each of these references is that the modular curves considered are smooth over the given base ring and that the q-expansions and spaces of modular forms are considered over the same ring. For non-smooth curves, one generally needs to consider q-expansions at a collection of cusps which intersects each irreducible component of each fiber in order to obtain a q-expansion principle, i.e., to obtain statements analogous to the two in the proposition above. As $X_1^{\mu}(M)$ has geometrically irreducible fibers, one could formulate a principle for each cusp for algebras over the base ring of the cusp, whereas in [Co07, 4.4.2], it is said that the space $M_k(M;\mathbb{Z})$ of weight k forms on $X_1(M)$ over $\mathbb{Z}$ are precisely those which have integral q-expansions at each of the N-gon cusps.

We see then that using the model $X_1^{\mu}(M)$ is the more natural option in defining algebraic q-expansions at ∞ as over $\mathbb{Z}$ it agrees with the analytic description of modular forms which have Fourier expansion at infinity with coefficients in $\mathbb{Z}$. The issue with using $X_1(M)$ instead is that the fibers in characteristics dividing the level are not geometrically irreducible and smooth, and so one does not have a simply stated q-expansion principle as above.

[2] *Though the Tate curves over $X_1(M)$ were defined over $\mathbb{Z}$, one requires geometric irreducibility of the fibers in order to state a q-expansion principle using only a single q-expansion. Geometric irreducibility holds only away from M for the model $X_1(M)$.*

3.2.3 Hecke operators

We now give an algebraic description of Hecke operators on the spaces of modular forms defined above and other cohomology groups of modular curves. For simplicity, we stick to the model $X_1(M)$, though everything should hold for $X_1^\mu(M)$ in place of $X_1(M)$ as well, with only minor changes in notation. In order to define the (non-dual) Hecke operators T_l and U_l, we consider the sheaf $\omega = \omega_{E/X}$ and the following commutative diagram of schemes

$$\begin{tikzcd}
& \overline{E}_1(M,l) \arrow[rr, "\varphi"] \arrow[dl, "h_1"'] \arrow[dr, "g_1"] & & \overline{E}_1(M,l)/C \arrow[dl, "g_2"'] \arrow[dr, "h_2"] & \\
\overline{E}_1(M) \arrow[dr, "f"'] & & X_1(M,l) \arrow[dl, "\pi_1^{(l)}"] \arrow[dr, "\pi_2^{(l)}"'] & & \overline{E}_1(M) \arrow[dl, "f"] \\
& X_1(M) & & X_1(M) &
\end{tikzcd} \tag{3.2.1}$$

where $\overline{E}_1(M,l)$ is the universal generalized elliptic curve over $X_1(M,l)$, C is the universal cyclic subgroup scheme of rank l of $E_1(M,l)^{\mathrm{sm}}$, φ is the corresponding isogeny in the sense of [Ce17, §2.2], f is the structure morphism, and the two squares are Cartesian. Our goal is to describe an endomorphism of $H^0(X_1(M),\omega)$, as this will induce an endomorphism on $H^0(X_1(M),\omega^{\otimes k})$.

We first consider the unit of the adjunction $(\pi_2^{(l)*} \dashv \pi_{2*}^{(l)})$ at ω to get a map

$$\omega \to \pi_{2*}^{(l)}\pi_2^{(l)*}\omega = \pi_{2*}^{(l)}\omega_{(\overline{E}_1(M,l))/C)/X_1(M,l)}.$$

Write e_1 and e_2 for the canonical sections of g_1 and g_2. We have an equality $e_2 = \varphi \circ e_1$ and a natural map $\varphi^*\Omega^1_{(\overline{E}_1(M,l)/C)/X_1(M,l)} \to \Omega^1_{\overline{E}_1(M,l)/X_1(M,l)}$, yielding a map we denote simply by φ^*:

$$\begin{aligned}
\pi_{2*}^{(l)}e_2^*\Omega^1_{(\overline{E}_1(M,l)/C)/X_1(M,l)} &= \pi_{2*}^{(l)}e_1^*\varphi^*\Omega^1_{(\overline{E}_1(M,l)/C)/X_1(M,l)} \\
&\to \pi_{2*}^{(l)}e_2^*\Omega^1_{\overline{E}_1(M,l)/X_1(M,l)} \\
&= \pi_{2*}^{(l)}\omega_{\overline{E}_1(M,l)/X_1(M,l)} = \pi_{2*}^{(l)}\pi_1^{(l)*}\omega.
\end{aligned}$$

Taking global sections, we thus far have a map

$$H^0(X_1(M),\omega) \to H^0(X_1(M),\pi_{2*}^{(l)}\pi_1^{(l)*}\omega) = H^0(X_1(M),\pi_{1*}^{(l)}\pi_1^{(l)*}\omega),$$

where the equality follows from the definition of sections of a pushforward sheaf and the fact that $\pi_1^{(l)}$ and $\pi_2^{(l)}$ have the common domain $X_1(M,l)$. Finally, as $\pi_1^{(l)}$ is finite and flat, there is a trace map which we denote $\pi_{1*}^{(l)}$, which coincides with the counit of the adjunction $(\pi_{1*}^{(l)} \dashv \pi_1^{(l)!})$, from $\pi_{1*}^{(l)}\pi_1^{(l)*}\omega$ back to ω.

The dual Hecke operators come from instead pulling back along $\pi_1^{(l)}$, pulling back along the dual isogeny $\varphi^\vee$, and then pushing forward along $\pi_2^{(l)}$.

Definition 3.2.14. *Suppose that $[\Gamma_1(M)]$ is representable over a subring R of $\mathbb{C}$. We define the Hecke operators T_l, writing T_l in place of U_l when $l \mid M$ for simplicity, on $M_k(M;R)$ by the formula*

$$lT_l = \pi_{1*}^{(l)} \circ \varphi^* \circ \pi_2^{(l)*},$$

which recovers the classical operator lT_l under analytification, and the dual Hecke operators T_l^* and U_l^* by

$$lT_l^* = \pi_{2*}^{(l)} \circ \varphi^{\vee *} \circ \pi_1^{(l)*}.$$

The factor of l in the above formulas is due to our use of the particular sheaf $\omega^{\otimes k}$. Below, we explain how the use of a related sheaf produces formulas without this extra factor. In the meantime, we remark that in order for the definition of T_l above to make sense, one needs to know that the endomorphism $\pi_{1*}^{(l)} \circ \varphi^* \circ \pi_2^{(l)*}$ has image in $lM_k(M;R)$. We do not prove this here, but instead indicate that this may be shown using calculations with q-expansions as in [Ka72, 1.11], and alternatively Conrad has proven this conceptually over $\mathbb{Z}$ by considering the morphism fiberwise in [Co07, 4.5.1].

Remark 3.2.15. In the above definition of T_l, we are considering the pullback under the degeneracy morphism $\pi_2^{(l)}$ which on points corresponds to $(E,\alpha,C) \mapsto (E/C,\overline{\alpha})$. On the other hand, the usual description of the effect of the Hecke operator T_l on points of the modular curve, given by

$$(E,\alpha) \mapsto \sum_{\substack{C \subset E \\ C \cap \mathrm{im}(\alpha)=1}} (E/C,\overline{\alpha})$$

where the sum is over order l subgroup schemes of E which intersect the image of α trivially, suggests that the Hecke operator should be described as pulling back along $\pi_1^{(l)}$ followed by pushing forward along $\pi_2^{(l)}$. This discrepancy arises because the convention for defining morphisms of the Jacobian of a curve induced by algebraic correspondences in arithmetic contexts is to view the Jacobian as the Albanese variety, which is an object covariantly associated with the curve.

We explain this standard convention. If R is a field and T is a correspondence on X over R, then T and its dual T^* induce endomorphisms on the Jacobian of X, $J_X := \mathrm{Pic}^0_{X/R}$, which we denote by the same symbols, by $T := \mathrm{Alb}(\pi_2) \circ \mathrm{Pic}^0(\pi_1)$ and $T^* := \mathrm{Alb}(\pi_1) \circ \mathrm{Pic}^0(\pi_2)$. Here, for any finite morphism of smooth, proper curves over of a field $\pi : Y \to X$, one has morphisms $\mathrm{Alb}(\pi) : J_Y \to J_X$ and $\mathrm{Pic}^0(\pi) : J_X \to J_Y$ which arise from viewing the Jacobian of a curve either as the Albanese variety or the identity component of the relative Picard scheme of the curve, respectively. The morphism T on J_X is often referred to in the literature as the Albanese or covariant action of the correspondence T on X (e.g. as in [Gr90, §3], [Ri90, §3], [Oh03, §1.2], and [Oh20, §§5, 6]), while T^* is referred to as the Picard or contravariant action of T – this is due to the convention that for a finite morphism $X \to Y$, one associates with it the correspondence (id, f) which then induces the map $T = \mathrm{Alb}(f) : \mathrm{Jac}(X) \to \mathrm{Jac}(Y)$ in the same direction as f.

This covariant/contravariant terminology has been carried over to general settings where one has Hecke actions. For instance, when discussing the action of Hecke correspondences on cohomology groups, it is standard to refer to the morphism T_l defined above as the contravariant action of the correspondence denoted by T_l; see for example the introduction of [Oh00]. This in particular means that the standard isomorphism between étale cohomology of a curve with $\mathbb{Z}_p(1)$-coefficients, whose Hecke action we review below, and the p-adic Tate module of its Jacobian

$$H^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1)) \cong T_p(J_X)$$

interchanges the dual and non-dual Hecke operators under the standard conventions on actions of Hecke operators on the two sides. On the other hand, this means that the identification

$$H^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Z}_p) \cong \operatorname{Hom}(T_p(J_X), \mathbb{Z}_p)$$

under Poincaré duality is Hecke-equivariant; see for example the top of page 410 of [Oh20].

We now describe an action of $(\mathbb{Z}/M\mathbb{Z})^\times$ on modular curves. For simplicity, we only write out the action for the case of $X_1(M)$, with the action on $X_1^\mu(M)$ defined similarly. An element $a \in (\mathbb{Z}/M\mathbb{Z})^\times$ acts on the constant group $\mathbb{Z}/M\mathbb{Z}$ by multiplication, inducing maps $\langle a \rangle\colon X_1(M) \to X_1(M)$ and $\langle a \rangle_E : \overline{E}_1(M) \to \overline{E}_1(M)$ fitting into a Cartesian diagram

$$\begin{array}{ccc} \overline{E}_1(M) & \xrightarrow{\langle a \rangle_E} & \overline{E}_1(M) \\ \downarrow & & \downarrow \\ X_1(M) & \xrightarrow{\langle a \rangle} & X_1(M) \end{array}$$

These automorphisms induce actions on $M_k(M; A)$ which are compatible with the classically defined diamond operators on classical modular forms. We again have the relation that v_M is compatible with $\langle a \rangle$ defined on both models, while w_M interchanges $\langle a \rangle$ with $\langle a^{-1} \rangle$. Note that $\langle -1 \rangle$ is the identity on $X_1(M)$, while $\langle -1 \rangle_E$ is the inversion automorphism, inducing an action of $(-1)^k$ on $M_k(M; A)$.

We now consider other cohomology groups on which we may define Hecke and diamond operators and explain how the corresponding Hecke algebras can be identified. We start with considering constant sheaves $\underline{S}_{E_1(M)^{\text{an}}}$ on the analytic universal elliptic curve $E_1(M)^{\text{an}}$ over $Y_1(M)^{\text{an}}$ for any commutative ring S, and we form the kth symmetric power $\operatorname{Sym}^k R^1 f_* \underline{S}_{E_1(M)^{\text{an}}}$ for $k \geq 0$ of the first derived pushforward along the structure morphism of E which we also denote by f. Note, we are taking symmetric tensors over $\underline{S}$, so that when $k = 0$, we have the constant sheaf $\underline{S}$. By considering the analog of the commutative diagram 3.2.1 for $E_1(M)^{\text{an}}/Y_2(M)^{\text{an}}$, noting that we have base change isomorphism for proper morphisms, we may define Hecke operators on $H^i(Y_1(M)^{\text{an}}, \operatorname{Sym}^k R^1 f_* \underline{S}_{E_1(M)^{\text{an}}})$. Similarly, if we let S denote a finite commutative ring and $\underline{S}_{E_1(M)}$ the constant étale sheaf on $E_1(M)$, then we obtain

Hecke operators on $H^i_{\text{ét}}(Y_1(N)_{\overline{\mathbb{Q}}}, \mathrm{Sym}^k R^1 f_* \underline{S}_{E_1(M)})$. The étale comparison theorem then gives us canonical Hecke equivariant isomorphisms

$$H^1(Y_1(M)^{\text{an}}, \mathrm{Sym}^k R^1 f_* \underline{\mathbb{Z}_p}_{E_1(M)^{\text{an}}}) \cong H^1_{\text{ét}}(Y_1(M)_{\overline{\mathbb{Q}}}, \mathrm{Sym}^k R^1 f_* \underline{\mathbb{Z}_p}_{E_1(M)})$$

which follows from [SGA4.3, Exp. XI 4.4] by noting that $Y_1(M)_{\overline{\mathbb{Q}}}$ and $Y_1(M)_{\mathbb{C}}$ have equivalent étale sites. The analogous claims for the closed modular curve in place of $Y_1(M)$ holds as well, and the claim for compactly supported cohomology in place of standard cohomology is also valid by [SGA4.3, XVII 5.3.5]. In order to compare the above Hecke action with that on the space of modular forms, we first need to give an alternative cohomological definition of the space of modular forms.

Proposition 3.2.16. *Let D be the divisor $X_1^\mu(M) \backslash Y_1^\mu(M)$. There is an isomorphism of sheaves on $Y_1^\mu(M)$ called the Kodaira-Spencer map*

$$\omega^2_{E_1^\mu(M)/Y_1^\mu(M)} \to \Omega^1_{Y_1^\mu(M)} (:= \Omega^1_{Y_1^\mu(M)/\mathrm{Spec}(\mathbb{Z})})$$

which extends to an isomorphism of $\mathcal{O}_{X_1^\mu(M)}$-modules

$$\omega^2_{\overline{E}_1^\mu(M)/X_1^\mu(M)} \to \Omega^1_{X_1^\mu(M)}(D).$$

A similar result holds for the model $X_1(M)$ over $\mathbb{Z}[1/N]$.

Proof. The map is constructed in [Ka72, A.1.3.17] for a general elliptic curve E over a scheme S that is smooth over a base scheme T as the dual to the tangent mapping of the classifying morphism from S to the classifying stack $\mathcal{M}_{1,1}$ of elliptic curves. There it is explained that this morphism must be étale in order for the Kodaira-Spencer map to be an isomorphism. As the classifying stack is smooth over $\mathbb{Z}$, this in particular implies that the modular curve $Y_1^{(\mu)}(M)/R$ must be smooth over R in order for the Kodaira-Spencer map to be an isomorphism. The converse is also true [KM85, 10.13.10], hence the need to restrict to $\mathbb{Z}[1/M]$ for the case of $X_1(M)$. The extension of the Kodaira-Spencer map to sheaves on the closed modular curves is done by explicit computation with Tate curves as in [Ka72, A.1.3.18]. ☐

Thus, we get a canonical isomorphism

$$H^0(X_1^\mu(M), \omega_{\overline{E}_1^\mu(M)/X_1^\mu(M)}^{\otimes k}) \to H^0(X_1^\mu(M), \omega_{\overline{E}_1^\mu(M)/X_1^\mu(M)}^{\otimes k-2} \otimes_{\mathcal{O}_{X_1^\mu(M)}} \Omega^1_{X_1^\mu(M)}(D)),$$

allowing us to alternatively define the space of modular and cusp forms on X_1^μ of weight k and level $\Gamma_1(M)$ using the right-hand side cohomology group (cf. Definition 3.2.5), and similarly for forms on $X_1(M)$. However, the isomorphism is not Hecke equivariant. Indeed, in [De69, 3.18], the composition of morphisms defined as above as

$$\pi_{1*}^{(l)} \circ \varphi^* \circ \pi_2^{(l)*}$$

produces the usual Hecke operator T_l on the right-hand side cohomology. Though the cited result uses cohomology of the analytic sheaves $\mathrm{Sym}^k R^1 f_* \underline{\mathbb{Q}}_{E_1(M)^{\mathrm{an}}}$, we have the following Eichler-Shimura isomorphism which compares spaces of modular forms with cohomology of the symmetric power local systems.

Proposition 3.2.17. *Suppose that $k \geq 2$ and $M \geq 4$. Let $j : Y_1(M) \hookrightarrow X_1(M)$ be the natural inclusion and $f : E_1(M) \to Y_1(M)$ be the structure morphism of the universal elliptic curve over $\mathbb{Z}[1/M]$. We have maps from $M_k(N; \mathbb{C})$ and $S_k(N; \mathbb{C})$*

$$H^0(X_1(M), \omega^{k-2} \otimes \Omega^1_{X_1(M)}(D)) \otimes \mathbb{C} \hookrightarrow H^1(Y_1(M)^{\mathrm{an}}, \mathrm{Sym}^{k-2} R^1 f_* \underline{\mathbb{Z}}) \otimes \mathbb{C}$$

and

$$H^0(X_1(M), \omega^{k-2} \otimes \Omega^1_{X_1(M)} \otimes \mathbb{C} \hookrightarrow H^1(X_1(M)^{\mathrm{an}}, j_* \mathrm{Sym}^{k-2} R^1 f_* \underline{\mathbb{Z}}) \otimes \mathbb{C}$$

inducing ismorphisms compatible with Hecke operators on both sides

$$M_k(N; \mathbb{C}) \oplus \overline{S_k(N; \mathbb{C})} \cong H^1(Y_1(M)^{\mathrm{an}}, \mathrm{Sym}^{k-2} R^1 f_* \underline{\mathbb{Z}}) \otimes \mathbb{C}$$
$$S_k(N; \mathbb{C}) \oplus \overline{S_k(N; \mathbb{C})} \cong H^1(X_1(M)^{\mathrm{an}}, j_* \mathrm{Sym}^{k-2} R^1 f_* \underline{\mathbb{Z}}) \otimes \mathbb{C}.$$

The formulation above is that given in [FK12, 1.5.6]. The original statements for the cuspidal case in [Ei57] for weight $k = 2$ and in [Sh59] for general weight used parabolic group cohomology $H^i_P(\Gamma_1(M), V_k)$ in place of sheaf cohomology $H^i(X_1(M)^{\mathrm{an}}, j_* \mathrm{Sym}^{k-2} R^1 f_* \underline{\mathbb{Z}})$, where V_k is the symmetric power $\mathrm{Sym}^{k-2}(\mathbb{Z}^2)$ of the standard $\Gamma_1(M)$-module $\mathbb{Z}^2$. Under the identification $\pi_1(Y_1(M)^{\mathrm{an}}) \cong \Gamma_1(M)$, the module V_k is precisely $\Gamma(Y_1(M)^{\mathrm{an}}, \mathrm{Sym}^{k-2}R^1 f_*\underline{\mathbb{Z}})$, and $H^i(Y_1(M)^{\mathrm{an}}, \mathrm{Sym}^{k-2}R^1 f_*\underline{\mathbb{Z}})$ can be identified with usual group cohomology $H^i(\Gamma_1(M), V_k)$ (under the assumption that $M \geq 4$ as in the statement of Proposition 3.2.17). The group $H^i(X_1(M)^{\mathrm{an}}, j_*\mathrm{Sym}^{k-2}R^1 f_*\underline{\mathbb{Z}})$ can then be naturally identified with the subgroup of parabolic cohomology $H^i_P(\Gamma_1(M), V_k) \subset H^i(\Gamma_1(M), V_k)$. For the non-cuspidal case, one may compare dimensions as in [DI95, 12.2.2].

We now relate the Galois actions on the étale cohomology groups of the two models of modular curves via the isomorphisms v_M and w_M of the last section. We start by reminding the reader of the natural actions of $G_{\mathbb{Q}}$ on étale cohomology and on rational points. For $\sigma \in G_{\mathbb{Q}}$, one has induced isomorphisms over $\mathrm{Spec}(\mathbb{Q})$

$$1 \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\sigma) : X_1(M)_{\overline{\mathbb{Q}}} \to X_1(M)_{\overline{\mathbb{Q}}}$$
$$1 \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\sigma) : X_1^{\mu}(M)_{\overline{\mathbb{Q}}} \to X_1^{\mu}(M)_{\overline{\mathbb{Q}}}$$

which define right actions of $G_{\mathbb{Q}}$ on $X_1(M)_{\overline{\mathbb{Q}}}$ and on $X_1^{\mu}(M)_{\overline{\mathbb{Q}}}$ over $\mathbb{Q}$. These right actions give rise to the standard left actions on étale cohomology via pullback. On the other hand, the $\overline{\mathbb{Q}}$ points of $X_1^{(\mu)}(M)_{\overline{\mathbb{Q}}}$ and $X_1(M)_{\overline{\mathbb{Q}}}$ *over* $\overline{\mathbb{Q}}$ acquire right actions via the morphisms $1 \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\sigma)$ which agree with the natural left actions of σ^{-1} on points by precomposition with $\mathrm{Spec}(\sigma^{-1})$. From now on, we follow usual convention and denote $1 \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\sigma)$ simply by σ.

The map v_M gives an isomorphism defined over $\mathbb{Q}(\mu_M)$, so one has $\sigma \circ v_M = v_M \circ \sigma$ for $\sigma \in G_{\mathbb{Q}(\mu_M)}$.

Lemma 3.2.18. *For $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_M)/\mathbb{Q})$ corresponding to $a \in (\mathbb{Z}/M\mathbb{Z})^\times$, we have $v_M \circ \sigma = \langle a \rangle \circ \sigma \circ v_M$ as morphisms $X_1^{\mu}(M)_{\mathbb{Q}(\mu_M)} \to X_1(M)_{\mathbb{Q}(\mu_M)}$.*

Proof. On $\overline{\mathbb{Q}}$-points, the left-hand side acts as

$$\begin{aligned}(E, \zeta_M \mapsto P \in E[M](\overline{\mathbb{Q}})) &\mapsto (E^\sigma, \zeta_M^{-a} \mapsto \sigma^{-1}(P)) \\ &= (E^\sigma, \zeta_M \mapsto P) \\ &\mapsto (E^\sigma, 1 \mapsto P)\end{aligned}$$

while the right-hand side is the composition

$$\begin{aligned}(E, \zeta_M \mapsto P \in E[M](\overline{\mathbb{Q}})) &\mapsto (E, 1 \mapsto P) \\ &\mapsto (E^\sigma, 1 \mapsto a^{-1}P) \\ &\mapsto (E^\sigma, 1 \mapsto P).\end{aligned}$$

□

Remark 3.2.19. In [FK12, 1.4.5.(1)], it is claimed that $v_M \circ \sigma = \langle a \rangle \sigma \circ v_M$ as morphisms on cohomology. This is a typo, as they prove the formula holds as morphisms of schemes, and so on cohomology one would have $\sigma \circ v_M = v_M \circ \sigma \langle a \rangle$, where we abuse notation, as they do, and use the same symbols to denote pullbacks on cohomology. This latter equality can be rearranged to read $v_M^{-1} \circ \sigma = \langle a \rangle \sigma \circ v_M^{-1}$, which is needed to obtain the relation in [FK12, 1.6.4.(3)], although there it should also read $[\sigma]^{-1}$ in place of $\langle \sigma \rangle^{-1}$ (the latter symbol does not make sense in $\tilde{\Lambda}$). One may compare this also with the discussion after [Sh11, 4.4] and with [Oh95, 2.4.8].

We also take the time to point out that our Hecke operators and diamond operators agree with those of [FK12] and Ohta's. Their diamond operators are given as morphisms of schemes in 1.2.2 and 1.1.4 in agreement with our definition and coincide with the operators $T(q, q)$ of [Oh95, Oh99, Oh03] for weight $k = 2$. Next, note that our curve $Y_1(M, l)$, which we used to describe our Hecke correspondences, corresponds to their curve $Y_1((l), M)$ in 1.2.3. The isomorphism $Y_1((l), M) \to Y_1(1, M(l))$ given in [Ka04, 2.8] composed with their map denoted π is our $\pi_1^{(l)}$, and the inverse of the isomorphism composed with our $\pi_2^{(l)}$ is their ψ. Therefore, their Hecke operators in 1.2.3 denoted $T(l)$ and $T^*(l)$ (on Betti and étale cohomology) agree with our T_l and T_l^* and those denoted $T(l)$ and $T^*(l)$ in [Oh95].

3.2.4 Hecke algebras

As the Hecke operators defined on modular forms and on analytic and étale cohomologies of symmetric powers of local systems are compatible under the Eichler-Shimura isomorphism, the Hecke algebras we define on either of these spaces are naturally isomorphic.

Definition 3.2.20. *For $M \geq 5$ and a general commutative ring A, we define the Hecke algebra and dual Hecke algebra of level M over A*

$$\mathfrak{H}_k(M; A), \quad \mathfrak{H}_k^*(M; A)$$

to be the A-subalgebras of the endomorphism rings $\mathrm{End}_A(M_k^\mu(M; A))$ *generated by the Hecke operators T_l^μ and U_l^μ, respectively $T_l^{\mu*}$ and $U_l^{\mu*}$, and the diamond operators $\langle a \rangle$ for $a \in (\mathbb{Z}/M\mathbb{Z})^\times$. We similarly define the cuspidal Hecke algebras*

$$\mathfrak{h}_k(M; A), \quad \mathfrak{h}_k^*(M; A)$$

as subrings of $\mathrm{End}_A(S_k^\mu(M; A))$.

Note that for S/R a flat extension of rings, we have that $\mathfrak{H}_k(M; S) = \mathfrak{H}_k(M; R) \otimes_R S$ by Lemma 3.2.7 and standard flat base change results [SP, 02KH], and similarly for the other Hecke algebras. In general this is not true, for instance when one wishes to consider mod p modular forms and Hecke operators for $p \mid M$ (see also [DI95, Theorem 12.3.2]), but we will use less suggestive notation whenever we wish to consider a non-flat extension of rings. It is well-known that these Hecke algebras are commutative, and being subquotients of the finitely generated A-module $\mathrm{End}_A(M_k(M; A))$, that they are themselves finitely generated over A. In the case $A = \mathbb{Z}$, we see that the endomorphism rings are themselves free $\mathbb{Z}$-modules, and so the Hecke algebras are as well. This implies that the Hecke algebras are flat over any characterstic zero base ring.

We make a final remark concerning the choice of model of modular curves. The model $X_1(M)$ could have also been used in defining the Hecke algebras, but as the model $X_1^{\mu}(M)$ is one which recovers the integral theory of q-expansions at infinity, we opted to use the latter. Over a suitably large base ring, the alternatively defined Hecke algebras can be seen to be isomorphic to those defined above by again using v_M, though the integral theories may differ. As it should cause no confusion, and for simplicity of notation, we now drop the superscript μ on our Hecke operators and spaces of modular forms.

We similarly have an isomorphism between Hecke algebras and dual Hecke algebras via $T_l \leftrightarrow T_l^*$, $U_l \leftrightarrow U_l^*$, and $\langle a \rangle \leftrightarrow \langle a^{-1} \rangle$. However, we will need to distinguish between the two Hecke operators, and so we do not drop the superscript *.

We now describe a pairing between Hecke algebras and spaces of modular forms due originally to Hida. For a modular form f in $M_k(M;\mathbb{Z})$, we let $a_n(f)$ denote the coefficient of q^n in the power series expansion of f. For A an integral domain containing $\mathbb{Z}$ (i.e., a domain which is a flat $\mathbb{Z}$-algebra), we define a subspace of modular forms

$$m_k(M;A) := \{f \in M_k(M;Q(A)) \mid a_n(f) \in A \ \forall n \geq 1\}.$$

Consider the A-bilinear Hecke-equivariant pairing on $M_k(M;A) \times \mathfrak{H}_k(M;A)$ given by

$$(f, T) \mapsto a_1(Tf) \in A.$$

For any positive integer e and prime l, we define the Hecke operator $T_{l^e} \in \mathfrak{H}_k(M;A)$ for $k > 0$ recursively by $T_{l^e} := T_l T_{l^{e-1}} - l^{k-1}\langle l \rangle T_{l^{e-2}}$ for $e \geq 2$ where T_1 is definined to be the identity element of $\mathfrak{H}_k(M;A)$, where here for simplicity we also take $T_l = U_l$ for $l \mid M$. For any positive integer $n = \prod p_i^{e_i}$ with $p_i \neq p_j$ for $i \neq j$, we define further the Hecke operator $T_n := \prod T_{p_i^e}$. We may similarly define analogous dual Hecke operators (additionally using $\langle l \rangle^{-1}$ in place of $\langle l \rangle$). By studying the action of Hecke operators on q-expansions, one finds that

$$a_1(T_n f) = a_n(f)$$

for any form f. Note that this is not the case with the dual Hecke operators.

Proposition 3.2.21 (Hida)**.** *For $k > 0$, the pairing above is perfect and restricts to a perfect pairing on $S_k(M; A) \times \mathfrak{h}_k(M; A)$.*

The cuspidal case is given in [Hi00, 3.17]. The proof easily generalizes to the non-cuspidal case, and we sketch it below. Note that the restriction $k > 0$ is not explicitly mentioned in *loc. cit.* as it is unnecessary in the cuspidal case, and Hida's definition of modular forms for an arbitrary ring A is defined simply by $M_k(M; \mathbb{Z}) \otimes A$, which does not agree with our convention for non-flat $\mathbb{Z}$-algebras (cf. again Definition 3.2.5 and Lemma 3.2.7).

Proof. We treat only the non-cuspidal case, as the cuspidal case follows by the same argument. We have non-degeneracy of the pairing on the right, for if $T \in \mathfrak{H}$ is such that $a_1(Tf) = 0$ for all f, then for any given f we have

$$a_n(Tf) = a_1(T \cdot T_n f) = 0$$

as $T_n f$ is also a modular form. Thus, we conclude that Tf is constant, but as $k > 0$, this implies $Tf = 0$. We also have non-degeneracy on the left, for if f is such that $a_1(Tf) = 0$ for all T, then we can consider $T = T_n$ for all n and as before conclude that $f = 0$. Thus, the induced morphisms

$$\mathfrak{H}_k(M; A) \to \mathrm{Hom}_A(m_k(M; A), A), \quad m_k(M; A) \to \mathrm{Hom}_A(\mathfrak{H}_k(M; A), A)$$

and their cuspidal variants are injective. We wish to verify surjectivity. If A is a field, then surjectivity follows from finite-dimensionality of the spaces of modular forms. Consider the second of the displayed maps above. For any $\varphi \in \mathrm{Hom}_A(\mathfrak{H}_k(M; A), A)$, we may linearly extend φ to an element of $\mathrm{Hom}_A(\mathfrak{H}_k(M; Q(A)), Q(A))$ and obtain a form $f \in m_k(M; Q(A))$ such that $a_1(Tf) = \varphi(T)$ for all $T \in \mathfrak{H}_k(M; Q(A))$. We find that f actually lies in $m_k(M; A)$ as

$$a_n(f) = a_1(T_n f) = \varphi(T_n) \in A.$$

For surjectivity of the first map $\mathfrak{H}_k(M; A) \to \mathrm{Hom}_A(m_k(M; A), A)$, apply $\mathrm{Hom}_A(-, A)$ to the second map, and note that $\mathfrak{H}_k(M; A)$ is a finitely generated, free A-module, as A is flat over $\mathbb{Z}$, and so it is canonically isomorphic to its double dual. The composition

$$\mathfrak{H}_k(M;A) \cong \mathrm{Hom}_A(\mathrm{Hom}_A(\mathfrak{H}_k(M;A),A),A) \xrightarrow{\cong} \mathrm{Hom}_A(m_k(M;A),A)$$

agrees with the map induced by the pairing. □

We now work towards defining Hida's universal Hecke algebras and spaces of Λ-adic forms. Recall that for any positive d, M', M such that $dM' \mid M$, we have degeneracy maps $i_d : M_k(M';A) \hookrightarrow M_k(M;A)$, and so by restriction we have natural surjections $\mathfrak{H}_k(M;A) \to \mathfrak{H}_k(M';A)$. Let $p \mid M$ be a prime divisor and consider the p-adic Hecke algebras $\mathfrak{h}_k^{(*)}(M;\mathbb{Z}_p)$ and $\mathfrak{H}_k^{(*)}(M;\mathbb{Z}_p)$, which are semi-local rings, being finitely generated as $\mathbb{Z}_p$-modules. We consider the maximal quotient rings in which the operator U_p (respectively U_p^*) act invertibly, and we denote by e_M and e_M^* the idempotents of $\mathfrak{H}_k(M;\mathbb{Z}_p)$ and $\mathfrak{H}_k^*(M;\mathbb{Z}_p)$ giving the projections onto these direct factors. We use the same symbols to denote the analogous idempotents in the cuspidal Hecke algebras $\mathfrak{h}_k(M;\mathbb{Z}_p)$ and $\mathfrak{h}_k^*(M;\mathbb{Z}_p)$, which will be the images of e_M and e_M^* under the natural surjections coming from restriction.

We now fix an odd prime p and an integer N prime to p such that $Np \geq 4$ as well as a $k \geq 2$. We form the inverse limits

$$\mathfrak{H}_k'^{(*)}(N)_{\mathbb{Z}_p} := \varprojlim_r \mathfrak{H}_k^{(*)}(Np^r;\mathbb{Z}_p),$$

$$\mathfrak{h}_k'^{(*)}(N)_{\mathbb{Z}_p} := \varprojlim_r \mathfrak{h}_k^{(*)}(Np^r;\mathbb{Z}_p),$$

and for any $\mathbb{Z}_p$-algebra A, we set $\mathfrak{H}_k'^{(*)}(N)_A = \mathfrak{H}_k'^{(*)}(N)_{\mathbb{Z}_p}\widehat{\otimes}_{\mathbb{Z}_p} A$ and $\mathfrak{h}_k'^{(*)}(N)_A = \mathfrak{h}_k'^{(*)}(N)_{\mathbb{Z}_p}\widehat{\otimes}_{\mathbb{Z}_p} A$. We denote by e and e^* the idempotents given by the projective system of idempotents $(e_{Np^r})_r$ and $(e^*_{Np^r})_r$.

Definition 3.2.22. *Let K be a complete subfield of $\mathbb{C}_p$, and denote by $\mathcal{O}$ its ring of integers. Let $\Lambda_{\mathcal{O}}$ be the completed group ring $\mathcal{O}[[\Gamma]]$, and define the universal p-ordinary (adjoint) Hecke algebra of tame level N by*

$$\mathfrak{H}^{(*)}_{\Lambda_{\mathcal{O}}} := e^{(*)}\mathfrak{H}_k'^{(*)}(N)_{\mathcal{O}},$$

and let

$$\mathfrak{h}^{(*)}_{\Lambda_{\mathcal{O}}} := e^{(*)}\mathfrak{h}'^{(*)}_k(N)_{\mathcal{O}}$$

denote the universal p-ordinary cuspidal (adjoint) Hecke algebra of tame level N with coefficients in $\mathcal{O}$. When $K = \mathbb{Q}_p$, we often write $\mathfrak{h}^{(*)}$ in place of $\mathfrak{h}^{(*)}_{\Lambda_{\mathbb{Z}_p}}$.

We denote the elements of the universal Hecke algebras corresponding to the projective systems, $(T_l^{(*)})_r$, $(U_l^{(*)})_r$, and $(\langle a\rangle)_r$ by the same symbols $T_l^{(*)}$, $U_l^{(*)}$, and $\langle a\rangle$ that are used at finite level.

Note that in the definition above, our notation for the universal ordinary Hecke algebras does not include mention of the weight k of the finite level Hecke algebras. This is because in fact the algebras defined for various k are all canonically isomorphic: for the cuspidal Hecke algebras, this is [Hi86a, 1.1] for $p > 3$, and [Hi88b, 3.2] for general p; for the non-cuspidal algebra, only the case $p > 3$ is stated in [Oh99, 1.5.7], however the proof is an immediate corollary of a control theorem which is only proved in *loc. cit.* for $p > 3$, but a more general control theorem covering all primes is given in [AS95, 5.1]. We also drop N from the notation as N will be fixed for most of the dissertation, and we refer to the universal Hecke algebra often.

The usual and dual universal Hecke algebras are canonically $\tilde{\Lambda}$-algebras. We have a morphism of $\mathbb{Z}_p$-algebras $\tilde{\Lambda} \to \mathfrak{H}^*$ induced by $[\sigma] \mapsto \langle \kappa_{Np}(\sigma^{-1})\rangle$, and we further compose with the natural quotient to $\mathfrak{h}^*$ to obtain a $\tilde{\Lambda}$-algebra structure on the dual cuspidal Hecke algebra as well. For both algebras, the image of $\tilde{\Lambda}$ is isomorphic to the quotient $\tilde{\Lambda}/([-1]-1)$, where $[-1]$ is the group element in $\mathbb{Z}_p[[\mathbb{Z}_{p,N}^\times]] \cong \tilde{\Lambda}$. The $\tilde{\Lambda}$-structures on the non-adjoint Hecke algebras are obtained by using instead the non-inverted diamond operators, and we see that the isomorphism $\mathfrak{H} \cong \mathfrak{H}^*$ described above is one of $\tilde{\Lambda}$-algebras.[3] We now state the control theorem for the ordinary universal Hecke algebras.

[3]Note that we may have defined these $\tilde{\Lambda}$-algebra structures before taking ordinary parts. However, those algebras are not isomorphic to one another, and in particular the operator $\langle -1\rangle$ acts as $(-1)^k$ in the weight k Hecke algebras. That Ohta wished to work more generally is one of the reasons why in [Oh95], the $\tilde{\Lambda}$-algebra structure is defined so that $[d]$ acts as $T^{(*)}(d,d) = d^{k-2}\langle d\rangle$.

Proposition 3.2.23 ([Hi88b, 3.4], [Oh99, 1.5.7]). *Let $\omega_r = \gamma^r - 1 \in \Lambda_{\mathcal{O}}$. The canonical maps*

$$\mathfrak{h}_{\Lambda_{\mathcal{O}}}^{(*)}/\omega_r \to e^{(*)}\mathfrak{h}_2^{(*)}(Np^r;\mathcal{O})$$

and

$$\mathfrak{H}_{\Lambda_{\mathcal{O}}}^{(*)}/\omega_r \to e^{(*)}\mathfrak{H}_2^{(*)}(Np^r;\mathcal{O})$$

are isomorphisms.

The cuspidal case is treated fully in [Hi88b], and the non-cuspidal case is treated in [Oh99] for $p > 3$. The argument of the latter reference compares the $\Lambda_{\mathcal{O}}$-rank of the universal Hecke algebra with the $\mathcal{O}$-rank of the finite level Hecke algebra. This rank is given in [Hi86a, Lemma 5.3] by counting the number of linearly independent p-ordinary Eisenstein series, and the proof there still works with $p = 3$ (assuming $N \geq 2$). We will give further properties of these Hecke algebras in the section below, after introducing spaces of Λ-adic forms.

3.3 Λ-adic forms

In this section, we define Λ-adic forms following [FK12] and [Oh95] as certain power series specializing to q-expansions of classical modular forms and relate them to inverse limits of spaces of modular forms.

We start off with bringing to attention the choice of normalization made in [Oh95, 2.1.1] and [Oh99, 1.5.1] for the weight k slash operator of a rational matrix $\delta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{Q})$ with positive determinant on a modular form $f \in M_k(M;\mathbb{C})$

$$(f|_k\delta)(z) := \det(\delta)(cz+d)^{-k} f(\frac{az+b}{cz+d}).$$

The normalizing term $\det(\delta)$ differs from that used in standard references such as [Se72, 3.1.a] and [Sh59, §3.4], which use $\det(\delta)^{k/2}$, and [Hi93, 5.1] and [DS05, pg. 165], which use $\det(\delta)^{k-1}$. The algebraic Atkin-Lehner involution $v_M^{-1} \circ w_M$ acting on the space of modular forms

$H^0(X_1(M)_A, \omega_A^{\otimes k})$ agrees with the analytically defined involution given by $|_k\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ when the action is defined *without* a factor of $\det(\delta)$, as we now explain.

The analytified algebraic $v_M^{-1} \circ w_M$ on the universal family of elliptic curves with an M-torsion point introduced in 3.2.1 sends $(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{M})$ to $(\mathbb{C}/(\frac{1}{M}\mathbb{Z}+\tau\mathbb{Z}), \frac{\tau}{M})$, which via homothety is isomorphic to $(\mathbb{C}/(\mathbb{Z}+M\tau\mathbb{Z}), \tau)$. Further acting by $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ gives an isomorphism with $(\mathbb{C}/(\mathbb{Z}+\frac{-\tau}{M}\mathbb{Z}), \frac{1}{M})$. Thus, we see that $v_M^{-1} \circ w_M$ acts on $f(z)(d\zeta)^{\otimes k}$ by pulling it back to $(Mz)^{-k} f(-1/Mz)(d\zeta)^{\otimes k}$. We may also consider the action of $v_M^{-1} \circ w_M$ on $H^0(X_1(M)_A, (\omega^{\otimes k-2} \otimes \Omega^1_{X_1(M)}(D))_A)$, where we find $f(z)$ is sent to $M(Mz)^{-k} f(-1/Mz)$. For simplicity, we write w_M in place of $v_M^{-1} \circ w_M$ for the remainder of this section.

Remark 3.3.1. In [La15b, §2], Lafferty takes Ohta's convention in defining the weight k operator, but does not adjust the normalization of the double coset operators. This leads to the operator denoted $T_{d,d}$ in *loc. cit.* for $d \in (\mathbb{Z}/M\mathbb{Z})^\times$ to operate on $M_K(M;\mathbb{C})$ as $d^{2-k}\langle d \rangle$. This leads to some incorrect formulas in the paper. E.g., the formula on page 744 of [La15b] which describes the effect of Hecke operators on Fourier coefficients is off by a factor of d^{k-1}. On the other hand, in Lafferty's dissertation [La15a, 2.1], he takes the normalization with the factor $\det(\delta)^{k-1}$, but does not mention Ohta's convention when citing some of Ohta's results. In [FK12, 1.5.9], they take Ohta's convention, but introduce a sign factor of $(-1)^k$. This sign is needed for a pairing that they define in [FK12, 1.6].

We now take Fukaya and Kato's convention in defining the Atkin-Lehner operator w_M acting on $M_k(M;A)$ and define spaces of modular forms whose Atkin-Lehner duals have integral Fourier coefficients

$$\begin{aligned} M_k^*(M;\mathbb{Z}) &= \{f \in M_k(M;\mathbb{Q}) \mid a_n(w_M(f)) \in \mathbb{Z}[[q]] \text{ for } n \geq 0\}, \\ m_k^*(M;\mathbb{Z}) &= \{f \in M_k(M;\mathbb{Q}) \mid a_n(w_M(f)) \in \mathbb{Z}[[q]] \text{ for } n \geq 1\}, \\ S_k^*(M;\mathbb{Z}) &= \{f \in S_k(M;\mathbb{Q}) \mid a_n(w_M(f)) \in \mathbb{Z}[[q]] \text{ for } n \geq 1\}. \end{aligned}$$

We set $M_k^*(M;A) = M_k^*(M;\mathbb{Z}) \otimes A$, and similarly for $m_k^*(M;A)$ and $S_k^*(M;A)$, for any ring A. For p an odd prime and N a positive integer coprime to p such that $Np > 4$, by direct computation as in [Oh95, 2.3], one can show that the trace maps $\pi_{1*} : M_k(Np^{r+1}; \mathbb{Q}) \to M_k(Np^r; \mathbb{Q})$ take $M_k^*(Np^{r+1}; \mathbb{Z})$ into $M_k^*(Np^r; \mathbb{Z})$ for $r \geq 1$, and similarly for $m_k^*(M; A)$ and $S_k^*(M; A)$. Additionally, these trace maps are compatible with the actions of $\mathfrak{H}_k^*(Np^{r(+1)}; \mathbb{Z})$ and $\mathfrak{h}_k^*(Np^{r(+1)}; \mathbb{Z})$, which then can be seen to stabilize $M_k^*(Np^r; \mathbb{Z})$, $m_k^*(Np^r; \mathbb{Z})$, and $S_k^*(Np^r; \mathbb{Z})$.

Definition 3.3.2. *Let K be a complete subfield of $\mathbb{C}_p$, and denote by $\mathcal{O}$ its ring of integers. Let $\Lambda_{\mathcal{O}}$ be the completed group ring $\mathcal{O}[[\Gamma]]$, and fix an integer $k \geq 2$. Define*

$$\mathfrak{M}_k'^*(N)_{\Lambda_{\mathcal{O}}} := \varprojlim_r M_k^*(Np^r; \mathcal{O}),$$

$$\mathfrak{m}_k'^*(N)_{\Lambda_{\mathcal{O}}} := \varprojlim_r m_k^*(Np^r; \mathcal{O}),$$

$$\mathfrak{S}_k'^*(N)_{\Lambda_{\mathcal{O}}} := \varprojlim_r S_k^*(Np^r; \mathcal{O}),$$

and further set

$$\mathfrak{M}_{k,\Lambda_{\mathcal{O}}}^* := e^* \mathfrak{M}_k'^*(N)_{\Lambda_{\mathcal{O}}},$$

$$\mathfrak{m}_{k,\Lambda_{\mathcal{O}}}^* := e^* \mathfrak{m}_k'^*(N)_{\Lambda_{\mathcal{O}}},$$

$$\mathfrak{S}_{k,\Lambda_{\mathcal{O}}}^* := e^* \mathfrak{S}_k'^*(N)_{\Lambda_{\mathcal{O}}}.$$

Recall our notation $U_r = 1 + p^r\mathbb{Z}_p \leqslant U_1$. Define for any finite order character $\epsilon \in \widehat{U}_1$ factoring through U_1/U_r and any ring A containing the values of ϵ, the subspace

$$M_k(Np^r, \epsilon; A) = \{f \in M_k(Np^r; A) \mid \langle a \rangle f = \epsilon(a) f \; \forall a \in U_1\},$$

and define $S_k(Np^r, \epsilon; A)$ analogously.

For K and $\mathcal{O}$ as above, we now define spaces of $\Lambda_{\mathcal{O}}$-adic modular forms as power series that specialize to classical modular forms. We will often suppress the coefficient ring $\mathcal{O}$ in the terminology and refer to them simply as Λ-adic forms.

Definition 3.3.3. *A $\Lambda_{\mathcal{O}}$-adic modular form (resp. cusp form) of level N and weight $k \geq 2$ is a power series*

$$\mathcal{F} = \sum_{n=0}^{\infty} a_n(\mathcal{F}) q^n \in \Lambda_{\mathcal{O}}[[q]]$$

in q with $a_n(\mathcal{F}) \in \Lambda_{\mathcal{O}}$ such that for all but finitely many characters $\epsilon \in \widehat{U}_1$, the power series

$$\mathcal{F}_{\epsilon,k} := \sum_{n=0}^{\infty} a(n;\mathcal{F})(\epsilon(\gamma)\gamma^{k-2} - 1)q^n$$

is the q-expansion of a modular form in $M_k(Np^r, \epsilon; \mathcal{O}[\epsilon])$ (resp. cusp form in $S_k(Np^r, \epsilon; \mathcal{O}[\epsilon])$) where $ker(\epsilon) = U_r$. We denote the space of all $\Lambda_{\mathcal{O}}$-adic modular forms (resp. cusp forms) of level N and weight k by $M'_k(N; \Lambda_{\mathcal{O}})$ (resp. $S'_k(N; \Lambda_{\mathcal{O}})$). We further take the ordinary parts and drop N from the notation in setting

$$M_{k,\Lambda_{\mathcal{O}}} = eM'_k(N; \Lambda_{\mathcal{O}})$$
$$S_{k,\Lambda_{\mathcal{O}}} = eS'_k(N; \Lambda_{\mathcal{O}}).$$

We define $m_{k,\Lambda_{\mathcal{O}}} := (M_{k,\Lambda_{\mathcal{O}}} \otimes_{\Lambda_{\mathcal{O}}} Q(\Lambda_{\mathcal{O}})) \cap (Q(\Lambda_{\mathcal{O}}) + q\Lambda_{\mathcal{O}}[[q]])$, and by abuse of terminology we call it also the space of $\Lambda_{\mathcal{O}}$-adic forms.

Proposition 3.3.4 (Hida, Wiles, Ohta)**.** *The $\Lambda_{\mathcal{O}}$-modules $M_{k,\Lambda_{\mathcal{O}}}$, $m_{k,\Lambda_{\mathcal{O}}}$, and $S_{k,\Lambda_{\mathcal{O}}}$ are finitely generated and free.*

For the cuspidal case, under the conditions that $p \geq 5$ and $\mathcal{O}$ is finite over $\mathbb{Z}_p$, Hida in [Hi86b, 2.2, 3.1] proves finiteness and freeness over $\Lambda_{\mathcal{O}}$ of the full and cuspidal universal ordinary Hecke algebras as well as the duality of the Hecke algebras with spaces of $\Lambda_{\mathcal{O}}$-adic forms. However, there the theory of Λ-adic forms is not presented using power series rings over Λ as above.

The presentation of Λ-adic forms in [Hi93, 7.3] is close to what we have above, the difference being that following Ohta, we have fixed a choice of weight k. Nevertheless, a proof of the claim for $M_{k,\Lambda_{\mathcal{O}}}$ and $S_{k,\Lambda_{\mathcal{O}}}$ for all primes p when $N = 1$ and $\mathcal{O}$ is finite over $\mathbb{Z}_p$ can be obtained from [Hi93, 7.3 Theorem 1], where it is attributed to Wiles. The proof works just the same without the condition that $N = 1$, and the condition that $\mathcal{O}$ is finite over $\mathbb{Z}_p$ can also be removed, as we now explain.

In the proof of the theorem, the finiteness condition is used to deduce compactness of $\Lambda_{\mathcal{O}}$, and this compactness is used to deduce that $\mathcal{O}$-finite, freeness of the reduction of $M_{k,\Lambda_{\mathcal{O}}}$ by the ideal $(P_k) \subset \Lambda_{\mathcal{O}}$, implies $\Lambda_{\mathcal{O}}$-finite, freeness of $M_{k,\Lambda_{\mathcal{O}}}$, where $P_k = T - (\gamma^k - 1)$. However, one may simply use instead Nakayama's lemma for this last claim.

As we work with a fixed weight k, we must also modify slightly the proof to consider instead of P_k some other element of $\Lambda_{\mathcal{O}}$ to deduce freeness. This is what is done in [Oh99, Lemma 2.4.6] (under the ambient but inessential assumption that $p \geq 5$), though the proof does not explicitly address the needed workaround of the compactness step of Hida's argument. The claim for $m_{k,\Lambda_{\mathcal{O}}}$ is [Oh99, Remark 2.5.5] and can be proved in the same manner as it was for $M_{k,\Lambda_{\mathcal{O}}}$. We additionally remark that the proof of $\Lambda_{\mathcal{O}}$-freeness in [La15a, Proposition 2.2.2] is incomplete, as it assumes $\mathcal{O}$ is a PID, which is only the case if $\mathcal{O}$ is finitely ramified over $\mathbb{Z}_p$.

Proposition 3.3.5 ([Oh95, 2.3.6], [Oh99, 2.2.3])**.** *For $k \geq 2$, we have isomorphisms of $\Lambda_{\mathcal{O}}$-modules*

$$M_{k,\Lambda_{\mathcal{O}}} \cong \mathfrak{M}^*_{k,\Lambda_{\mathcal{O}}},$$
$$m_{k,\Lambda_{\mathcal{O}}} \cong \mathfrak{m}^*_{k,\Lambda_{\mathcal{O}}},$$
$$S_{k,\Lambda_{\mathcal{O}}} \cong \mathfrak{S}^*_{k,\Lambda_{\mathcal{O}}},$$

where $\Lambda_{\mathcal{O}}$ acts on the left-hand spaces by scalar multiplication and on the right-hand spaces via their $\mathfrak{H}^*_{\Lambda_{\mathcal{O}}}$-structures. The maps are explicitly given by $F \mapsto (f_r)_r$, where

$$f_r = \frac{1}{p^{r-1}} \left(\sum_{\epsilon : U_1/U_r \to \overline{\mathbb{Q}}^\times} w_{Np^r}^{-1} U_p^{-r} F(\epsilon(\gamma)\gamma^{k-2} - 1) \right),$$

with inverse $(g_r)_r \mapsto G$, where G is the unique element satisfying

$$G(\epsilon(\gamma)\gamma^{k-2} - 1) = \sum_{a \in U_1/U_r} \epsilon(a) \langle a \rangle^{-1} U_p^r w_{Np^r} g_r$$

for all $\epsilon : U_1/U_r \to \overline{\mathbb{Q}}^\times$, where we view $U_1/U_r \leqslant (\mathbb{Z}/Np^r\mathbb{Z})^\times$ in order to define $\langle a \rangle$.

Though Ohta only made the claim for $p \geq 5$ for the cases of $M_{k,\Lambda_{\mathcal{O}}}$ and $S_{k,\Lambda_{\mathcal{O}}}$, the proof works just as well when $p = 3$ and for $m_{k,\Lambda_{\mathcal{O}}}$. The proposition allows us to import the

$\mathfrak{H}^*_{\Lambda_\mathcal{O}}$-module structure of the right-hand terms to the left-hand terms. The effects of the adjoint Hecke operators T_l^* on the coefficients of Λ-adic forms specialize to the usual effects of the standard Hecke operators T_l on Fourier coefficients of classical modular forms.

Remark 3.3.6. Various authors make different conventions in defining and notating a Hecke-module structure on the space of Λ-adic forms. We give a summary here for the primary references used in this dissertation.

In [Oh95], the $\mathfrak{h}^*$-module structure on the projective limit of spaces of classical modular forms is imported to the space of Λ-adic forms as was done above. However, via the isomorphism $\mathfrak{h}^* \cong \mathfrak{h}$, the space of Λ-adic forms is considered throughout as an $\mathfrak{h}$-module. The papers [Oh99, Oh00, Oh03, Oh20] and [La15b] adopt this convention as well.

In [FK12], only the inverse limit of spaces of classical forms with a dual Hecke structure is considered. They embed this space into a power series ring over $\tilde{\Lambda}$. However, the $\tilde{\Lambda}$-module structure on its image via its Hecke-module structure is actually the inverse of the $\tilde{\Lambda}$ action afforded by scalar multiplication under the involution $[a] \mapsto [a]^{-1}$ for $a \in \mathbb{Z}_{p,N}^\times$.

We write $\tilde{\Lambda}_\mathcal{O}$ for $\mathcal{O}[[\mathbb{Z}_{p,N}^\times]] = \Lambda_\mathcal{O}[\Delta]$. Following [FK12, 1.5.11], we may embed $S_{k,\Lambda_\mathcal{O}}$ and $M_{k,\Lambda_\mathcal{O}}$ into $\tilde{\Lambda}_\mathcal{O}[[q]]$ and $m_{k,\Lambda_\mathcal{O}}$ into $Q(\tilde{\Lambda}_\mathcal{O}) + q\tilde{\Lambda}_\mathcal{O}[[q]]$ by

$$(f_r)_r \mapsto \varprojlim_r \left(\sum_{a \in (\mathbb{Z}/Np^r\mathbb{Z})^\times} \langle a^{-1} \rangle T(p)^r w_{Np^r}(f) \cdot [a] \right).$$

We denote their images by $S_{k,\tilde{\Lambda}_\mathcal{O}}$, $M_{k,\tilde{\Lambda}_\mathcal{O}}$, and $m_{k,\tilde{\Lambda}_\mathcal{O}}$. For uniformity, we may also write $\mathfrak{h}^{(*)}_{\tilde{\Lambda}_\mathcal{O}}$ for $\mathfrak{h}^{(*)}_{\Lambda_\mathcal{O}}$. The following duality result lifts the finite level dualities between spaces of modular forms and Hecke algebras.

Proposition 3.3.7 (Hida, Ohta)**.** *There is a perfect $\tilde{\Lambda}_\mathcal{O}$-bilinear pairing of $\tilde{\Lambda}_\mathcal{O}$-modules $m_{k,\tilde{\Lambda}_\mathcal{O}} \times \mathfrak{H}^*_{\tilde{\Lambda}_\mathcal{O}} \to \tilde{\Lambda}_\mathcal{O}$ given by*

$$(f, T) \mapsto a_1(Tf)$$

which furthermore restricts to a perfect pairing $S_{k,\tilde{\Lambda}_\mathcal{O}} \times \mathfrak{h}^*_{\tilde{\Lambda}_\mathcal{O}} \to \tilde{\Lambda}_\mathcal{O}$. The analogous claim for $\Lambda_\mathcal{O}$ in place of $\tilde{\Lambda}_\mathcal{O}$ also holds.

The proof that the natural map $m_{k,\Lambda_{\mathcal{O}}} \to \mathrm{Hom}_{\Lambda_{\mathcal{O}}}(\mathfrak{H}^*_{k,\Lambda_{\mathcal{O}}}, \Lambda_{\mathcal{O}})$ is an isomorphism works just as it did in the finite level case in Proposition 3.2.21. That $\mathfrak{H}^*_{\Lambda_{\mathcal{O}}} \to \mathrm{Hom}_{\Lambda_{\mathcal{O}}}(m_{k,\Lambda_{\mathcal{O}}}, \Lambda_{\mathcal{O}})$ is an isomorphism requires a bit more work, as we do not yet know that $\mathfrak{H}^*_{\Lambda_{\mathcal{O}}}$ is finitely generated and free as a $\Lambda_{\mathcal{O}}$-module. In [Oh99, 1.5.7] it is directly proved that it is finite and free in the case that $p \geq 5$. In [Hi93, 7.5 Theorem 5], the duality is proved directly when $\mathcal{O}$ is a DVR, i.e., when it is finitely ramified over $\mathbb{Z}_p$, which then implies it in general. To obtain a $\tilde{\Lambda}_{\mathcal{O}}$-adic perfect pairing from a $\Lambda_{\mathcal{O}}$-adic one, one can use Lemma 4.1.6 below. The same argument applies for the cuspidal pairing.

This duality result allows us to deduce properties of the Hecke algebras from the spaces of Λ-adic forms and vice versa.

Corollary 3.3.8. *The Hecke algebras $\mathfrak{H}^{(*)}_{\Lambda_{\mathcal{O}}}$ and $\mathfrak{h}^{(*)}_{\Lambda_{\mathcal{O}}}$ are finitely generated and free as $\Lambda_{\mathcal{O}}$-modules, and the spaces of $\tilde{\Lambda}_{\mathcal{O}}$-adic forms $m_{k,\tilde{\Lambda}_{\mathcal{O}}}$, $M_{k,\tilde{\Lambda}_{\mathcal{O}}}$, and $S_{k,\tilde{\Lambda}_{\mathcal{O}}}$ inside $Q(\tilde{\Lambda}_{\mathcal{O}}[[q]])$ are independent of k. Denoting $\omega_r = [\gamma^{p^{r-1}}] - 1 \in \Lambda_{\mathcal{O}}$, the natural maps*

$$S_{k,\Lambda_{\mathcal{O}}}/\omega_r S_{k,\Lambda_{\mathcal{O}}} \to e^* S_2^*(Np^r; \mathcal{O})$$

and

$$M_{k,\Lambda_{\mathcal{O}}}/\omega_r M_{k,\Lambda_{\mathcal{O}}} \to e^* M_2^*(Np^r; \mathcal{O})$$

are isomorphisms for all $k \geq 2$.

We have the following commutative algebra lemma.

Lemma 3.3.9. *Let R be an integral domain, and let S be an R-finite, R-torsion-free R-algebra. Then we have an isomorphism $S \otimes_R Q(R) \cong Q(S)$ of S-algebras. In particular, for any S-finite S-module M, the S-torsion and R-torsion of M coincide.*

Proof. We have a well-defined injection $S \otimes_R Q(R) \hookrightarrow Q(S)$ of S-algebras as S is R-torsion-free. We wish to see that any non-zero-divisor s of S is already invertible in the left-hand side. The endomorphism of S given by multiplication by s is injective and extends to an injection on the finite-dimensional $Q(R)$-vector space $S \otimes_R Q(R)$ as $Q(R)$ is R-flat, being a localization of R, and so must be an isomorphism.

For the final claim, recall that the S-torsion elements of M are given by the kernel of the map $M \to M \otimes_S Q(S)$, and note that $M \otimes_S Q(S) \cong M \otimes_S S \otimes_R Q(R) \cong M \otimes_R Q(R)$. □

The lemma then gives us the isomorphisms $Q(\mathfrak{h}) \cong \mathfrak{h} \otimes_\Lambda Q(\Lambda) \cong \mathfrak{h} \otimes_{\tilde{\Lambda}} Q(\tilde{\Lambda})$ as both $\mathfrak{h}$ and $\tilde{\Lambda}$ are finite, free Λ-modules, and the analogous statements hold for the non-cuspidal and dual Hecke algebras as well.

By Corollary 3.3.8, we may and do drop the weight k from the notation for our spaces of modular forms, denoting them by $M_{\tilde{\Lambda}_\mathcal{O}}, S_{\tilde{\Lambda}_\mathcal{O}} \subset Q(\tilde{\Lambda}_\mathcal{O})[[q]]$.

3.3.1 p-adic L-functions, $\tilde{\Lambda}$-adic Eisenstein series, and the Eisenstein ideal

Below we define particular $\tilde{\Lambda}$-adic modular forms which interpolate classical Eisenstein series, following [La15b, §3.2] and [Oh03, §1.4]. Before doing so, we first detail the construction of an element $\xi \in \tilde{\Lambda} = \mathbb{Z}_p[\Delta][[U_1]] \cong \mathbb{Z}_p[\Delta][[T]]$ which specializes along the quotient maps $\tilde{\Lambda} \to \tilde{\Lambda}_\theta \cong \mathbb{Z}_p[\theta][[T]]$ induced by even characters θ of Δ to power series corresponding to Kubota-Leopoldt p-adic L-functions as in [FK12, §4.1]. The reason for doing so is that these power series are the constant terms of the Λ-adic Eisenstein series.

We follow the exposition of [Wa97, §7.2], where it is assumed that the characters θ are primitive. The reader may also wish to compare this with the original construction of Iwasawa in [Iw69]. We fix an odd prime p and positive integer N such that $p \nmid N$ for this section (there is no need to assume that $Np > 3$ in this section – allowing $p = 2$ is also possible if one modifies some of the arguments; cf. Washington).

We write $\Delta_r = (\mathbb{Z}/Np^r\mathbb{Z})^\times$ for brevity. For any $x \in \mathbb{Z}_{p,N}^\times$ we denote the corresponding group-like element in $\mathbb{Z}_p[\Delta_r]$ by $[x]_{\Delta_r}$, and we write $[x]_{\Delta_r} = [x]_\Delta [x]_{U_r}$ corresponding to the decomposition of x in $\Delta_r = \Delta \times (1 + p\mathbb{Z})/p^r\mathbb{Z}$. By slight abuse of notation, we write $[1 + p]$ for the group-like element corresponding to $1 + p \in (\mathbb{Z}/p^r\mathbb{Z})^\times \leqslant \Delta_r$. We define for each integer $r \geq 1$

$$\xi_r^{(0)} := -\frac{1}{Np^r} \sum_{\substack{a=1 \\ (a,Np)=1}}^{Np^r} a[a]_{\Delta_r} \in Q(\mathbb{Z}_p[\Delta_r]),$$

and

$$\eta_r^{(0)} := (1 - (1+p)[1+p])\xi_r^{(0)}.$$

For a given r and any $1 \leq a \leq Np^r$ coprime to Np, we associate to a the unique $a_1, a_2 \in \mathbb{Z}$ such that $0 \leq a_1 < Np^r$ satisfying

$$a = a_1 + a_2 Np^r.$$

We may then rewrite

$$\begin{aligned}\eta_r^{(0)} &= \xi_r^{(0)} + \frac{1}{Np^r} \sum_{\substack{a=1 \\ (a,Np)=1}}^{Np^r} (a_1 + a_2 Np^r)[a_1]_{\Delta_r} \\ &= \sum_{\substack{a=1 \\ (a,Np)=1}}^{Np^r} a_2 [a_1]_{\Delta_r}\end{aligned}$$

and see that $\eta_r^{(0)}$ is in fact integral.

Lemma 3.3.10. *The specializations of $\xi_r^{(0)}$ and $\eta_r^{(0)}$ at odd characters θ of Δ are compatible under the natural quotient maps $Q(\mathbb{Z}_p[\Delta_{r+1}])_\theta \to Q(\mathbb{Z}_p[\Delta_r])_\theta$.*

Proof. Denote the projection map $Q(\mathbb{Z}_p[\Delta_{r+1}]) \to Q(\mathbb{Z}_p[\Delta_r])$ by ϕ_r. We have

$$\begin{aligned}\phi_r(\xi_{r+1}^{(0)}) &= -\frac{1}{Np^{r+1}} \sum_{\substack{a=1 \\ (a,Np)=1}}^{Np^{r+1}} a[a]_{\Delta_r} \\ &= -\frac{1}{Np^{r+1}} \sum_{\substack{a=1 \\ (a,Np)=1}}^{Np^r} \sum_{i=0}^{p-1} (a + iNp^r)[a]_{\Delta_r} \\ &= -\frac{1}{Np^{r+1}} \sum_{\substack{a=1 \\ (a,Np)=1}}^{Np^r} p(a + \frac{p-1}{2} Np^r)[a]_{\Delta_r} \\ &= \xi_r - \frac{p-1}{2} \sum_{\substack{a=1 \\ (a,Np)=1}}^{Np^r} [a]_{\Delta_r}.\end{aligned}$$

We have that $[a]_{U_r} = [-a]_{U_r}$, and so for odd θ, the specialization at θ of the final sum can be seen to vanish by pairing the summands corresponding to the indices a and $-a$. The claim for $\eta_r^{(0)}$ follows from that for $\xi_r^{(0)}$. $\square$

Recall that $\Delta' \leqslant \Delta$ denotes the prime-to-p part of Δ. The element $-1 \in \Delta$ in fact lives in Δ' as p is odd, and so it makes sense to describe characters of Δ' as either odd or even, and as $\tilde{\Lambda}_{\mathbb{Z}_p}$ decomposes into a direct product of local rings indexed by Galois-conjugacy classes of characters of Δ', we may describe a local direct factor as odd or even in the case that it corresponds to a class of odd or even characters of Δ'.

Definition 3.3.11. *We define $\eta^{(0)} \in \tilde{\Lambda}$ and $\xi^{(0)} \in Q(\tilde{\Lambda})$ to be the sums of the odd components of the inverse limits of the $\eta_r^{(0)}$ and $\xi_r^{(0)}$ along the natural quotient maps. For any integer $t \geq 0$, we further define the twists*

$$\eta^{(t)} = \mathrm{Tw}_t(\eta^{(0)}),\ \xi^{(t)} = \mathrm{Tw}_t(\xi^{(0)})$$

where $\mathrm{Tw}_t : Q(\tilde{\Lambda}) \xrightarrow{\cong} Q(\tilde{\Lambda})$ is induced by $[(a,b)] \mapsto a^t[(a,b)]$ for $(a,b) \in \mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$.

Note that the twisting map Tw_t sends the idempotent associated with the Galois conjugacy class of a character θ to that of $\theta\omega^{-t}$, and so $\eta^{(t)}$ and $\xi^{(t)}$ are only nontrivial on components whose parities agree with that of $t+1$.

Writing $\tilde{\Lambda} = \varprojlim_r \mathbb{Z}/p^r\mathbb{Z}[\Delta_r]$, we may represent $\eta^{(t)}$ by the inverse system

$$\eta_r^{(t)} := (1 - (1+p)^{1+t}[1+p]) \sum_{\substack{a=1 \\ (a,Np)=1}}^{Np^r} a^{1+t}[a]_{\Delta_r}$$

modulo p^r on parity-of-$(t+1)$ components. Alternatively, we may also represent $\eta^{(t)}$ by the inverse system

$$\eta_r^{(t)} \equiv \sum_{\substack{a=1 \\ (a,Np)=1}}^{Np^r} a_2 a_1^t [a_1]_{\Delta_r} \pmod{p^r}$$

on parity-of-$(t+1)$ components, though note that while the a_1 are level-compatible, the a_2 are not. For any character θ of Δ, we let $\eta_\theta^{(t)}$ denote the image of $\eta^{(t)}$ under the quotient map $\tilde{\Lambda} \to \tilde{\Lambda}_\theta$.

Let $\tilde{g}_\theta^{(t)}(T), h^{(t)}(T) \in \mathbb{Z}_p[\theta][[T]]$ be the power series corresponding to $\eta_\theta^{(t)}$ and $(1-(1+p)^{1+t}[1+p])$ under the usual correspondence $[1+p] \leftrightarrow 1+T$, so that $\xi_\theta^{(t)}$ corresponds to $g_\theta^{(t)} := \tilde{g}_\theta^{(t)}/h^{(t)}$. We have the following interpolation property for $\tilde{g}_\theta^{(t)}$.

Proposition 3.3.12. *For any integer $m \geq 1$ and finite order character ψ of U_1, we have*

$$\begin{aligned}&\tilde{g}_\theta^{(t)}(\psi(1+p)(1+p)^{m-1}-1)\\ &\qquad = -h^{(t)}(\psi(1+p)(1+p)^{m-1}-1)(1-\theta\psi\omega^{1-m}(p)p^{m+t-1})\frac{B_{m+t,\theta\psi\omega^{1-m}}}{m+t}\end{aligned}$$

where $B_{m+t,\theta\psi\omega^{1-m}}$ is the $(m+t)$th generalized Bernoulli number associated with $\theta\psi\omega^{1-m}$.

Proof. We have

$$\tilde{g}_\theta^{(t)}(T) \equiv \sum_{\substack{a=1\\(a,Np)=1}}^{Np^r} a_2 a_1^t \theta(a_1)(1+T)^{i(a_1)} \pmod{(1+T)^{p^r}-1}.$$

Therefore, for r sufficiently large, we have

$$\begin{aligned}\tilde{g}_\theta^{(t)}(\psi(1+p)(1+p)^{m-1}-1) &\equiv \sum_{\substack{a=1\\(a,Np)=1}}^{Np^r} a_2 a_1^t \theta(a_1)(\psi(1+p)(1+p)^{m-1})^{i(a_1)}\\ &\equiv \sum_{\substack{a=1\\(a,Np)=1}}^{Np^r} a_2 \theta\psi\omega^{1-m}(a_1) a_1^{m+t-1} \pmod{p^r}. \end{aligned} \tag{3.3.1}$$

The congruence

$$(a_1+a_2Np^r)^{m+t} \equiv a_1^{m+t} + (m+t)a_2Np^r a_1^{m+t-1} \pmod{p^{2r}},$$

implies that for r large enough so that $\mathrm{cond}(\theta\psi)$ divides Np^r, we have

$$\theta\psi\omega^{1-m}(1+p)(1+p)^{m+t} \sum_{\substack{a=1\\(a,Np)=1}}^{Np^r} \theta\psi\omega^{1-m}(a)a^{m+t}$$
$$\equiv \sum_{\substack{a=1\\(a,Np)=1}}^{Np^r} \theta\psi\omega^{1-m}(a_1)a_1^{m+t} + (m+t)Np^r \sum_{\substack{a=1\\(a,Np)=1}}^{Np^r} a_2\theta\psi\omega^{1-m}(a_1)a_1^{m+t-1} \pmod{p^{2r}}.$$

The left-hand sum and the first right-hand sum are equivalent mod p^{2r}, and the last sum is the one in which we're interested. Solving for the third sum and substituting it into the congruence of 3.3.1, we find

$$\tilde{g}_\theta^{(t)}(\psi(1+p)(1+p)^{m-1}-1)$$
$$= (\theta\psi\omega^{1-m}(1+p)(1+p)^{m+t}-1)\frac{1}{m+t}\lim_{r\to\infty}\frac{1}{Np^r}\sum_{\substack{a=1\\(a,Np)=1}}^{Np^r} \theta\psi\omega^{1-m}(a)a^{m+t}.$$

We claim that

$$\lim_{r\to\infty}\frac{1}{Np^r}\sum_{\substack{a=1\\(a,Np)=1}}^{Np^r} \theta\psi\omega^{1-m}(a)a^{m+t} = (1-\theta\psi\omega^{1-m}(p)p^{m+t-1})B_{m+t,\theta\psi\omega^{1-m}}.$$

For this, recall the definition of the Bernoulli polynomials

$$B_n(X) = \sum_{i=0}^{n}\binom{n}{i}B_iX^{n-i}$$

where B_i is the ith Bernoulli number (with $B_1 = \frac{-1}{2}$), and recall that for any Dirichlet character χ of modulus dividing a positive integer F, one has that

$$B_{n,\chi} = \frac{1}{F}\sum_{j=1}^{F}\chi(j)F^nB_i(\frac{j}{F}).$$

We have

$$\begin{aligned}
B_{m+t,\theta\psi\omega^{1-m}} &= \frac{1}{Np^r}\sum_{j=1}^{Np^r}\theta\psi\omega^{1-m}(j)(Np^r)^{m+t}B_{m+t}\left(\frac{j}{Np^r}\right)\\
&\equiv \sum_{j=1}^{Np^r}\theta\psi\omega^{1-m}(j)\left(j^{m+t}-\frac{m+t}{2}j^{m+t-1}Np^r\right) \pmod{p^{r-1}}\\
&\equiv \sum_{j=1}^{Np^r}\theta\psi\omega^{1-m}(j)j^{m+t} \pmod{p^{r-1}}.
\end{aligned}$$

Therefore,

$$B_{m+t,\theta\psi\omega^{1-m}} = \lim_{r\to\infty}\frac{1}{Np^r}\sum_{j=1}^{Np^r}\theta\psi\omega^{1-m}(j)j^{m+t},$$

and

$$(1-\theta\psi\omega^{1-m}(p)p^{m+t-1})B_{m+t,\theta\psi\omega^{1-m}} = \lim_{r\to\infty}\frac{1}{Np^r}\sum_{\substack{j=1\\(j,Np)=1}}^{Np^r}\theta\psi\omega^{1-m}(j)j^{m+t}.$$

The equality in the proposition statement then follows from observing that

$$-h^{(t)}(\psi(1+p)(1+p)^{m-1}-1) = \theta\psi\omega^{1-m}(1+p)(1+p)^{m+t}-1,$$

as $\theta(1+p)=\omega(1+p)=1$ (recall that in our notation we write $1+p\in(\mathbb{Z}/p^r\mathbb{Z})^\times \leqslant \Delta_r$). $\square$

We indicate to which p-adic L-function the power series $g_\theta^{(t)}$ of the above proposition corresponds. Recall that

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

for k a positive integer, where $L(\chi,s)$ is the Dirichlet L-function associated with a Dirichlet character χ. The above proposition then says that

$$\begin{aligned}
g_\theta^{(t)}(\psi(1+p)(1+p)^{m-1}-1) &= (1-\theta\psi\omega^{1-m}(p)p^{m+t-1})L(\theta\psi\omega^{1-m},1-(m+t))\\
&= L_p(\theta\psi\omega^{1+t},1-(m+t)),
\end{aligned}$$

so that for $s\in\mathbb{Z}_p$

$$g_\theta^{(t)}(\psi(1+p)(1+p)^s-1) = L_p(\theta\psi\omega^{1+t},-s-t). \tag{3.3.2}$$

We may also consider the images of $\xi^{(t)}$ and $\eta^{(t)}$ under the involution of $\tilde{\Lambda}$ induced by $[c] \mapsto [c]^{-1}$. For characters θ of parity equal to that of $t+1$, the θ-eigenspaces of these elements then correspond to power series $f_\theta^{(t)}(T)$ and $\tilde{f}_\theta^{(t)}(T)$ with

$$f_\theta^{(t)}(T) = \tilde{f}_\theta^{(t)}(T)/(1-(1+p)^{1+t}(1+T)^{-1}),$$

and one has that for any finite order character ψ of Γ,

$$f_\theta^{(t)}(\psi(1+p)(1+p)^s - 1) = L_p(\theta^{-1}\psi^{-1}\omega^{1+t}, s-t). \tag{3.3.3}$$

It will be useful later to note that $g_\theta^{(1)}((1+p)^{-1}(1+T)^{-1}-1) = f_{\theta\omega}^{(0)}(T)$ and that $\tilde{f}_{\omega^{-1}}^{(0)}(T)$ is a unit [Wa97, Lemma 7.12], so that $f_{\omega^{-1}}^{(0)}(T)$ has a simple pole at $T=p$ and $g_{\omega^{-2}}^{(1)}(T)$ has a simple pole at $(1+p)^{-1}(1+T)^{-1}-1=p$, or equivalently at $T=(1+p)^{-2}-1$.

Remark 3.3.13. Taking $m=1$, we see that $\xi^{(t)}$ agrees with the element ${}^{-t}\xi^*$ of [FK12, §4.1] and $f_\theta^{(t)}$ corresponds to their ${}^{-t}\xi$. Additionally, $g_\theta^{(1)}(T)$ agrees with $G(T,\theta\omega^2)$ of [Oh03, 1.4.5] and [La15b, §3.2], and $f_{\omega\theta_{(0)}^{-1}}^{(0)}(X)$ agrees with $F(T,\theta\omega^2)$ of [Oh03, A.1.10] and [La15b, §1].

For any Dirichlet character χ, we let $\chi_{(0)}$ denote the associated primitive character of χ. We now set $\xi = \xi^{(1)}$.

Definition 3.3.14. *Define the equivariant Eisenstein series to be the element*

$$\mathcal{E} = \frac{1}{2}\xi + \sum_{n=1}^{\infty}\left(\sum_{\substack{0<d\mid n \\ p\nmid d}} d[d]\right) q^n$$

in $Q(\tilde{\Lambda})[[q]]$ which specializes for each character θ of Δ to the $\tilde{\Lambda}_\theta$-adic Eisenstein series

$$\mathcal{E}_\theta := \theta(\mathcal{E}) = \frac{1}{2}\xi_\theta + \sum_{n=1}^{\infty}\left(\sum_{\substack{0<d\mid n \\ p\nmid d}} d\theta(d)[d]_\Gamma\right) q^n$$

where $\xi_\theta := \theta(\xi) \in Q(\tilde{\Lambda}_\theta)$ (and is in $\tilde{\Lambda}_\theta$ if $\theta \neq 1$), and $[d]_\Gamma$ is defined by the factorization $[x] = [x]_\Delta [x]_\Gamma$ for any $x \in \mathbb{Z}_{p,N}^\times$.

These Eisenstein series $\mathcal{E}_\theta$ may be seen to specialize to classical Eisenstein series, and by our convention they are eigenforms for the adjoint Hecke operators.

Lemma 3.3.15 ([Oh03, 1.4.8],[La15b, Proposition 5])**.** *For θ an even character, denoting by $\gamma = 1 + p$ the topological generator of $1 + p\mathbb{Z}_p$, we have*

(i) $\langle a\rangle^{-1}\mathcal{E}_\theta = \theta(a)\langle\gamma^{i(a)}\rangle^{-1}\mathcal{E}_\theta$ *for* $a \in \mathbb{Z}_{p,N}^\times$,

(ii) $T_l^*\mathcal{E}_\theta = (1 + \theta(l)l\langle\gamma^{i(l)}\rangle^{-1})\mathcal{E}_\theta$ *for* $l \nmid Np$,

(iii) $U_l^*\mathcal{E}_\theta = \mathcal{E}_\theta$ *for* $l \mid Np$.

Definition 3.3.16. *We define the Eisenstein ideal $I \subset \mathfrak{H}^*_{\Lambda_\mathcal{O}}$ to be the ideal generated by the elements $T_l^* - (1 + l\langle l\rangle^{-1})$ for $l \nmid Np$ and $U_l^* - 1$ for $l \mid Np$. We also denote by I its image in the cuspidal Hecke algebra $\mathfrak{h}^*_{\Lambda_\mathcal{O}}$ and refer to it as the Eisenstein ideal as well.*

We let $\mathfrak{H}^*_{\Lambda_\mathcal{O},E}$ and $\mathfrak{h}^*_{\Lambda_\mathcal{O},E}$ denote the products of the localizations at the (finitely many) maximal ideals containing the Eisenstein ideal and refer to them as the Eisenstein components of $\mathfrak{H}^*_{\Lambda_\mathcal{O}}$ and $\mathfrak{h}^*_{\Lambda_\mathcal{O}}$, respectively. For any $\mathfrak{H}^*_{\Lambda_\mathcal{O}}$-module M, we let M_E denote the corresponding localized module over $\mathfrak{H}^*_{\Lambda_\mathcal{O},E}$.

For a character θ of Δ, we denote by I_θ the ideal generated by $T_l^* - (1 + l\theta(l)\langle\gamma^{i(l)}\rangle^{-1})$ and $U_l^* - 1$ in $\mathfrak{H}^*_{\Lambda_{\mathcal{O}[\theta]}}$ or its image in $\mathfrak{h}^*_{\Lambda_{\mathcal{O}[\theta]}}$. We define $\mathfrak{m}_\theta = (\pi, \langle\gamma\rangle^{-1} - 1) + I_\theta$ the maximal (or unit) ideal of $\mathfrak{h}^*_{\Lambda_\mathcal{O}}$ containing I_θ, where $\pi \in \mathcal{O}$ is a uniformizer.

Note in particular that for $\theta \neq 1$, I_θ is the annihilator in $\mathfrak{H}^*_{\Lambda_{\mathcal{O}[\theta]}}$ of $\mathcal{E}_\theta$ (and not $\mathcal{E}_{\theta^{-1}}$) as $\langle a\rangle^{-1} - \theta(a) \in I_\theta$ for $a \in (\mathbb{Z}/pN\mathbb{Z})^\times \subset \mathbb{Z}_{p,N}^\times$. For $\theta = 1$, the analogous claim in $Q(\mathfrak{H}^*_{\Lambda_{\mathcal{O}[\theta]}})$ is true.

CHAPTER 4

Cohomology of modular curves

In this chapter, we define the p-adic Eichler-Shimura cohomology groups of Ohta and use results of Lafferty to extend the construction of Υ to cases where θ is non-exceptional but possibly imprimitive and for general tame level N such that $Np > 3$. In the second part of the chapter, we show that Υ is surjective by extending the arguments of Ohta in [Oh20] to these new cases.

4.1 Eichler-Shimura cohomology groups

For the remainder of the chapter, we fix an odd prime p and a positive integer N such that $p \nmid N$ and $Np > 3$. We introduce our principal object of study, the ordinary p-adic Eichler-Shimura cohomology group of [Oh95]. Let

$$ES_r = H^1_{\text{ét}}(X_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))$$

denote the first étale cohomology group of the curve $X_1(Np^r)_{\overline{\mathbb{Q}}}$ for $r \geq 1$, and let

$$ES = \varprojlim_r ES_r$$

be the p-adic Eichler-Shimura cohomology group of level N of Ohta, where the inverse limit is along the trace maps π_{1*}, where $\pi_1 : X_1(Np^{r+1}) \to X_1(Np^r)$ are the degeneracy maps of section 3.1.3. Similarly, let

$$GES_r = H^1_{\text{ét}}(Y_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1)),$$

and let

$$GES = \varprojlim_r GES_r$$

be the so-called generalized p-adic Eichler-Shimura cohomology groups of level N, and let $GES_{r,c}$ and GES_c denote the compactly supported variants.

Definition 4.1.1. *Set*

$$\mathcal{T}_r := e_r^* ES_r, \quad \mathcal{T} := \varprojlim_r \mathcal{T}_r = e^* ES,$$
$$\tilde{\mathcal{T}}_r := e_r^* GES_r, \quad \tilde{\mathcal{T}} := \varprojlim \tilde{\mathcal{T}}_r = e^* GES,$$
$$\tilde{\mathcal{T}}_{r,c} := e_r^* GES_{r,c}, \quad \tilde{\mathcal{T}}_c := \varprojlim \tilde{\mathcal{T}}_{r,c} = e^* GES_c.$$

We refer to the right-hand groups as the ordinary, resp. ordinary generalized, resp. ordinary compactly supported generalized, p-adic Eichler-Shimura cohomology groups of level N. The groups are modules over $\mathfrak{H}^*$, and so are modules over $\tilde{\Lambda}$ via action of group elements by inverse diamond operators.

For a $\mathbb{Z}_p$-algebra $\mathcal{O}$, we denote by $\mathcal{T}_{\Lambda_{\mathcal{O}}}$ the scalar extension $\mathcal{T}\widehat{\otimes}_{\mathbb{Z}_p}\mathcal{O}$, and we define the modules $\tilde{\mathcal{T}}_{\Lambda_{\mathcal{O}}}$, $\tilde{\mathcal{T}}_{c,\Lambda_{\mathcal{O}}}$, $\mathcal{T}_{r,\mathcal{O}}$, $\tilde{\mathcal{T}}_{r,\mathcal{O}}$, and $\tilde{\mathcal{T}}_{r,c,\mathcal{O}}$ similarly.

We have the following result due to Ohta [Oh00, 1.3.6, 1.3.8, 2.1.11] in the case $p > 3$, though see [FK12, §1.7] for statements closer to the formulation given here, and see the discussion below for the case $p = 3$.

Theorem 4.1.2 ([Oh95, Oh00], [FK12, §1.7])**.** *There are short exact sequences of $\mathfrak{H}^*[G_{\mathbb{Q}_p}]$-modules, finitely generated and free over $\mathbb{Z}_p$,*

$$0 \longrightarrow \mathcal{T}_{r,\mathrm{sub}} \longrightarrow \mathcal{T}_r \longrightarrow \mathcal{T}_{r,\mathrm{quo}} \longrightarrow 0$$

and

$$0 \longrightarrow \tilde{\mathcal{T}}_{r,\mathrm{sub}} \longrightarrow \tilde{\mathcal{T}}_r \longrightarrow \tilde{\mathcal{T}}_{r,\mathrm{quo}} \longrightarrow 0,$$

characterized by the following properties:

(i) The actions of $G_{\mathbb{Q}_p}$ on $\mathcal{T}_{r,\mathrm{quo}}$ and $\tilde{\mathcal{T}}_{r,\mathrm{quo}}$ are unramified.

(ii) For an element $\sigma \in I_p$ in the inertia group of $G_{\mathbb{Q}_p}$, the actions of σ on $\mathcal{T}_{r,\mathrm{sub}}$ and $\tilde{\mathcal{T}}_{r,\mathrm{sub}}$ are given by multiplication by $\kappa_p(\sigma)\langle\kappa_{Np}(\sigma)\rangle^{-1}$.

Moreover, the canonical maps $\mathcal{T}_{(r,)\mathrm{sub}} \to \tilde{\mathcal{T}}_{(r,)\mathrm{sub}}$ are isomorphisms, and the inverse limit of the exact sequences yield short exact sequences of $\mathfrak{H}^*[G_{\mathbb{Q}_p}]$-modules, finitely generated and free over Λ,

$$0 \longrightarrow \mathcal{T}_{\mathrm{sub}} \longrightarrow \mathcal{T} \longrightarrow \mathcal{T}_{\mathrm{quo}} \longrightarrow 0 \tag{4.1.1}$$

and

$$0 \longrightarrow \tilde{\mathcal{T}}_{\mathrm{sub}} \longrightarrow \tilde{\mathcal{T}} \longrightarrow \tilde{\mathcal{T}}_{\mathrm{quo}} \longrightarrow 0,$$

which satisfy the properties analogous to the two listed above. Additionally, there are isomorphisms of $\mathfrak{H}^*$-modules $\mathcal{T}_{\mathrm{quo}} \cong S_\Lambda$, $\tilde{\mathcal{T}}_{\mathrm{quo}} \cong M_\Lambda$, and $\mathcal{T}_{\mathrm{sub}} \cong \mathfrak{h}^*$.

This result is a p-adic étale version of the classical Eichler-Shimura result of Proposition 3.2.17 in the sense that we have a comparison between spaces of modular forms and cohomology of modular curves. In the classical setting, one has a Hodge filtration on the Betti cohomology of modular curves with $\mathbb{C}$-coefficients which splits and whose associated graded pieces canonically give spaces of modular or cuspidal forms. In the p-adic setting, the local action at p produces a similar filtration which gives rise to the short exact sequences above, which may be assembled into a Λ-adic family. When working with $\mathbb{C}_p$-coefficients (or coefficients in a complete subfield of $\mathbb{C}_p$ containing all roots of unity), the quotient modules of the sequences may be canonically identified with spaces of p-adic or Λ-adic forms. In [FK12, §1.7], it is explained that these canonical identifications over $\mathbb{C}_p$ noncanonically, but functorially in a sense, descend to isomorphisms over $\mathbb{Z}_p$. As we have no need for our isomorphisms to be canonical, we give the statement above only with $\mathbb{Z}_p$-coefficients.

Remark 4.1.3. Ohta's result was an improvement over results of Mazur-Wiles and Tilouine in which they obtained non-canonical isomorphisms of the form $\mathcal{T}_{\mathrm{quo}} \cong S_\Lambda$ under some additional assumptions: in [MW86] the tame level N is assumed to be trivial and the trivial eigenspace of $(\mathbb{Z}/p\mathbb{Z})^\times$ is excluded, and in [Ti87] the trivial and ω^{-1}-eigenspaces of $(\mathbb{Z}/p\mathbb{Z})^\times$ are excluded. There are two reasons for the exclusion of these eigenspaces: the abelian variety quotients considered in their papers have bad reduction at the trivial eigenspace, and in order to obtain a Hecke-equivariant splitting of the short exact sequence associated with $\mathcal{T}$ in Theorem 4.1.2, one asks that the Galois actions on the submodule and the quotient module are distinct. These eigenspaces were also excluded in [Oh95] for the same reasons and only added back in [Oh00], though in the latter Ohta does not pursue the splitting of the sequence for the problematic eigenspaces.

We now take the time to point out how to handle the case $p = 3$ in Theorem 4.1.2, which was excluded in [Oh95, Oh00, MW86, Ti87, FK12], etc., due to a chain of dependencies originating in the works [Hi86a] and [Hi86b], where the assumption $p \geq 5$ was made "for a technical reason", namely, the fact that the congruence subgroups $\Gamma_1(M)$ have nontrivial torsion elements when $M < 4$. This torsion prevents one from immediately comparing group cohomology of the congruence subgroup, the setting in which Hida originally developed his theory, with sheaf cohomology on the corresponding modular curve. Taking $Np > 3$ should resolve all problems, but to be careful, we now trek through [Oh00] and summarize the arguments therein.[1]

4.1.1 The case $p = 3$ for $\tilde{\Lambda}$-adic Eichler-Shimura

Throughout, Ohta works with the model $X_1^\mu(M)$ instead of $X_1(M)$, but we will suppress any notation indicating that we are working with the μ-model for simplicity. Section 1 of [Oh00] is largely algebro-geometric and arrives at the finite level short exact sequences of Theorem 4.1.2 (up to a twist of coefficients and choice of model) by taking the Poincaré dual

[1] It is worth mentioning that Hida theory has been developed even in the presence of torsion in the congruence subgroup in the book [Hi93], which predates the papers of Ohta to which we refer in this dissertation, but the precise statements that Ohta needed were not present in the book.

of a short exact sequence of p-adic Tate modules of certain p-divisible groups defined over $\mathbb{Z}_p[\zeta_{p^r}]$. The Galois action on the sequence can be computed on the geometric objects via well-known techniques as in [MW84, MW86] and can then be translated into an action on cohomology, as Poincaré duality is Galois-equivariant. We detail this process below.

We start off in [Oh00, §1.1] with the construction of the quotient abelian varieties $\mathcal{A}_r$ of the Jacobian $J_r := J_1(Np^r)_{/\mathbb{Q}}$ and $\mathcal{Q}_r$ of the generalized Jacobian $GJ_r := GJ_1(Np^r)_{/\mathbb{Q}}$ for $r \geq 1$. Here, it is sufficient to assume that $Np > 3$ so that we have representable moduli problems $[\Gamma_1(Np)]$ on $(\mathrm{Ell}/\mathbb{Q})$ in the notation of Section 3.1. This assumption is also used in the identification in [Oh00, Proposition 1.1.5] of the cotangent spaces of $\mathcal{A}_r$ and $\mathcal{Q}_r$ with certain spaces of classical modular forms of level Np^r.

We remark that Mazur and Wiles in [MW84, Chapter 3] construct similar abelian varieties and compare their cotangent spaces to spaces of modular forms without assuming $Np > 3$; this is explained for example in [DI95, §12]. See also [Ca18, §2.2] for constructions of and comparisons between the abelian variety quotients considered by Mazur-Wiles and by Ohta in [Oh99], though note that the constructions of the latter differ from those in [Oh00] slightly.

We next identify the U_p-ordinary parts of the p-divisible groups of J_r and $\mathcal{A}_r$ and of GJ_r and $\mathcal{Q}_r$ using [Hi85, Lemma 3.2], which has no restriction on p. For $n \geq 0$, we form the "fixed part" (or rather, finite part)

$$(\mathcal{A}^0_{r,\mathbb{Z}_p[\zeta_{p^r}]}[p^n])^f$$

of the quasi-finite separated group scheme given by the p^n-torsion of the connected component of the Néron model $\mathcal{A}_{r,\mathbb{Z}_p[\zeta_{p^r}]}$ of $\mathcal{A}_{r,\mathbb{Q}_p(\zeta_{p^r})}$, and we take the ordinary part of the associated p-divisible group over $\mathbb{Z}_p[\zeta_{p^r}]$

$$g_r := e \cdot \mathcal{A}^0_{r,\mathbb{Z}_p[\zeta_{p^r}]}(p)^f,$$

which may be shown to be an ordinary p-divisible group just as in [Oh00, Proposition 1.2.4], which appeals to the works of Mazur-Wiles and Hida cited above. Here, an ordinary p-divisible group is one whose connected component g_r^0 has étale Cartier dual, i.e., is multiplicative.[2]

We then have a short exact sequence of $\mathfrak{h}[G_{\mathbb{Q}_p}]$-modules

$$0 \to T_p(g_r^0) \to e \cdot T_p(J_r) \to E_r \to 0 \tag{4.1.2}$$

where g_r^0 is the connected component of g_r, T_p denotes the p-adic Tate module, and E_r is defined by exactness of the sequence. With respect to a twisted Weil pairing, the proof of [Oh00, Proposition 1.2.8] shows that $T_p(g_r^0)$ is isotropic and pairs perfectly against E_r, and the action of an element $\sigma \in I_p$ of inertia is given by multiplication by $\kappa_p(\sigma)$ on $T_p(g_r^0)$ and by $\langle \kappa_{Np}(\sigma) \rangle^{-1}$ on E_r.

We next consider the Atkin-Lehner twisted abelian variety quotients $\mathcal{A}_r^*$ of J_r and $\mathcal{Q}_r^*$ of GJ_r over $\mathbb{Q}$ as in section 1.3 of [Oh00], and we set $\mathcal{N}_r^* = \ker(\mathcal{Q}_r^* \to \mathcal{A}_r^*)$. It is these quotients that we ultimately care about – that Ohta considers $\mathcal{A}_r$ and $\mathcal{Q}_r$ separately seems to be a matter of preference, as the analysis of both types of quotients may essentially be done in parallel, as it was done in [Ca18, §2.2].

We associate with these abelian varieties their connected components of Néron models to obtain a short exact sequence of commutative group schemes

$$0 \to \mathcal{N}^{*0}_{r,\mathbb{Z}_p[\zeta_p^r]} \to \mathcal{Q}^{*0}_{r,\mathbb{Z}_p[\zeta_p^r]} \to \mathcal{A}^{*0}_{r,\mathbb{Z}_p[\zeta_p^r]} \to 0,$$

which gives rise to a short exact sequence of ordinary p-divisible groups

$$0 \to \mathcal{H}_r \to \widetilde{\mathcal{G}}_r \to \mathcal{G}_r \to 0$$

where $\mathcal{H}_r = e^* \cdot \mathcal{N}^{*0}_{r,\mathbb{Z}_p[\zeta_p^r]}(p)^f$, $\widetilde{\mathcal{G}}_r = e^* \cdot \mathcal{Q}^{*0}_{r,\mathbb{Z}_p[\zeta_p^r]}(p)^f$, and $\mathcal{G}_r = e^* \cdot \mathcal{A}^{*0}_{r,\mathbb{Z}_p[\zeta_p^r]}(p)^f$. Ordinariness of these p-divisible groups follows from ordinariness of g_r and from the isomorphism $g_r \cong \mathcal{G}_r$ over $\mathbb{Z}_p[\mu_{Np^r}]$.

As before, we form the exact sequence

$$0 \to T_p(\mathcal{G}_r^0) \to e^* \cdot T_p(J_r) \to E_r^* \to 0$$

[2]This is different from being of μ-type, a notion which is used below and in [Oh20], which asks for constant Cartier dual.

where E_r^* is defined by exactness of the sequence. Taking the $\mathbb{Z}_p$-linear dual of this sequence, we obtain via Poincaré duality the short exact sequence of free $\mathbb{Z}_p$-modules

$$0 \to e^* H^1_{\text{ét}}(X_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p)^{I_p} \to e^* H^1_{\text{ét}}(X_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p) \to \mathfrak{B}_r^* \to 0 \tag{4.1.3}$$

where $\sigma \in I_p$ acts on $\mathfrak{B}_r$ by multiplication by $\kappa_p^{-1}(\sigma)\langle\kappa_{Np}(\sigma)\rangle$.

We similarly have a sequence with the generalized Jacobian in place of the Jacobian

$$0 \to T_p(\widetilde{\mathcal{G}}_r^0) \to e^* \cdot T_p(GJ_r) \to E_r^* \to 0,$$

where the cokernel is able to be identified with E_r^* because $\mathcal{H}_r$ is also the kernel of the quotient $\widetilde{\mathcal{G}}_r^0 \twoheadrightarrow \mathcal{G}_r^0$. Taking $\mathbb{Z}_p$-duals and using Poincaré duality gives the exact sequence of free $\mathbb{Z}_p$-modules

$$0 \to e^* H^1_{\text{ét}}(Y_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p)^{I_p} \to e^* H^1_{\text{ét}}(Y_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p) \to \widetilde{\mathfrak{B}}_r^* \to 0 \tag{4.1.4}$$

where $\sigma \in I_p$ acts on $\widetilde{\mathfrak{B}}_r$ by multiplication by $\kappa_p^{-1}(\sigma)\langle\kappa_{Np}(\sigma)\rangle$.

Denoting $\mathfrak{A}_r^* := e^* H^1_{\text{ét}}(X_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p)^{I_p} \cong e^* H^1_{\text{ét}}(Y_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p)^{I_p}$ and taking inverse limits, we obtain the final short exact sequences of section 1

$$0 \to \mathfrak{A}_\infty^* \to e^* ES_p(N)_{\mathbb{Z}_p} \to \mathfrak{B}_\infty^* \to 0, \tag{4.1.5}$$

$$0 \to \mathfrak{A}_\infty^* \to e^* GES_p(N)_{\mathbb{Z}_p} \to \widetilde{\mathfrak{B}}_\infty^* \to 0, \tag{4.1.6}$$

where $e^*GES_p(N)_{\mathbb{Z}_p} := \varprojlim_r e^* H^1_{\text{ét}}(Y_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p)$, $e^*ES_p(N)_{\mathbb{Z}_p} := \varprojlim_r e^* H^1_{\text{ét}}(X_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p)$ are the Eichler-Shimura cohomology groups in Ohta's notation.

In section 2 of [Oh00], the cokernels $\widetilde{\mathfrak{B}}_r$ and $\mathfrak{B}_r$ are identified with spaces of modular forms, and Hida-theoretic perfect control of the terms of the above sequences is proved. The latter proceeds via group cohomological methods and makes use of the assumption that $Np > 3$.

Control of $e^*GES_p(N)_{\mathbb{Z}_p}$ is proved as in [Oh99, Theorem 1.3.5] as follows. For integers

$s_1 \geq s_2 \geq r \geq 1$, we have the diagram in group cohomology

$$\begin{tikzcd} e^*H^1(\Gamma_1(Np^{s_1}), \mathbb{Z}_p) \arrow[r, "\omega_r"] \arrow[d, "cor"] & e^*H^1(\Gamma_1(Np^{s_1}), \mathbb{Z}_p) \arrow[r, "cor"] \arrow[d, "cor"] & e^*H^1(\Gamma_1(Np^r), \mathbb{Z}_p) \arrow[r] \arrow[d, equal] & 0 \\ e^*H^1(\Gamma_1(Np^{s_2}), \mathbb{Z}_p) \arrow[r, "\omega_r"] & e^*H^1(\Gamma_1(Np^{s_2}), \mathbb{Z}_p) \arrow[r, "cor"] & e^*H^1(\Gamma_1(Np^r), \mathbb{Z}_p) \arrow[r] & 0 \end{tikzcd}$$

where $\omega_r = (1+T)^{p^{r-1}} - 1 \in \Lambda_{\mathbb{Z}_p}$ and “cor” denotes corestriction. Exactness of the horizontal sequences would give under inverse limits

$$e^*GES_p(N)_{\mathbb{Z}_p}/\omega_r \cong e^*H^1_{\text{ét}}(Y_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p)$$

as $e^*H^1_{\text{ét}}(Y_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p) \cong e^*H^1(\Gamma_1(Np^r), \mathbb{Z}_p)$ under our assumption $Np > 3$. Exactness follows from the computation of a double coset decomposition as in [Oh99, Lemmas 1.2.10, 1.2.12] and may also be found in the recently published book of Hida [Hi22, Lemma 4.2.14]. Considering parabolic cohomology instead in the above also proves control of $e^*ES_p(N)_{\mathbb{Z}_p}$.

By the above control results, we have a commutative diagram with exact rows

$$\begin{tikzcd} & \mathcal{A}^*_\infty/\omega_r \arrow[r] \arrow[d] & e^*GES_p(N)_{\mathbb{Z}_p}/\omega_r \arrow[r] \arrow[d, "\cong"] & \widetilde{\mathfrak{B}}^*_\infty/\omega_r \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \mathfrak{A}^*_r \arrow[r] & e^*H^1_{\text{ét}}(Y_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p) \arrow[r] & \widetilde{\mathfrak{B}}^*_r \arrow[r] & 0. \end{tikzcd}$$

This gives us morphisms $\mathfrak{B}^*_\infty \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathbb{C}_p} \to \varprojlim_r (\mathfrak{B}^*_r \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathbb{C}_p})$ and $\widetilde{\mathfrak{B}}^*_\infty \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathbb{C}_p} \to \varprojlim_r (\widetilde{\mathfrak{B}}^*_r \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathbb{C}_p})$ which may be proved to be injective just as in [Oh00, Lemma 2.1.6].

We have injections $\mathfrak{B}^*_r \otimes_{\mathbb{Z}_p} \mathbb{C}_p \hookrightarrow S_2(Np^r; \mathbb{C}_p)(-1)$ and $\widetilde{\mathfrak{B}}^*_r \otimes_{\mathbb{Z}_p} \mathbb{C}_p \hookrightarrow M_2(Np^r; \mathbb{C}_p)(-1)$ which compile to give injections into spaces of Λ-adic forms

$$\mathfrak{B}^*_\infty \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathbb{C}_p} \to \mathfrak{S}^*_{k,\Lambda_{\mathcal{O}_{\mathbb{C}_p}}}(-1)$$
$$\widetilde{\mathfrak{B}}^*_\infty \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathbb{C}_p} \to \mathfrak{m}^*_{k,\Lambda_{\mathcal{O}_{\mathbb{C}_p}}}(-1).$$

The main result [Oh00, Theorem 2.1.11] says that these injections are isomorphisms. By Nakayama's lemma, it is equivalent to prove surjectivity after modding out by $\omega_1 = T$. By control of the space of Λ-adic forms 3.3.8 and the identifications $\mathfrak{B}^*_r \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathbb{C}_p} \cong e^*\mathrm{Cot}(\mathcal{A}^{*0}_{r,\mathcal{O}_{\mathbb{C}_p}})(-1)$

and $\widetilde{\mathfrak{B}}_r^* \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathbb{C}_p} \cong e^*\mathrm{Cot}(\mathcal{Q}^{*0}_{r,\mathcal{O}_{\mathbb{C}_p}})(-1)$, this is equivalent to proving that the inclusions

$$e^*\mathrm{Cot}(J^0_{r,\mathcal{O}_{\mathbb{C}_p}}) \hookrightarrow e^* S_2(Np; \mathcal{O}_{\mathbb{C}_p})$$
$$e^*\mathrm{Cot}(GJ^0_{r,\mathcal{O}_{\mathbb{C}_p}}) \hookrightarrow e^* m_2(Np; \mathcal{O}_{\mathbb{C}_p})$$

are surjections. This can be proved over $\mathbb{Z}_p[\mu_{Np}]$

The key now is that regular differentials on the modular curve $X_1(Np)_{\mathbb{Z}_p[\mu_{Np}]}$ for $Np > 3$ correspond to weight 2 modular forms that have integral Fourier expansion at both the zero and infinity cusps [Gr90, Prop. 8.4]. One must then show that the ordinary forms which are integral at either the ∞ or the 0 cusp are in fact integral at both.

The argument breaks into two cases, depending on whether the diamond operator action of $(\mathbb{Z}/p\mathbb{Z})^\times$ is trivial or not. In the case of nontrivial eigenspaces, the cuspidal case is handled in [Oh95, §3.4] following Mazur and Wiles' study of Hecke operators on the special fiber in [MW84], and in the non-cuspidal case in [Oh99, §§4.4-4.5], where Ohta computes residues of ordinary modular forms to verify integrality at all cusps. The proof may easily be verified to work in the case $p = 3$. In fact, Ohta shows integrality for all eigenspaces in [Oh99, 4.4.22], so the only case left is the case of cusp forms with trivial action [Oh00, 2.2.4], which relies on a description by Gross [Gr90, Prop. 8.18] of the U_p operator on the trivial eigenspace of the space of regular differentials of the special fiber of $X_1(Np)_{\mathbb{Z}_p[\mu_{Np}]}$. As Gross' work holds without restriction on p so long as $Np > 3$ (see [Gr90, §10]), this completes the verification of the validity of Ohta's p-adic Eichler-Shimura isomorphism theorem in the case $p = 3$.

Remark 4.1.4. There are minor mistakes in [FK12, 1.7.9, 1.7.11, 1.7.12, 1.7.13] concerning p-adic and Λ-adic Eichler-Shimura isomorphisms as in Theorem 4.1.2. In their notation, $M_2(M)_{\mathbb{Z}_p}$ and M_Λ are spaces of modular forms whose constant terms are not necessarily integral [FK12, §1.5]. The isomorphisms proved by Ohta, however, concern modular forms whose constant terms *are* integral. The mistakes in this section can largely be fixed by taking the integral spaces instead. However, the claim that $\tilde{\mathcal{T}}_{\mathrm{quo}}$ is a dualizing module for $\mathfrak{H}^*$ is not true, though it does not seem to be used in their paper. Additionally, the integral and non-integral spaces often coincide on Eisenstein local components, see [Oh03, Proposition 3.3.1], whose argument also works for $p \mid \varphi(N)$ and imprimitive θ.

4.1.2 The $\tilde{\Lambda}$-adic pairing

We return to our discussion of the sequences of Theorem 4.1.2. The module $\mathcal{T}$ plays the role of the canonical lattice in the discussion of Wiles' proof of the Iwasawa main conjecture following the statement of Theorem 2.2.8. The goal in the remainder of this chapter is to define and study a short exact sequence of $\mathfrak{h}/I[G_{\mathbb{Q}}]$-modules in order to define Υ as the restrction of a cocycle associated with the extension class of the sequence. For this, we will have to work component-wise with respect to characters of $(\mathbb{Z}/Np\mathbb{Z})^{\times}$.

Theorem 4.1.5. *Let θ be an even character of $(\mathbb{Z}/Np\mathbb{Z})^{\times}$ such that either $\theta|_{(\mathbb{Z}/p\mathbb{Z})^{\times}} \neq \omega^{-1}$ or $\theta|_{\mathbb{Z}/N\mathbb{Z})^{\times}}(p) \neq 1$, and set $\mathcal{O} = \mathbb{Z}_p[\mu_{Np\varphi(N)}]$ where φ is the Euler totient function. There is a canonical surjection of $\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}[G_{\mathbb{Q}}]$-modules*

$$(\xi_{\theta_{(0)}} s(c_\theta), -)_{\tilde{\Lambda}} : \mathcal{T}_{\Lambda_{\mathcal{O}}}/I_\theta \to (\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}/I_\theta)^{\flat}(1)$$

given by pairing $x \in \mathcal{T}_{\Lambda_{\mathcal{O}}}/I_\theta$ with $\xi_{\theta_{(0)}} s(c_\theta) \in \mathcal{T}_{\Lambda_{\mathcal{O}}}$ on the left.

We define below the twisted Poincaré duality pairing $(-,-)_{\tilde{\Lambda}}$ as well as the element $\xi_{\theta_{(0)}} s(c_\theta)$ arising from results of Lafferty. We start with the pairing.

We detail the construction of a $\tilde{\Lambda}$-valued pairing defined on $\mathcal{T} \times \mathcal{T}$. The reader only interested in the statement of the properties of the pairing may skip to Proposition 4.1.7.

Recall that there is a graded-commutative, perfect Poincaré duality pairing on the étale cohomology of a smooth variety (integral, separated scheme of finite type) X over a separably closed field k of dimension d

$$(\, , \,) : H^i_{\text{ét}}(X, \mathbb{Z}_p(d)) \times H^{2d-i}_{\text{ét},c}(X, \mathbb{Z}_p(d)) \to H^{2d}_c(X, \mathbb{Z}_p(2d)) \cong \mathbb{Z}_p(d) \tag{4.1.7}$$

for any prime $p \neq \text{char}(k)$ satisfying $(\sigma x, \sigma y) = \sigma(x, y)$ for $\sigma \in \text{Gal}(\overline{k}/k)$. Note that if X is a smooth, projective curve, then the Poincaré duality pairing agrees with the Weil pairing on the Tate module $T_p(\mathrm{Jac}(X)) \cong H^1_{\text{ét}}(X, \mathbb{Z}_p(1))$.

For any finite, flat morphism $f : X \to Y$ of smooth varieties of equal dimension and any sheaf $\mathcal{G}$ of abelian groups on the étale site $Y_{\text{ét}}$ of Y, we have morphisms

$$f_* : H^i_{\text{ét}(,c)}(X, f^{-1}\mathcal{G}) \to H^i_{\text{ét}(,c)}(Y, \mathcal{G})$$

and

$$f^* : H^i_{\text{ét}(,c)}(Y, \mathcal{G}) \to H^i_{\text{ét}(,c)}(X, f^{-1}\mathcal{G}),$$

and Poincaré duality satisfies the adjunction relations

$$(f_* x, y) = (x, f^* y), \quad (f^* x, y) = (x, f_* y).$$

In particular, this implies that the operators T_l, U_l, and $\langle a \rangle$ are adjoint to the dual Hecke operators T_l^*, U_l^*, and $\langle a \rangle^{-1}$, respectively, on ES_r and GES_r. Denote the Poincaré duality pairings on ES_r and $GES_{r(,c)}$ by $(-,-)_{\mathrm{PD}_r}$. To obtain perfect, $\mathfrak{H}^*$- and $\mathfrak{H}$-self-adjoint pairings, we then consider the twisted pairings

$$(\, , \,)'_r : ES_r \times ES_r \ni (x, y) \mapsto (x, v_{Np^r}^{-1} w_{Np^r} y)_{\mathrm{PD}_r} \in \mathbb{Z}_p(1)$$

and

$$(\, , \,)'_r : GES_r \times GES_{r,c} \ni (x, y) \mapsto (x, v_{Np^r}^{-1} w_{Np^r} y)_{\mathrm{PD}_r} \in \mathbb{Z}_p(1)$$

where here we write v_M, w_M for the pullbacks on cohomology of the corresponding maps of schemes introduced in section 3.1.

These pairings are still skew-symmetric, as one has that Poincaré duality is invariant under the action of the Atkin-Lehner involution (cf. the discussion above Remark 3.1.4):

$$(x, y)_{\mathrm{PD}_r} = (v_{Np^r}^{-1} w_{Np^r} x, v_{Np^r}^{-1} w_{Np^r} y)_{\mathrm{PD}_r}.$$

However, they are no longer Galois-equivariant – we will consider the Galois action later once we have arrived at our final pairings.

We have the following general result which allows us to augment a perfect pairing with the action of a finite abelian group, though abelianness is not necessary if one keeps track of left versus right actions.

We first introduce some terminology. Let R be a commutative ring, G a finite abelian group, and M a finitely generated $R[G]$-module. Let $(-)^* : R[G] \to R[G]$ denote the R-linear involution of rings induced by the involution homomorphism $(-)^{-1} : G \to G$. We say that a map $f : M \to N$ of R-modules between two $R[G]$-modules is $R[G]$-antilinear if for all $r \in R[G], m \in M$ one has $f(rm) = r^* f(m)$.

Lemma 4.1.6. *Let R be a commutative ring, G a finite abelian group, and M and N finitely generated $R[G]$-modules. Denote the $R[G]$-module of all $R[G]$-antilinear maps from M to N by $\mathrm{Hom}^*_{R[G]}(M, N)$. Then there is an $R[G]$-linear isomorphism, defined in the proof below,*

$$\mathrm{Hom}_R(M, R) \cong \mathrm{Hom}_{R[G]}(M, R[G])$$

which upon postcomposing with $(-)^*$ gives an $R[G]$-linear isomorphism

$$\mathrm{Hom}_R(M, R) \cong \mathrm{Hom}^*_{R[G]}(M, R[G]).$$

Proof. The usual adjunction isomorphism

$$\mathrm{Hom}_R(M, R) = \mathrm{Hom}_R(M \otimes_{R[G]} R[G], R) \xrightarrow{\sim} \mathrm{Hom}_{R[G]}(M, \mathrm{Hom}_R(R[G], R))$$

gives an isomorphism $R[G]$-modules where the G-action on each Hom-module is given by precomposition with the given G-action. The map

$$\sum_{g \in G} a_g [g]^\vee \mapsto \sum_{g \in G} a_g [g^{-1}],$$

where $[g]^\vee : R[G] \to R$ is the R-linear projection to the coefficient of the $[g]$ term, gives an $R[G]$-linear bijection

$$\mathrm{Hom}_R(R[G], R) \to R[G].$$

Composing with $(-)^*$ gives the map

$$\sum_{g\in G} a_g[g]^\vee \mapsto \sum_{g\in G} a_g[g],$$

which is an $R[G]$-antilinear bijection

$$\mathrm{Hom}_R(R[G], R) \to R[G].$$

The first bijection gives an $R[G]$-linear isomorphism

$$\mathrm{Hom}_R(M, R) \cong \mathrm{Hom}_{R[G]}(M, R[G]),$$

explcitly given by

$$f \mapsto \{m \mapsto \sum_{g\in G} f(g\cdot m)[g^{-1}]\},$$

and

$$\{m \mapsto [e]^\vee(\phi(m))\} \leftarrow\!\shortmid \phi.$$

The second bijection gives an $R[G]$-linear isomorphism

$$\mathrm{Hom}_R(M, R) \cong \mathrm{Hom}^*_{R[G]}(M, R[G])$$

which may similarly be described. $\square$

Denote $(\mathbb{Z}/Np^r\mathbb{Z})^\times$ by Δ_r for brevity. By applying the above lemma to the pairings $(\ ,\ )'_r$, we obtain perfect, Hecke-self-adjoint, equivariant $\mathbb{Z}_p[\Delta_r]$-bilinear pairings for each r

$$ES_r \times ES_r \ni (x, y) \mapsto \sum_{a\in\Delta_r} (x, \langle a\rangle^{-1} v_{Np^r}^{-1} w_{Np^r} y)_{\mathrm{PD}_r}[a] \in \mathbb{Z}_p[\Delta_r](1)$$

$$GES_r \times GES_{r,c} \ni (x, y) \mapsto \sum_{a\in\Delta_r} (x, \langle a\rangle^{-1} v_{Np^r}^{-1} w_{Np^r} y)_{\mathrm{PD}_r}[a] \in \mathbb{Z}_p[\Delta_r](1).$$

However, these pairings are not compatible along trace maps π_{1*} on ES_r and $GES_{r(,c)}$ and the natural quotient maps $\mathbb{Z}_p[\Delta_r](1) \to \mathbb{Z}_p[\Delta_r](1)$.

We instead define the finite level pairings

$$
\begin{gathered}
(-,-)_{\tilde{\Lambda}_r} : ES_r \times ES_r \to \mathbb{Z}_p[\Delta_r](1), \quad (-,-)_{\tilde{\Lambda}_r} : GES_r \times GES_{r,c} \to \mathbb{Z}_p[\Delta_r](1), \\
(x,y) \mapsto \sum_{a \in \Delta_r} (x, \langle a \rangle^{-1} v_{Np^r}^{-1} w_{Np^r} U_p^{*r} y)_{\mathrm{PD}_r}[a].
\end{gathered}
\tag{4.1.8}
$$

For each r, the restriction of $(\ ,\ )_{\tilde{\Lambda}_r}$ to a subspace on which U_p^* is invertible is then a perfect $\tilde{\Lambda}_r$-bilinear pairing.

We explain why the pairings are level-compatible. One must have for each $a \in (\mathbb{Z}/Np^{r+1}\mathbb{Z})^\times$ that

$$
(x_{r+1}, \langle a \rangle^{-1} \sum_{j=0}^{p-1} \langle 1 + jNp^r \rangle v_{Np^{r+1}}^{-1} w_{Np^{r+1}} U_p^{*(r+1)} y_{r+1})_{\mathrm{PD}_{r+1}} = (x_r, \langle \overline{a} \rangle^{-1} v_{Np^r}^{-1} w_{Np^r} U_p^{*r} y_r)_{\mathrm{PD}_r},
$$

where $\overline{a}$ is the image of a in $(\mathbb{Z}/Np^r\mathbb{Z})^\times$. Writing $x_r = \pi_{1*}x_{r+1}$, $y_r = \pi_{1*}y_{r+1}$ and using the adjunction properties of $(,)_{\mathrm{PD}_r}$, the right-hand side is equivalent to

$$
(x_{r+1}, \pi_1^*(\langle \overline{a} \rangle^{-1} v_{Np^r}^{-1} w_{Np^r} U_p^{*r} \pi_{1*} y_{r+1}))_{\mathrm{PD}_{r+1}}.
$$

As $\pi_1 \circ \langle a \rangle = \langle \overline{a} \rangle \circ \pi_1$ and π_{1*} commutes with U_p^{*r}, we are reduced to showing that

$$
\sum_{j=0}^{p-1} \langle 1 + jNp^r \rangle^{-1} v_{Np^{r+1}}^{-1} w_{Np^{r+1}} U_p^{*r+1} y_{r+1} = \pi_1^* v_{Np^r}^{-1} w_{Np^r} \pi_{1*} U_p^{*r} y_{r+1}.
$$

This calculation is carried out in terms of group cohomology in the proof of [Oh95, 4.1.13], which works just as well for $p = 3$.

We may now assemble the pairings into $\tilde{\Lambda}$-adic pairings

$$
\begin{gathered}
(-,-)_{\tilde{\Lambda}} : ES \times ES \to \tilde{\Lambda}(1), \quad (-,-)_{\tilde{\Lambda}} : GES \times GES_c \to \tilde{\Lambda}(1), \\
((x_r, y_r))_{r \geq 1} \mapsto \left((x_r, y_r)_{\tilde{\Lambda}_r}\right)_{r \geq 1}.
\end{gathered}
\tag{4.1.9}
$$

We next look at the action of $G_{\mathbb{Q}}$. For $\sigma \in G_{\mathbb{Q}}$, we have the relation $v_{Np^r}^{-1} \circ \sigma = \langle \kappa_{Np}(\sigma) \rangle \sigma \circ v_{Np^r}^{-1}$ on cohomology from Lemma 3.2.18. The Galois-equivariance of w_{Np^r} and of Poincaré duality and the commutativity of the Hecke and Galois actions then gives

$$
(\sigma(x), \sigma(y))_{\tilde{\Lambda}_r} = \kappa_p(\sigma)(x, \langle \kappa_{Np}(\sigma) \rangle^{-1} y)_{\tilde{\Lambda}_r} = \kappa_p(\sigma)[\kappa_{Np}(\sigma)](x,y)_{\tilde{\Lambda}_r},
$$

where here we abuse notation slightly and view $\kappa_{Np}(\sigma)$ as an element of $(\mathbb{Z}/Np^r\mathbb{Z})^\times$. In order to obtain a Galois-equivariant pairing, we therefore indicate the target of the pairings by $\tilde{\Lambda}_r^\flat(1)$ and $\mathbb{Z}_p[\Delta_r]^\flat(1)$, where we use a superscript $\flat$ on a $\tilde{\Lambda}$-module to denote the same underlying $\tilde{\Lambda}$-module equipped with a Galois-module structure where $\sigma \in G_{\mathbb{Q}}$ acts by multiplication by $[\kappa_{Np}(\sigma)] \in \tilde{\Lambda}$.

We summarize these properties below, abusing notation wherever necessary.

Proposition 4.1.7 (Ohta). *There are bilinear, skew-symmetric, Galois-equivariant pairings*

$$\begin{aligned} (-,-)_{\tilde{\Lambda}_r} &: \mathcal{T}_r \times \mathcal{T}_r \to \mathbb{Z}_p[\Delta_r]^\flat(1) \\ (-,-)_{\tilde{\Lambda}_r} &: \tilde{\mathcal{T}}_r \times \tilde{\mathcal{T}}_{r,c} \to \mathbb{Z}_p[\Delta_r]^\flat(1), \\ (-,-)_{\tilde{\Lambda}} &: \mathcal{T} \times \mathcal{T} \to \tilde{\Lambda}^\flat(1), \\ (-,-)_{\tilde{\Lambda}} &: \tilde{\mathcal{T}} \times \tilde{\mathcal{T}}_c \to \tilde{\Lambda}^\flat(1), \end{aligned} \tag{4.1.10}$$

given explicitly by

$$\begin{aligned} (x,y) &\mapsto \sum_{a\in\Delta_r} (x, \langle a\rangle^{-1} v_{Np^r}^{-1} w_{Np^r} U_p^{*r} y)_{\mathrm{PD}_r}[a] \in \mathbb{Z}_p[\Delta_r]^\flat(1), \\ ((x_r,y_r))_{r\geq 1} &\mapsto \left(\sum_{a\in\Delta_r} (x, \langle a\rangle^{-1} v_{Np^r}^{-1} w_{Np^r} U_p^{*r} y)_{\mathrm{PD}_r}[a] \right)_{r\geq 1} \in \tilde{\Lambda}^\flat(1) \end{aligned}$$

which satisfy

(1) $(Tx,y)_{\tilde{\Lambda}_{(r)}} = (x,Ty)_{\tilde{\Lambda}_{(r)}}$ *for all* $T \in \mathfrak{H}^*$,

(2) $(\langle a\rangle x,y)_{\tilde{\Lambda}_{(r)}} = (x,\langle a\rangle y)_{\tilde{\Lambda}_{(r)}} = [a^{-1}](x,y)_{\tilde{\Lambda}_{(r)}}$ *for all* $a \in \mathbb{Z}_{p,N}^\times$ *(resp.* $a \in \Delta_r$*),*

(3) $(\sigma x,\sigma y)_{\tilde{\Lambda}_{(r)}} = \kappa_p(\sigma)(x,\langle\kappa_{Np}(\sigma)\rangle^{-1}y)_{\tilde{\Lambda}_{(r)}} = \kappa_p(\sigma)[\kappa_{Np}(\sigma)](x,y)_{\tilde{\Lambda}_{(r)}}$ *for all* $\sigma \in G_{\mathbb{Q}}$.

Remark 4.1.8. Instead of a $\tilde{\Lambda}$-adic pairing, we may also view Λ as a Λ-module direct summand of $\tilde{\Lambda}$ and compose with the projection $\tilde{\Lambda} \twoheadrightarrow \Lambda$ to obtain Λ-bilinear, Galois-equivariant pairings

$$(-,-)_\Lambda : ES \times ES \to \Lambda^\flat(1), \quad (-,-)_\Lambda : GES \times GES_c \to \Lambda^\flat(1),$$

where we use the superscript $\flat$ in a slight abuse of notation, as we have

$$(\sigma(x), \sigma(y))_\Lambda = \kappa_p(\sigma)(x, \langle \kappa_{Np}(\sigma)\rangle y)_\Lambda,$$

but the action of Δ_1 through the diamond operators cannot be pulled out (compare with [Oh95, 4.2.8]).

Proof. Though the pairing $(-,-)_\Lambda$ on $\mathcal{T} \times \mathcal{T}$ is introduced in [Oh95, §4], it is not explicitly claimed to be perfect. However, the same argument as in the proof of [Oh95, Theorem 4.3.1] or [Oh00, Theorem 2.3.5] gives perfectness, as we explain.

The induced map

$$\mathcal{T} \to \mathrm{Hom}_\Lambda(\mathcal{T}, \Lambda^\flat(1))$$

may be checked to be an isomorphism upon reducing modulo $T \in \Lambda$, as $\mathcal{T}$ is finitely generated and free over Λ, whereupon one obtains the map

$$\mathcal{T}_1 \to \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{T}_1, \mathbb{Z}_p(1))$$

which is an isomorphism as it is induced by Poincaré duality on $\mathcal{T}_1$. The same argument also gives perfectness of the finite level $\mathbb{Z}_p[U_1/U_r]^\flat(1)$-valued pairings.

To extend these perfectness results to the $\tilde{\Lambda}^\flat(1)$- and $\mathbb{Z}_p[\Delta_r]^\flat(1)$-valued pairings, one may argue similarly to the proof of Lemma 4.1.6 above. For example if we use $\mathrm{Hom}^*_\Lambda(\mathcal{T}, \Lambda)$ in place of $\mathrm{Hom}_R(M, R)$ with $G = (\mathbb{Z}/Np\mathbb{Z})^\times$, we obtain an isomorphism of $\tilde{\Lambda}$-modules

$$\mathcal{T} \cong \mathrm{Hom}_\Lambda(\mathcal{T}, \Lambda) \cong \mathrm{Hom}_{\tilde{\Lambda}}(\mathcal{T}, \tilde{\Lambda})$$

which coincides with the natural induced map $\mathcal{T} \to \mathrm{Hom}_{\tilde{\Lambda}}(\mathcal{T}, \tilde{\Lambda})$. □

Remark 4.1.9. In the case that $p \nmid \varphi(N)$, one has that $\mathcal{T}$ and $\tilde{\mathcal{T}}$ are finitely generated projective $\tilde{\Lambda}$-modules. This follows from the fact that they are finite free as Λ-modules, that in this case $\tilde{\Lambda}$ is isomorphic to a product of power series rings over unramified extensions of $\mathbb{Z}_p$, and [SP, Tag 00MP] (where we use the aforementioned unramifiedness to satisfy condition (3)). One may also then verify perfectness of $(\ ,\ )_{\tilde{\Lambda}}$ after localizing at maximal ideals.

4.1.3 Homology of modular curves and the Drinfeld-Manin splitting

In preparation for describing the element $\xi_{\theta_{(0)}} s(c_\theta) \in \mathcal{T}_{\Lambda_{\mathcal{O}}}$, in this section we review the relation between homology and cohomology of modular curves and the Drinfeld-Manin splitting.

For each $r \geq 1$, let $C_r(N) = X_1(Np^r) - Y_1(Np^r)$ be the cuspidal divisor and consider the long exact sequence in relative homology of $\mathfrak{H}_2(Np^r; \mathbb{Z}_p)$-modules of the pair $(X_1(Np^r)^{\mathrm{an}}, C_r(N)^{\mathrm{an}})$

$$\begin{aligned} 0 \to H_1(X_1(Np^r)^{\mathrm{an}}; \mathbb{Z}_p) \to H_1(X_1(Np^r)^{\mathrm{an}}, C_r(N)^{\mathrm{an}}; \mathbb{Z}_p) \to H_0(C_r(N)^{\mathrm{an}}; \mathbb{Z}_p) \\ \to H_0(X_1(Np^r)^{\mathrm{an}}; \mathbb{Z}_p) \to H_0(X_1(Np^r)^{\mathrm{an}}, C_r(N)^{\mathrm{an}}; \mathbb{Z}_p) = 0. \end{aligned}$$

Via identification of this sequence with the localization sequence in Borel-Moore homology, Poincaré duality gives a level-compatible isomorphism of the sequence with the localization sequence in cohomology

$$\begin{aligned} 0 \to H^1(X_1(Np^r)^{\mathrm{an}}; \mathbb{Z}_p) \to H^1(Y_1(Np^r)^{\mathrm{an}}; \mathbb{Z}_p) \to H^0(C_r(N)^{\mathrm{an}}; \mathbb{Z}_p) \\ \to H^2(X_1(Np^r)^{\mathrm{an}}; \mathbb{Z}_p) \to H^2(Y_1(Np^r)^{\mathrm{an}}; \mathbb{Z}_p) = 0 \end{aligned}$$

which intertwines the usual Hecke operators on homology with adjoint Hecke operators on cohomology. The comparison isomorphism between Betti and étale cohomology [SGA4.3, XVI 4.1] then gives a Hecke-equivariant, level-compatible identification of this sequence with the Gysin sequence

$$\begin{aligned} 0 \to H^1_{\text{ét}}(X_1(Np^r)_{\overline{\mathbb{Q}}}; \mathbb{Z}_p(1)) \to H^1_{\text{ét}}(Y_1(Np^r)_{\overline{\mathbb{Q}}}; \mathbb{Z}_p(1)) \to H^0_{\text{ét}}(C_r(N)_{\overline{\mathbb{Q}}}; \mathbb{Z}_p) \\ \to H^2_{\text{ét}}(X_1(Np^r)_{\overline{\mathbb{Q}}}; \mathbb{Z}_p(1)) \to 0, \end{aligned}$$

and through which the terms of the preceding two sequences acquire a Galois action. There are unique Hecke-equivariant splittings s_r of the inclusions

$$H_1(X_1(Np^r)^{\mathrm{an}}, \mathbb{Q}_p) \hookrightarrow H_1(X_1(Np^r)^{\mathrm{an}}, C_r(N); \mathbb{Q}_p)$$

called the Manin-Drinfeld splittings [La87b, Ch.IV §2]. The terminology is due to their existence being equivalent to the result of Manin and Drinfeld giving that the cuspidal subgroup of a modular Jacobian is finite [El90].

Via these identifications, we may view the ordinary generalized Eichler-Shimura cohomology group as the space of ordinary level-compatible families of modular symbols

$$\tilde{\mathcal{T}} = e^* \varprojlim_r H^1_{\text{ét}}(Y_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1)) \cong e^* \varprojlim_r H_1(X_1(Np^r)^{\text{an}}, C_r(N)^{\text{an}}; \mathbb{Z}_p).$$

Moreover, Ohta has shown [Oh99, 3.4.12] that by taking inverse limits of ordinary parts of the above sequences, one obtains the short exact sequence of $\mathfrak{H}^*[G_{\mathbb{Q}}]$-modules

$$0 \to \mathcal{T} \to \tilde{\mathcal{T}} \to C_\Lambda \to 0$$

where $C_\Lambda = e^*(\varprojlim_r H^0_{\text{ét}}(C_r(N)_{\overline{\mathbb{Q}}}; \mathbb{Z}_p))$. The Manin-Drinfeld splittings then induce a splitting [FK12, 1.9.3]

$$s : \tilde{\mathcal{T}} \otimes_\Lambda Q(\Lambda) \to \mathcal{T} \otimes_\Lambda Q(\Lambda)$$

which we will also call the Manin-Drinfeld splitting.

4.1.4 The map $(\xi_{\theta_{(0)}} s(c_\theta), -)_{\Lambda_{\mathcal{O}}}$

We now fix a character θ of $\Delta = (\mathbb{Z}/Np\mathbb{Z})^\times$, and we let $\theta_{(0)}$ denote its associated primitive character and θ' its restriction to the prime-to-p subgroup Δ' of Δ. We write $\Lambda_\theta = \Lambda_{\mathbb{Z}_p[\theta]} \cong \mathbb{Z}_p[\theta][[T]]$, and let $g^{(1)}_{\theta_{(0)}}(T) \in \Lambda_\theta$ be the power series such that $g^{(1)}_{\theta_{(0)}}(\gamma^s - 1) = L_p(\theta_{(0)}\omega^2, -1 - s)$ associated with $\theta_{(0)}$, so that by comparing interpolation properties of $L_p(\theta\omega^2, s)$ and $L_p(\theta_{(0)}\omega^2, s)$ (recall Proposition 3.3.12 and the discussion afterwards; see also the proof of [La15b, Proposition 4]), we have

$$g^{(1)}_\theta(T) = g^{(1)}_{\theta_{(0)}}(T) \cdot \prod_{l|N} (1 - \theta_{(0)}(l) l (1+T)^{i(l)}).$$

If $\theta_{(0)} \neq \omega^{-2}$, then we let $\xi_{\theta_{(0)}} \in \Lambda_\theta$ correspond to $g^{(1)}_{\theta_{(0)}}(T)$. When $\theta_{(0)} = \omega^{-2}$, we let $\xi_{\theta_{(0)}} \in \Lambda_\theta$ correspond to $((1+p)^{-1}(1+T)^{-1} - (1+p))g^{(1)}_{\theta_{(0)}}$, and in this case we also modify the definition of the Λ_θ-adic Eisenstein series $\mathcal{E}_\theta$ by multiplying through by the factor $(1+p)^{-1}(1+T)^{-1}-(1+p)$ so that $\mathcal{E}_\theta \in \Lambda_\theta[[q]]$. To streamline the discussion, we will write $\xi_{\theta_{(0)}}$ in place of the corresponding power series below.

As in the statement of Theorem 4.1.5, we let $\mathcal{O}$ denote the extension of $\mathbb{Z}_p$ obtained by adjoining all $Np\varphi(N)$th roots of unity. We describe how to use the results of [La15b] to obtain an element of $\mathcal{T}_{\Lambda_\mathcal{O}}$, yielding a map $\mathcal{T}_{\Lambda_\mathcal{O}}/I_\theta \to \Lambda_\theta/(\xi_{\theta_{(0)}})$ via the pairing introduced in section 4.1.2, generalizing the construction in [FK12, 6.3.8]. Let $K \subset \mathbb{C}_p$ be a complete subfield containing all roots of unity, and let $\tilde{\Lambda}_\infty = \mathcal{O}_K[[\mathbb{Z}_{p,N}^\times]]$, $\Lambda_\infty = \mathcal{O}_K[[1+p\mathbb{Z}_p]]$ be the corresponding Iwasawa algebras. In [Oh99, Oh00], Ohta has constructed the following commutative diagram of $\mathfrak{H}^*[G_{\mathbb{Q}_p}]$-modules

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & \mathcal{T}_{\Lambda_\infty,\mathrm{sub}} \arrow[r, "\cong"] \arrow[d] & \tilde{\mathcal{T}}_{\Lambda_\infty,\mathrm{sub}} \arrow[d] & & \\
0 \arrow[r] & \mathcal{T}_{\Lambda_\infty} \arrow[r] \arrow[d] & \tilde{\mathcal{T}}_{\Lambda_\infty} \arrow[r] \arrow[d] & C_{\Lambda_\infty} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & S_{\Lambda_\infty} \arrow[r] \arrow[d] & M_{\Lambda_\infty} \arrow[r, "\mathrm{Res}"] \arrow[d] & C_{\Lambda_\infty} \arrow[r] & 0 \\
 & 0 & 0 & &
\end{tikzcd} \tag{4.1.11}$$

with exact rows and columns, where Res is the Λ-adic residue map, constructed as the projective limit of finite level residue maps as in [Oh03, §2.4]. Lafferty has computed [La15b, Theorem 3]

$$\mathrm{Res}(\mathcal{E}_\theta) = \xi_{\theta_{(0)}}\mathfrak{e}_\theta$$

for an explicit element $\mathfrak{e}_\theta \in C_{\Lambda_\theta} \subset C_{\Lambda_\infty}$.

Remark 4.1.10. Lafferty computed residues of more general Eisenstein series $\mathcal{E}_{\theta,\psi;t}$ in [La15b, Theorem 3], though it is stated that, in his notation, the element $\mathfrak{e}_{\theta,\psi;t}$ lives in $C_{\Lambda_\mathcal{O}}$, which may not be the case if the coefficient ring $\mathcal{O}$ does not contain the ratio of Gauss sums

$$g((\psi\chi^{-1})_{(0)})/g(\chi_{(0)}^{-1})$$

which appears in the definition of $\mathfrak{e}_{\theta_{(0)},\psi_{(0)};t}$ in equation (27) of *op. cit.*, where $\theta = \chi\omega^i$ with p not dividing the modulus of χ. If $\mathcal{O}$ contains all Npth roots of unity, then one has $\mathfrak{e}_{\theta,\psi;t} \in C_{\Lambda_{\mathcal{O}[\theta,\psi]}}$ for all valid θ, ψ. This is the reason for our definition of $\mathcal{O}$ above.

Our Eisenstein series $\mathcal{E}_\theta$ corresponds to the Eisenstein series $\mathcal{E}_{\theta,1}$ of Lafferty, and so we indeed have $\mathfrak{e}_\theta \in C_{\Lambda_\theta}$.

By Lafferty's computation and the remark, the map Res restricts to a map $M_{\Lambda_{\mathcal{O}}} \to C_{\Lambda_{\mathcal{O}}}$ which is necessarily surjective, as $C_{\Lambda_{\mathcal{O}}} \otimes_{\Lambda_{\mathcal{O}}} \Lambda_\infty \cong C_{\Lambda_\infty}$, $M_{\Lambda_{\mathcal{O}}} \otimes_{\Lambda_{\mathcal{O}}} \Lambda_\infty \cong M_{\Lambda_\infty}$, and Λ_∞ is faithfully flat over $\Lambda_{\mathcal{O}}$ [Oh95, 2.1.1]. Therefore, we may replace Λ_∞ everywhere with $\Lambda_{\mathcal{O}}$ in diagram 4.1.11 without sacrificing exactness. The diagram over $\Lambda_{\mathcal{O}}$ can then be obtained as the inverse limit of diagrams at finite level

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & \mathcal{T}_{r,\mathcal{O},\mathrm{sub}} \arrow[r, "\cong"] \arrow[d] & \tilde{\mathcal{T}}_{r,\mathcal{O},\mathrm{sub}} \arrow[d] & & \\
0 \arrow[r] & \mathcal{T}_{r,\mathcal{O}} \arrow[r] \arrow[d] & \tilde{\mathcal{T}}_{r,\mathcal{O}} \arrow[r] \arrow[d] & C_{r,\mathcal{O}} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & e^*S_2^*(Np^r;\mathcal{O}) \arrow[r] \arrow[d] & e^*M_2^*(Np^r;\mathcal{O}) \arrow[r, "\mathrm{Res}_r"] \arrow[d] & C_{r,\mathcal{O}} \arrow[r] & 0 \\
 & 0 & 0 & &
\end{tikzcd} \tag{4.1.12}$$

where $C_{r,\mathcal{O}} = e^*H^0_{\text{ét}}(C_r(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathcal{O}$. Note that all objects in diagram 4.1.11, resp. diagram 4.1.12, are finitely generated and free over Λ_∞, resp $\mathcal{O}[U_1/U_r]$.

As $\mathcal{E}_\theta$ is a Hecke eigenform by Lemma 3.3.15 and Res is a map of $\mathfrak{H}^*$-modules, we have that $\Lambda_{\mathcal{O}}\mathfrak{e}_\theta \subset C_{\Lambda_{\mathcal{O}}}$ is an $\mathfrak{h}^*$-submodule.[3] Denote by $\mathfrak{e}_{\theta,r}$ the image of $\mathfrak{e}_\theta$ in $C_{r,\mathcal{O}}$. Then $\mathcal{O}[U_1/U_r]\mathfrak{e}_{\theta,r}$

[3]One can also see that $\Lambda_{\mathcal{O}}\mathfrak{e}_\theta$ is $\mathfrak{H}^*$-stable from the explicit formula for $\mathfrak{e}_\theta$ in equation (27) of [La15b]. Note

is a Hecke-submodule of $C_{r,\mathcal{O}}$. We may then pull back diagram 4.1.12 along the inclusion $\mathcal{O}[U_1/U_r]e_{\theta,r} \hookrightarrow C_{r,\mathcal{O}}$ to obtain the commutative diagram of $\mathfrak{H}^*[G_{\mathbb{Q}_p}]$-modules

$$
\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & \mathcal{T}_{r,\mathcal{O},\mathrm{sub}} \arrow[r, "\cong"] \arrow[d] & \tilde{\mathcal{T}}_{P_{\theta,r},\mathrm{sub}} \arrow[d] & & \\
0 \arrow[r] & \mathcal{T}_{r,\mathcal{O}} \arrow[r] \arrow[d] & \tilde{\mathcal{T}}_{P_{\theta,r}} \arrow[r] \arrow[d] & \mathcal{O}[U_1/U_r]\mathfrak{e}_{\theta,r} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & e^*S_2^*(Np^r;\mathcal{O}) \arrow[r] \arrow[d] & P_{\theta,r} \arrow[r, "\mathrm{Res}_r"] \arrow[d] & \mathcal{O}[U_1/U_r]\mathfrak{e}_{\theta,r} \arrow[r] & 0 \\
 & 0 & 0 & &
\end{tikzcd}
\tag{4.1.13}
$$

in which all rows and columns are exact, where $P_{\theta,r}$, $\tilde{\mathcal{T}}_{P_{\theta,r}}$, and $\tilde{\mathcal{T}}_{P_{\theta,r},\mathrm{sub}}$ are defined by pullback. We may similarly consider diagram 4.1.11 with $\Lambda_{\mathcal{O}}$ in place of Λ_∞ and pull back along the inclusion $\Lambda_{\mathcal{O}}\mathfrak{e}_\theta \hookrightarrow C_{\Lambda_{\mathcal{O}}}$, and obtain

$$
\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & \mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{sub}} \arrow[r, "\cong"] \arrow[d] & \tilde{\mathcal{T}}_{P_\theta,\mathrm{sub}} \arrow[d] & & \\
0 \arrow[r] & \mathcal{T}_{\Lambda_{\mathcal{O}}} \arrow[r] \arrow[d] & \tilde{\mathcal{T}}_{P_\theta} \arrow[r] \arrow[d] & \Lambda_{\mathcal{O}}\mathfrak{e}_\theta \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & S_{\Lambda_{\mathcal{O}}} \arrow[r] \arrow[d] & P_\theta \arrow[r, "\mathrm{Res}"] \arrow[d] & \Lambda_{\mathcal{O}}\mathfrak{e}_\theta \arrow[r] & 0 \\
 & 0 & 0 & &
\end{tikzcd}
\tag{4.1.14}
$$

which may be identified with the inverse limit of the diagrams 4.1.13 for $r \geq 1$, as inverse limits commute with pullbacks.

---

however that in the formula, the term $(1+X)^{s(\frac{\mathfrak{m}_\theta \Delta^c}{m_\xi c})}$ can be simplified to $(1+X)^{\frac{\mathfrak{m}_\theta \Delta^c}{m_\xi}}$ as the sum is meant to range over cusps represented by pairs (a,c) satisfying $c \equiv \omega(c) \pmod{p}^r$, among other conditions. See the notation set at the end of [La15b, §4.1.2]. One may also compare this to the proof of [Oh03, 2.6.9] where a similar simplification is made.

The Manin-Drinfeld splitting induces a splitting of the sequence of $\mathfrak{H}^*$-modules

$$0 \to \mathcal{T}_{\Lambda_{\mathcal{O}}} \to \tilde{\mathcal{T}}_{P_\theta} \to \Lambda_{\mathcal{O}}\mathfrak{e}_\theta \to 0 \tag{4.1.15}$$

after tensoring with $Q(\Lambda_{\mathcal{O}})$. This induces a splitting of the sequence

$$0 \to S_{\Lambda_{\mathcal{O}}} \otimes_{\Lambda_{\mathcal{O}}} Q(\Lambda_{\mathcal{O}}) \to P_\theta \otimes_{\Lambda_{\mathcal{O}}} Q(\Lambda_{\mathcal{O}}) \to Q(\Lambda_{\mathcal{O}})\mathfrak{e}_\theta \to 0$$

and we let $t : Q(\Lambda_{\mathcal{O}})\mathfrak{e}_\theta \to P_\theta \otimes_{\Lambda_{\mathcal{O}}} Q(\Lambda_{\mathcal{O}})$ denote the splitting. Lafferty's computation shows that $t(\mathfrak{e}_\theta) = U\xi_{\theta_{(0)}}\mathcal{E}_\theta$ where $U \in \Lambda_{\mathcal{O}}^\times$, and so the congruence module of this sequence is

$$\Lambda_{\mathcal{O}}\mathfrak{e}_\theta/(\mathrm{Res}(P_\theta \cap t(Q(\Lambda_{\mathcal{O}})\mathfrak{e}_\theta)) = \Lambda_{\mathcal{O}}/\xi_{\theta_{(0)}}.$$

Remark 4.1.11. We point out an oversight in [La15b] and [La15a] related to the discussion above and the last remark. In [La15b, §5], it is claimed that for a general ring $\mathcal{O} \supset \mathbb{Z}_p$ containing the values of θ and ψ, there is a form $F \in M_{\Lambda_{\mathcal{O}}}$ such that $\mathrm{Res}(F) = \mathfrak{e}_{\theta,\psi}$, where Res denotes the residue map $M_{\Lambda_\infty} \to C_{\Lambda_\infty}$. The issue here is that it is not clear that this is so without the stronger assumption that $\mathcal{O}$ additionally contains all $Np\varphi(N)$th roots of unity.[4] Under this assumption, as explained above, the exact sequence of Λ_∞-modules

$$0 \to S_{\Lambda_\infty} \to M_{\Lambda_\infty} \xrightarrow{\mathrm{Res}} C_{\Lambda_\infty} \to 0$$

descends to an exact sequence of $\Lambda_{\mathcal{O}}$-modules,

$$0 \to S_{\Lambda_{\mathcal{O}}} \to M_{\Lambda_{\mathcal{O}}} \to C_{\Lambda_{\mathcal{O}}} \to 0,$$

and the surjectivity of $M_{\Lambda_{\mathcal{O}}} \to C_{\Lambda_{\mathcal{O}}}$ provides such an F. Without this assumption on $\mathcal{O}$, we may not immediately claim that the residue map descends to a map from $M_{\Lambda_{\mathcal{O}}}$ to $C_{\Lambda_{\mathcal{O}}}$.

The argument used in [La15a, §3.3] does not seem to work, as we now explain. Lafferty defines $P = \mathrm{Res}^{-1}(\Lambda_{\mathcal{O}}\mathfrak{e}_{\theta,\psi}) \cap M_{\Lambda_{\mathcal{O}}}$ (where Res is defined on M_{Λ_∞}). The inclusion $P \hookrightarrow M_{\Lambda_{\mathcal{O}}}$

[4] The issue of this remark is distinct from the issue of the previous remark, as the argument that Lafferty attempts to employ does not seem to make use of the claim that $\mathfrak{e}_\theta$ is indeed an element of $\mathbb{C}_{\Lambda_{\mathcal{O}}}$ or that Res descends to a map $M_{\Lambda_{\mathcal{O}}} \to C_{\Lambda_{\mathcal{O}}}$. It is however the case that both issues are resolved simply by requiring that $\mathcal{O}$ contain all $Np\varphi(N)$th roots of unity.

induces the inclusion $P \otimes_{\Lambda_{\mathcal{O}}} \Lambda_\infty \hookrightarrow M_{\Lambda_\infty}$. We have $S_{\Lambda_{\mathcal{O}}} \subset P$ and $S_{\Lambda_\infty} \subset P \otimes_{\Lambda_{\mathcal{O}}} \Lambda_\infty$, so we have a morphism of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & S_{\Lambda_\infty} \arrow[r, "j"] \arrow[d, equal] & P \otimes_{\Lambda_{\mathcal{O}}} \Lambda_\infty \arrow[r] \arrow[d, hook] & \operatorname{coker}(j) \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & S_{\Lambda_\infty} \arrow[r] & \operatorname{Res}^{-1}(\Lambda_\infty \mathfrak{e}_{\theta,\psi}) \arrow[r] & \Lambda_\infty \mathfrak{e}_{\theta,\psi} \arrow[r] & 0.
\end{tikzcd}$$

Lafferty makes the claim that

$$0 \to S_{\Lambda_{\mathcal{O}}} \otimes_{\Lambda_{\mathcal{O}}} \Lambda_\infty \to P \otimes_{\Lambda_{\mathcal{O}}} \Lambda_\infty \to \Lambda_{\mathcal{O}} \mathfrak{e}_{\theta,\psi} \otimes_{\Lambda_{\mathcal{O}}} \Lambda_\infty \to 0$$

is exact, which by the above is equivalent to the inclusion $P \otimes_{\Lambda_{\mathcal{O}}} \Lambda_\infty \to \operatorname{Res}^{-1}(\Lambda_\infty \mathfrak{e}_{\theta,\psi})$ being surjective. No further explanation is given, and it is not clear to me how this might be proven abstractly, or whether it is true.

The sequence that we use above

$$0 \to S_{\Lambda_{\mathcal{O}}} \to P_\theta \to \Lambda_{\mathcal{O}} \mathfrak{e}_\theta \to 0$$

may be used in place of Lafferty's so that the results in [La15a, §§5, 6] still hold with minor modifications (essentially just extensions of scalars).

We compare the Δ- and $G_{\mathbb{Q}_p}$-actions of $\tilde{\mathcal{T}}_{P_\theta,\mathrm{sub}}$ and $\Lambda_{\mathcal{O}} \mathfrak{e}_\theta$. Recall from Theorem 4.1.2 that $\sigma \in I_p$ acts on $\tilde{\mathcal{T}}_{\Lambda_{\mathcal{O}},\mathrm{sub}}$ by multiplication by $\kappa_p(\sigma)\langle \kappa_{Np}(\sigma)\rangle^{-1}$, while $\sigma \in G_{\mathbb{Q}}$ acts on the cuspidal group

$$C_{\Lambda_{\mathcal{O}}} = e^*(\varprojlim_r H^0_{\text{ét}}(C_r(N)_{\overline{\mathbb{Q}}}; \mathcal{O}))$$

by pullback. We recall from Lemma 3.2.11 that

$$\sigma \cdot \begin{bmatrix} a \\ c \end{bmatrix} = \begin{bmatrix} \kappa_{Np}^{-1}(\sigma) a \\ c \end{bmatrix},$$

and so from formulas (27) and (28) of [La15b], we find that $G_{\mathbb{Q}}$ acts trivially on $\mathfrak{e}_\theta$ and that $\langle a \rangle^{-1} \mathfrak{e}_\theta = \theta(a) \mathfrak{e}_\theta$ for $a \in \Delta$.[5] We see then that if either $\theta|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega^{-1}$ or $\theta|_{(\mathbb{Z}/N\mathbb{Z})^\times}(p) \neq 1$,

[5]That $\langle a \rangle^{-1} \mathfrak{e}_\theta = \theta(a) \mathfrak{e}_\theta$ can be seen from the Hecke-equivariance of the residue map and from $\langle a \rangle^{-1} \mathcal{E}_\theta = \theta(a) \mathcal{E}_\theta$. In [La15b, 4.1.2], his convention is to use the non-adjoint Hecke algebra with the Albanese functoriality of the Jacobian which explains the difference in our notation.

then the image of the splitting $Q(\Lambda_{\mathcal{O}})\mathfrak{e}_\theta \to \tilde{\mathcal{T}}_{P_\theta} \otimes_{\Lambda_{\mathcal{O}}} Q(\Lambda_{\mathcal{O}})$ intersects trivially with $\tilde{\mathcal{T}}_{P_\theta,\mathrm{sub}}$. This implies that the bottom two horizontal sequences of 4.1.14 have isomorphic congruence modules. We call the condition that $\theta|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega^{-1}$ or $\theta|_{(\mathbb{Z}/N\mathbb{Z})^\times}(p) \neq 1$ the non-exceptionality hypothesis for θ, after the terminology of [Oh03, 1.4.10].

We now choose a lift $c_\theta \in \tilde{\mathcal{T}}_{P_\theta}$ of $\mathfrak{e}_\theta$ and consider the product $\xi_{\theta_{(0)}} s(c_\theta) \in \mathcal{T}_{\Lambda_{\mathcal{O}}} \otimes_{\Lambda_{\mathcal{O}}} Q(\Lambda_{\mathcal{O}})$ where $s(c_\theta) \in \mathcal{T}_{\Lambda_{\mathcal{O}}} \otimes_{\Lambda_{\mathcal{O}}} Q(\Lambda_{\mathcal{O}})$ is the image of c_θ under the Manin-Drinfeld splitting s on $\tilde{\mathcal{T}}_{\Lambda_{\mathcal{O}}}$ (inside which $\tilde{\mathcal{T}}_{P_\theta}$ sits). By the above paragraph, $s(\tilde{\mathcal{T}}_{P_\theta} \otimes_{\Lambda_{\mathcal{O}}} Q(\Lambda_{\mathcal{O}}))/\mathcal{T}_{\mathcal{O}} \cong \Lambda_{\mathcal{O}}/(\xi_{\theta_{(0)}})$ under the non-exceptionality hypthesis, and so $\xi_{\theta_{(0)}} s(c_\theta)$ lies in $\mathcal{T}\Lambda_{\mathcal{O}} \subset \mathcal{T} \otimes_{\Lambda_{\mathcal{O}}} Q(\Lambda_{\mathcal{O}})$. We record this as a proposition.

Proposition 4.1.12. *Suppose that either $\theta|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega^{-1}$ or $\theta|_{(\mathbb{Z}/N\mathbb{Z})^\times}(p) \neq 1$. Then $\xi_{\theta_{(0)}} s(c_\theta)$ lies in $\mathcal{T}_{\Lambda_{\mathcal{O}}} \subset \mathcal{T}_{\Lambda_{\mathcal{O}}} \otimes_{\Lambda_{\mathcal{O}}} Q(\Lambda_{\mathcal{O}})$.*

As this construction will be essential for us, we suppose that the non-exceptionality hypothesis holds going forward.

Hypothesis 4.1.13. *We assume that θ satisfies at least one of*

(1) $\theta|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega^{-1}$

(2) $\theta|_{(\mathbb{Z}/N\mathbb{Z})^\times}(p) \neq 1$.

We now have the analog of [FK12, 6.2.4].

Proposition 4.1.14. *The element $\xi_{\theta_{(0)}} s(c_\theta)$ is part of a $\Lambda_{\mathcal{O}}$-basis of $\mathcal{T}_{\Lambda_{\mathcal{O}}}$.*

Proof. If we can show that $s(\tilde{\mathcal{T}}_{P_\theta})$ is $\Lambda_{\mathcal{O}}$-free, then as $s(c_\theta)$ would be part of a $\Lambda_{\mathcal{O}}$-basis of $s(\tilde{\mathcal{T}}_{P_\theta})$, the congruence module computation $s(\tilde{\mathcal{T}}_{P_\theta})/\mathcal{T}_{\Lambda_{\mathcal{O}}} \cong \Lambda_{\mathcal{O}}/(\xi_{\theta_{(0)}})$ would give the claim. Now, $\Lambda_{\mathcal{O}}$ is a regular local ring with $1-\gamma \in \mathfrak{M}_{\Lambda_{\mathcal{O}}}$, so that $s(\tilde{\mathcal{T}}_{P_\theta})$ is $\Lambda_{\mathcal{O}}$-free if and only if $\gamma - 1$ is a non-zero-divisor of $s(\tilde{\mathcal{T}}_{P_\theta})$ and $s(\tilde{\mathcal{T}}_{P_\theta})/(\gamma-1)$ is $\mathcal{O}$-free [SP, Tag 00NS]. Since $s(\tilde{\mathcal{T}}_{P_\theta}) \subset \mathcal{T}_{\Lambda_{\mathcal{O}}} \otimes_{\Lambda_{\mathcal{O}}} Q(\Lambda_{\mathcal{O}})$, $s(\tilde{\mathcal{T}}_{P_\theta})$ is $\Lambda_{\mathcal{O}}$-torsion-free. We have perfect control of $\tilde{\mathcal{T}}_{P_\theta}$, in the sense that $\tilde{\mathcal{T}}_{P_\theta}/(\gamma^{p^{r-1}}-1) \cong \tilde{\mathcal{T}}_{P_{\theta,r}}$, as it is an extension of $\Lambda_{\mathcal{O}}\mathfrak{e}_\theta$ by $S_{\Lambda_{\mathcal{O}}}$, both of which satisfy perfect control. As the Manin-Drinfeld splitting is Hecke-equivariant, this implies that $s(\tilde{\mathcal{T}}_{P_\theta})/(1-\gamma) \cong s_1(\tilde{\mathcal{T}}_{P_{\theta,1}}) \subset \tilde{\mathcal{T}}_{1,\mathcal{O}} \otimes_{\mathcal{O}} Q(\mathcal{O})$, and so $s(\tilde{\mathcal{T}}_{P_\theta})/(1-\gamma)$ is $\mathcal{O}$-free. □

Corollary 4.1.15. *The map $(\xi_{\theta_{(0)}} s(c_\theta), -)_{\tilde{\Lambda}_{\mathcal{O}}} : \mathcal{T}_{\Lambda_{\mathcal{O}}} \to (\tilde{\Lambda}_{\mathcal{O},\theta}/(\xi_{\theta_{(0)}}))^\flat(1)$ given by the reduction of pairing against $\xi_{\theta_{(0)}} s(c_\theta)$ is surjective and factors through $\mathcal{T}_{\Lambda_{\mathcal{O}},\theta}/I_\theta$.*

Proof. Surjectivity follows from perfectness of the pairing $(-,-)_{\Lambda_{\mathcal{O}}}$ and from $\xi_{\theta_{(0)}} s(c_\theta)$ being part of a $\mathcal{O}$-basis of $\mathcal{T}_{\Lambda_{\mathcal{O}}}$. That the map factors through $\mathcal{T}_{\Lambda_{\mathcal{O}},\theta}/I_\theta$ follows from properties of the pairing 4.1.7, and the fact that for $a \in \Delta$, we have $\langle a\rangle^{-1}\mathfrak{e}_\theta = \theta(a)\mathfrak{e}_\theta$, and so $\langle a\rangle^{-1}c_\theta = \theta(a)c_\theta$. □

We would like to determine the kernel of this surjection as an $\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}/I_\theta[G_{\mathbb{Q}}]$-module. To this end, we start with a splitting of the p-ordinary sequence of Ohta on Eisenstein θ-eigenspaces. We will need the following result of Lafferty, which also finishes the proof of Theorem 4.1.5 along with Corollary 4.1.15.

Proposition 4.1.16 ([La15b, Proposition 13])**.** *There is a canonical isomorphism of $\Lambda_{\mathcal{O}}$-modules*

$$\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}/I_\theta \xrightarrow{\cong} \Lambda_{\mathcal{O}}/(\xi_{\theta_{(0)}}).$$

Denote by Δ_p the decomposition group at p in Δ, and denote the prime-to-p part of Δ_p by Δ'_p and the p-Sylow part by $\Delta_p^{(p)}$.

Proposition 4.1.17. *If $\omega\theta$ is nontrivial on Δ'_p, then the sequence of $\mathfrak{h}^*_{\Lambda_{\mathcal{O}},\theta,E}$-modules*

$$0 \to \mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{sub},\theta,E} \to \mathcal{T}_{\Lambda_{\mathcal{O}},\theta,E} \to \mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{quo},\theta,E} \to 0 \tag{4.1.16}$$

splits. If $\omega\theta$ is nontrivial on $\Delta_p^{(p)}$, then the sequence splits after tensoring with $\mathbb{Q}_p$.

Proof. Consider an element $\sigma \in I_p \leqslant G_{\mathbb{Q}_p}$. We know from Theorem 4.1.2 that σ acts on $\mathcal{T}_{\mathrm{sub}}$ by $\kappa_p(\sigma)\langle\kappa_{Np}(\sigma)\rangle^{-1}$ and on $\mathcal{T}_{\mathrm{quo}}$ trivially. Define

$$S = S_\sigma = \{x \in \mathcal{T} \mid \sigma x = x\}.$$

We'd like to see whether this maps surjectively onto $\mathcal{T}_{\text{quo}}$. Consider then an element $x \in \mathcal{T}$, and write $\sigma x = x + z$ for some $z \in \mathcal{T}_{\text{sub}}$. We are interested in finding an element $y \in S$ so that $y + \mathcal{T}_{\text{sub}} = x + \mathcal{T}_{\text{sub}}$. For a general $y \in S$, we have

$$\sigma(y - x) = \sigma y - \sigma x = y - (x + z),$$

and to have $y - x$ be in $\mathcal{T}_{\text{sub}}$ means $\sigma(y - x) = \kappa_p(\sigma)\langle\kappa_{Np}(\sigma)\rangle^{-1}(y - x)$. Note that $\mathcal{T}$ is $\mathfrak{h}^*$-torsion-free by Lemma 3.3.9 and Theorem 4.1.2 so that $\mathcal{T} \hookrightarrow \mathcal{T} \otimes_{\mathfrak{h}^*} Q(\mathfrak{h}^*) = \mathcal{T} \otimes_\Lambda Q(\Lambda)$. Thus, for any $x \in \mathcal{T}$, the element

$$y = x + (1 - \kappa_p(\sigma)\langle\kappa_{Np}(\sigma)\rangle^{-1})^{-1} z \in \mathcal{T} \otimes_\Lambda Q(\Lambda)$$

is in $\mathcal{T}$ if and only if there is a lift of $x + \mathcal{T}_{\text{sub}}$ in S. If $1 - \kappa_p(\sigma)\langle\kappa_{Np}(\sigma)\rangle^{-1}$ were invertible in $\mathfrak{h}^*$, then we would have a splitting. This leads us to considering direct factors of $\mathfrak{h}^*$ where this element, for an appropriate choice of $\sigma \in I_p$, is invertible. Let $\theta' = \theta|_{\Delta'}$ be the restriction of θ to the prime-to-p part of Δ. When $\theta'|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq \omega^{-1}$, if we choose a $\sigma \in I_p$ so that $\kappa_{Np}(\sigma) \in (\mathbb{Z}/p\mathbb{Z})^\times \subset \mathbb{Z}_{p,N}^\times$ is nontrivial, we see that $1 - \kappa_p(\sigma)\langle\kappa_{Np}(\sigma)\rangle^{-1}$ in $\mathfrak{h}^*_{\Lambda_{\mathcal{O}},\theta'}$ is of the form $1 - \zeta$ for ζ a nontrivial $(p-1)$th root of unity and is therefore invertible in the direct factor of $\mathfrak{h}^*$. In this case, the exact sequence

$$0 \to \mathcal{T}_{\text{sub},\theta'} \to \mathcal{T}_{\theta'} \to \mathcal{T}_{\text{quo},\theta'} \to 0$$

splits, and this implies that the corresponding sequence for θ in place of θ' is itself exact and splits.

For direct subfactors of $\mathfrak{h}^*_{\theta'}$ when $\theta'|_{(\mathbb{Z}/p\mathbb{Z})^\times} = \omega^{-1}$, we can consider instead the action of a Frobenius $\Phi_p \in G_{\mathbb{Q}_p}$ at p. By [FK12, §1.8], we know Φ_p acts on $\mathcal{T}_{\text{quo}}$ as U_p^*, and therefore it acts on $\mathcal{T}_{\text{sub}}$ by $U_p^{*-1}\kappa_p(\Phi_p)\langle\kappa_{Np}(\Phi_p)\rangle^{-1}$. This time, we define

$$S_{\Phi_p} = \{x \in \mathcal{T} \mid \sigma x = U_p^* x\},$$

and by the same computation, we seek to identify sufficient conditions characterizing direct factors of $\mathfrak{h}^*$ so that $U_p^* - U_p^{*-1}\kappa_p(\Phi_p)\langle\kappa_{Np}(\Phi_p)\rangle^{-1}$ is invertible in that direct factor. We ultimately will only care about Eisenstein local direct factors, those local subfactors of $\mathfrak{h}^*_{\theta',E}$. We have in fact that, after extending scalars to contain $\mathcal{O}$, the Hecke algebra $\mathfrak{h}^*_{\Lambda_{\mathcal{O}},\theta',E}$ is a local ring. This follows from the facts that any maximal ideal of $\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}$ must contain a uniformizer of the coefficient ring as $\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}$ is flat over $\Lambda_{\mathcal{O}}$, that the quotient $\mathfrak{h}^*_{\theta'} \to \mathfrak{h}^*_{\theta}$ is an isomorphism modulo a uniformizer, and that $\mathfrak{h}^*_{\Lambda_{\mathcal{O}},\theta}/I_\theta \cong \Lambda_{\mathcal{O}}/(\xi_{\theta_{(0)}})$ is local. The element $U_p^{*-1}\kappa_p(\Phi_p)\langle\kappa_{Np}(\Phi_p)\rangle^{-1} \in \mathfrak{h}^*_{\Lambda_{\mathcal{O}},\theta',E}$ is invertible if and only if its image in the residue field of $\mathfrak{h}^*_{\Lambda_{\mathcal{O}},\theta',E}$ is nonzero. We have that $U_p^* = 1$ in the residue field, and so we are concerned with $1 - \kappa_p(\Phi_p)\langle\kappa_{Np}(\Phi_p)\rangle^{-1}$ being nonzero in the residue field. We choose Φ_p so that it restricts to the trivial automorphism of $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$, and so $\kappa_p(\Phi_p) = 1$ and $\kappa_{Np}(\Phi_p) = p \in (\mathbb{Z}/N\mathbb{Z})^\times \subset \mathbb{Z}_{p,N}^\times$. The non-exceptionality hypothesis 4.1.13 on θ in this case says that $\theta|_{(\mathbb{Z}/N\mathbb{Z})^\times}(p) \neq 1$. This, however, is not enough to guarantee invertibility in the case that $p \mid \varphi(N)$, as we see that $1 - \theta_{(\mathbb{Z}/N\mathbb{Z})^\times}(p)$ is a unit if and only if $\theta_{(\mathbb{Z}/N\mathbb{Z})^\times}(p)$ is not a pth power root of unity. This of course is unavoidable at times, for example if $N = p^{p^r} - 1$ for $r \geq 1$, then the order of $p \in (\mathbb{Z}/N\mathbb{Z})^\times$ is a power of p. As in the first case, the splitting of the sequence along Eisenstein θ'-components implies exactness and splitness of the sequence on θ-components.

If $\omega\theta$ is nontrivial on $\Delta_p^{(p)}$, then the same argument gives a splitting of the sequence with p inverted (except one considers instead the residue field of $\mathfrak{h}^*_{\Lambda_{\mathcal{O}},\theta',E}[1/p]$). $\square$

In what follows, we will only explicitly address sequence 4.1.16 with p not inverted, leaving implicit all analogous claims for the p-inverted sequence.

We have now established that when $\omega\theta$ is nontrivial on Δ_p', the sequence

$$0 \to \mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{sub},\theta,E} \to \mathcal{T}_{\Lambda_{\mathcal{O}},\theta,E} \to \mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{quo},\theta,E} \to 0$$

is exact and splits as a sequence of $\mathfrak{h}^*_{\Lambda_{\mathcal{O}},\theta,E}$-modules. Note that $\mathcal{T}_{\Lambda_{\mathcal{O}},\theta,E}/I_\theta = \mathcal{T}_{\Lambda_{\mathcal{O}}}/I_\theta$ as $\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}/I_\theta$ is local, and similarly for the sub and quotient modules. Consider the map of $\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}/I_\theta[G_{\mathbb{Q}_p}]$-modules

$$f : \mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{sub}}/I_\theta \to \mathcal{T}_{\Lambda_{\mathcal{O}}}/I_\theta \xrightarrow{(\xi_{\theta_{(0)}} s(c_\theta),-)_{\tilde{\Lambda}_{\mathcal{O}}}} (\Lambda_{\mathcal{O}}/(\xi_{\theta_{(0)}}))^\flat(1) \cong (\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}/I_\theta)^\flat(1).$$

The induced map $\mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{quo}}/I_\theta \to \mathrm{coker}(f)$ is surjective, but $\sigma \in G_{\mathbb{Q}_p}$ acts nontrivially as multiplication by $\kappa_p(\sigma)\langle\kappa_{Np}(\sigma)\rangle^{-1}$ on $\mathrm{coker}(f)$ and trivially on $\mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{quo}}/I_\theta$, so by the assumptions on θ, the cokernel must be trivial. Using Theorem 4.1.2, we see that the map f is then a surjection of free rank 1 $\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}/I_\theta$-modules, and so is an isomorphism. This implies that the kernel P of $(\xi_{\theta_{(0)}} s(c_\theta), -)_{\Lambda_{\mathcal{O}}}$ on $\mathcal{T}_{\Lambda_{\mathcal{O}}}/I_\theta$ may be identified with $\mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{quo}}/I_\theta$ as $\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}/I_\theta[G_{\mathbb{Q}_p}]$-modules. Denoting $Q := (\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}/I_\theta)^\flat(1)$, it follows that

$$0 \to P \to \mathcal{T}/I_\theta \to Q \to 0$$

is split as a sequence of $\mathfrak{h}^*[G_{\mathbb{Q}_p}]$-modules.

We would like to determine the full action of $G_{\mathbb{Q}}$ on P, and we do so by comparing the determinant of the action on $\mathcal{T}$ with the action on Q. The argument is exactly as in [FK12, 6.3.15], but we give the explanation here as the discussion leads to contructions that will be relevant for the next section. To declutter the notation, we suppress the subscript $\Lambda_{\mathcal{O}}$ attached to the various objects of interest.

Using the splitting $\mathcal{T}_{\theta,E} \cong \mathcal{T}_{\mathrm{quo},\theta,E} \oplus \mathcal{T}_{\mathrm{sub},\theta,E}$, we consider the generalized matrix algebra components of $G_{\mathbb{Q}} \to \mathrm{GL}_{\mathfrak{h}^*_{\theta,E}}(\mathcal{T}_{\theta,E})$

$$G_{\mathbb{Q}} \ni \sigma \mapsto \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$$

where

$$a(\sigma) \in \mathrm{End}_{\mathfrak{h}^*_{\theta,E}}(\mathcal{T}_{\mathrm{quo},\theta,E}), \quad b(\sigma) \in \mathrm{Hom}_{\mathfrak{h}^*_{\mathcal{O},\theta,E}}(\mathcal{T}_{\mathrm{sub},\theta,E}, \mathcal{T}_{\mathrm{quo},\theta,E})$$
$$c(\sigma) \in \mathrm{Hom}_{\mathfrak{h}^*_{\theta,E}}(\mathcal{T}_{\mathrm{quo},\theta,E}, \mathcal{T}_{\mathrm{sub},\theta,E}), \quad d(\sigma) \in \mathrm{End}_{\mathfrak{h}^*_{\theta,E}}(\mathcal{T}_{\mathrm{sub},\theta,E}).$$

In order to make sense of the notion of the determinant on $\mathcal{T}$, we choose elements $e_- = 1 \in \mathfrak{h}^*_{\theta,E} \cong \mathcal{T}_{\mathrm{sub},\theta,E}$ and $e_+ \in \mathcal{T}_{\mathrm{quo},\theta,E}$ such that e_+ generates $\mathcal{T}_{\mathrm{quo},\theta,E} \otimes_{\mathfrak{h}^*} Q(\mathfrak{h}^*)$ as a $Q(\mathfrak{h}^*_{\theta,E})$-module, which is possible as $\mathcal{T}_{\mathrm{quo}} \cong \mathrm{Hom}_{\Lambda_{\mathcal{O}}}(\mathfrak{h}^*, \Lambda_{\mathcal{O}})$ by Theorem 4.1.2 and Proposition 3.3.7.[6] Using

[6]The subscripts of e_-, e_+ correspond to the eigenvalue of the action of complex conjugation on the reductions modulo I_θ of $\mathcal{T}_{\mathrm{sub}}$ and $\mathcal{T}_{\mathrm{quo}}$, respectively.

Hecke-torsion-freeness of $\mathcal{T}$ from Lemma 3.3.9, we may identify $a(\sigma), b(\sigma), c(\sigma)$, and $d(\sigma)$ with elements of $Q(\mathfrak{h}^*_{\theta,E})$. We have that $d(\sigma)$ lies in $\mathfrak{h}^*_{\theta,E}$, as does $a(\sigma)$, since $\mathcal{T}_{\mathrm{quo}} \cong S_\Lambda \cong \mathrm{Hom}_\Lambda(\mathfrak{h}^*, \Lambda)$ so that

$$\begin{aligned}\mathrm{End}_\Lambda(\mathcal{T}_{\mathrm{quo}}) &\cong \mathrm{Hom}_\Lambda(\mathrm{Hom}_\Lambda(\mathfrak{h}^*, \Lambda), \mathrm{Hom}_\Lambda(\mathfrak{h}^*, \Lambda)) \\ &\cong \mathrm{Hom}_\Lambda(\mathrm{Hom}_\Lambda(\mathfrak{h}^*, \Lambda) \otimes_{\mathfrak{h}^*} \mathfrak{h}^*, \Lambda) \\ &\cong \mathrm{Hom}_\Lambda(\mathrm{Hom}_\Lambda(\mathfrak{h}^*, \Lambda), \Lambda)\end{aligned}$$

and this last term is canonically isomorphic to $\mathfrak{h}^*$ due to the Λ-freeness of $\mathfrak{h}^*$. Inside $Q(\mathfrak{h}^*_{\theta,E})$, for $\sigma \in G_{\mathbb{Q}}$, we may define the determinant

$$\det(\sigma) = a(\sigma)d(\sigma) - b(\sigma)c(\sigma) \in \mathfrak{h}^*_{\theta,E}.$$

We have then that $b(\sigma)c(\sigma) \in \mathfrak{h}^*_{\theta,E}$, and as $c(\sigma) \equiv 0 \bmod I_{\theta,E}$ from the fact that $\mathcal{T}_{\mathrm{quo}}/I_\theta$ is Galois-stable in $\mathcal{T}/I_\theta$, we have $a(\sigma)d(\sigma) \equiv \kappa_p(\sigma)\langle\kappa_{Np}(\sigma)\rangle^{-1} \bmod I_{\theta,E}$ in $\mathfrak{h}^*_{\theta,E}$. Finally, we know that $d(\sigma) \equiv \kappa_p(\sigma)\langle\kappa_{Np}(\sigma)\rangle^{-1} \bmod I_{\theta,E}$, so that $a(\sigma) \equiv 1 \bmod I_{\theta,E}$. This gives us that the action of $G_{\mathbb{Q}}$ on P is trivial. This allows us to further identify P as the conjugation-fixed part $(\mathcal{T}/I_\theta)^+$ and $Q = (\mathcal{T}/I_\theta)^-$ since the action of complex conjugation on $Q = (\mathfrak{h}^*/I_\theta)^\flat(1)$ is $-\langle -1\rangle = -1$. We record the results of this discussion below.

Proposition 4.1.18. *If $\omega\theta$ is nontrivial on Δ'_p, then the natural map*

$$\mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{sub}}/I_\theta \to (\Lambda_{\mathcal{O}}/(\xi_{\theta_{(0)}}))^\flat(1)$$

is an isomorphism of $\mathfrak{h}^*[G_{\mathbb{Q}_p}]$-modules. Moreover, the kernel of

$$(\xi_{\theta_{(0)}} s(c_\theta), -)_{\tilde{\Lambda}_{\mathcal{O}}} : \mathcal{T}_{\Lambda_{\mathcal{O}}}/I_\theta \to (\Lambda_{\mathcal{O}}/(\xi_{\theta_{(0)}}))^\flat(1)$$

is isomorphic to $\mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{quo}}/I_\theta$ as $\mathfrak{h}^*[G_{\mathbb{Q}_p}]$-modules and is a $G_{\mathbb{Q}}$-module with trivial action.

If $\omega\theta$ is nontrivial on $\Delta_p^{(p)}$, then the natural map $\mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{sub}}/I_\theta[1/p] \to (\Lambda_{\mathcal{O}}/(\xi_{\theta_{(0)}}))^\flat(1)[1/p]$ is an isomorphism of $\mathfrak{h}^*[G_{\mathbb{Q}_p}]$-modules. Moreover, the kernel of

$$(\xi_{\theta_{(0)}} s(c_\theta), -)_{\tilde{\Lambda}_{\mathcal{O}}} : \mathcal{T}_{\Lambda_{\mathcal{O}}}/I_\theta[1/p] \to (\Lambda_{\mathcal{O}}/(\xi_{\theta_{(0)}}))^\flat(1)[1/p]$$

is isomorphic to $\mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{quo}}/I_\theta[1/p]$ as $\mathfrak{h}^*[G_{\mathbb{Q}_p}]$-modules and is a $G_{\mathbb{Q}}$-module with trivial action.

In either case, the sequence in consideration is therefore split as a sequence of $\mathfrak{h}^*[G_{\mathbb{Q}_p}]$-modules.

Our construction of Υ then must break into two cases depending on whether $\omega\theta^{-1}$ is nontrivial on Δ'_p or on $\Delta_p^{(p)}$. Note that taken together these conditions are simply Hypothesis 4.1.13.

4.2 Υ

In this section, we define Υ.

Definition 4.2.1. *Let $Q := (\Lambda_{\mathcal{O}}/(\xi_{\theta_{(0)}}))^\flat(1) \cong (\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}/I_\theta)^\flat(1)$ and define*

$$P := \ker\left((\xi_{\theta_{(0)}} s(c_\theta), -)_{\Lambda_{\mathcal{O}}} : \mathcal{T}_{\Lambda_{\mathcal{O}}}/I_\theta \to Q\right).$$

Consider the exact sequence of $\mathfrak{h}^*_{\Lambda_{\mathcal{O}}}/I_\theta[G_{\mathbb{Q}}]$-modules

$$0 \to P \to \mathcal{T}_{\Lambda_{\mathcal{O}}}/I_\theta \to Q \to 0. \tag{4.2.1}$$

We start off in this section with the assumption that $\omega\theta$ is nontrivial on Δ'_p, and we will later address the case when is it nontrivial on $\Delta_p^{(p)}$ while possibly being trivial on Δ'_p. We then have identifications $P \cong \mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{quo}}/I_\theta$ and $Q \cong \mathcal{T}_{\Lambda_{\mathcal{O}},\mathrm{sub}}/I_\theta$ as $\mathfrak{h}^*/I_\theta[G_{\mathbb{Q}_p}]$-modules obtained in Proposition 4.1.18 which give a splitting as $\mathfrak{h}^*[G_{\mathbb{Q}_p}]$-modules. We again opt to suppress the subscript $\Lambda_{\mathcal{O}}$ from our notation for purposes of readability. Sequence 4.2.1 gives rise to a cocycle

$$\bar{b} : G_{\mathbb{Q}} \to \mathrm{Hom}_{\mathfrak{h}^*}(Q, P)\,;\, \sigma \mapsto \{Q \ni x \mapsto (\sigma - 1)\tilde{x} \in P\}$$

where $\tilde{x} \in \mathcal{T}/I_\theta$ is any lift of x. This cocycle is the reduction modulo I_θ of the map $b : G_{\mathbb{Q}} \to \mathrm{Hom}_{\mathfrak{h}^*}(\mathcal{T}_{\mathrm{sub},\theta,E}, \mathcal{T}_{\mathrm{quo},\theta,E})$ of the previous section. Moreover, it forms the top-right component of the "generalized matrix representation"

$$\rho : G_{\mathbb{Q}} \to \begin{pmatrix} \mathrm{End}_{\mathfrak{h}^*}(P) & \mathrm{Hom}_{\mathfrak{h}^*}(Q,P) \\ \mathrm{Hom}_{\mathfrak{h}^*}(P,Q) & \mathrm{End}_{\mathfrak{h}^*}(Q) \end{pmatrix}$$

with

$$\sigma \mapsto \begin{pmatrix} \bar{a}(\sigma) & \bar{b}(\sigma) \\ 0 & \bar{d}(\sigma) \end{pmatrix}$$

where $\bar{a}$ and $\bar{d}$ are the reductions of the maps a and d that were defined analogously to b from the previous section. Explicitly, we have $\bar{a}(\sigma) = 1$ and $\bar{d}(\sigma) = \kappa_p(\sigma)\langle\kappa_{Np}(\sigma)\rangle^{-1}$.

For the remainder of the dissertation, we set $F = \mathbb{Q}(\mu_{Np})^{\ker(\omega\theta)}$ and redefine $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ while viewing $\omega\theta$ as a character of both $(\mathbb{Z}/Np\mathbb{Z})^\times$ and Δ. In the case that $\theta_{(0)} = \omega^{-2}$, we have that $F = \mathbb{Q}(\mu_p)$, and the element $\xi_{\theta_{(0)}}$, with corresponding power series satisfying $\tilde{g}^{(1)}_{\theta_{(0)}}(\gamma^s - 1) = L_p(\theta_{(0)}\omega^2, s)$, is a unit by [Wa97, Lemma 7.12]. In this case, Stickelberger's theorem tell us that the ω-eigenspace under the action of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ of the p-part of the class group of $\mathbb{Q}(\mu_p)$ is trivial, and so the same eigenspace of the unramified Iwasawa module $X_{\mathbb{Q}(\mu_p),\infty}$ is trivial by Nakayama's lemma and Lemma 2.2.7, while Proposition 4.1.16 tells us that $\mathfrak{h}^*/I_\theta$ is trivial, and so Υ in this case would be a map between two trivial modules. Therefore, we assume going forward that $\theta_{(0)} \neq \omega^{-2}$.

Let F_∞ be the cyclotomic $\mathbb{Z}_p$-extension of F, and define $\tilde{\Gamma} = \mathrm{Gal}(F_\infty/\mathbb{Q})$ with the usual decomposition $\tilde{\Gamma} \cong \mathrm{Gal}(F/\mathbb{Q}) \times \Gamma$. We may make sense of $\det(\rho)$ by noting that $\mathrm{End}_{\mathfrak{h}^*}(P)$ and $\mathrm{End}_{\mathfrak{h}^*}(Q)$ are both isomorphic to $\mathfrak{h}^*/I_\theta$.

Lemma 4.2.2 ([Oh00, 3.3.8]). *We have $F_\infty = \overline{\mathbb{Q}}^{\ker(\det(\rho))}$.*

Proof. We have $F \subset \overline{\mathbb{Q}}^{\ker(\det(\rho))}$, and we seek to show that the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$ is also contained in $\overline{\mathbb{Q}}^{\ker(\det(\rho))}$. Suppose otherwise, so that the image of $\ker(\det(\rho))$ under the reduction map $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ is nontrivial. Then some power γ^{p^n} of $\gamma \in \Gamma \cong \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ satisfies

$$\gamma^{p^n}\langle\gamma^{p^n}\rangle^{-1} = 1 \in \mathfrak{h}^*/I_\theta$$

and $g^{(1)}_{\theta_{(0)}}(T) \mid \gamma^{p^n}(1+T)^{p^n}-1$ in $\mathcal{O}[[T]] \cong \Lambda_{\mathcal{O}}$ by Proposition 4.1.16. The roots of $\gamma^{p^n}(1+T)^{p^n}-1$ are of the form $\zeta\gamma^{-1}-1$, where ζ is a p^nth root of unity. On the other hand, for a character $\epsilon \in \widehat{\Gamma}$ such that $\epsilon(\gamma)=\zeta$, we have that

$$g^{(1)}_{\theta_{(0)}}(\zeta\gamma^{-1}-1) = L_p(\theta_{(0)}\omega^2\epsilon, 0) \neq 0$$

by [Wa97, Theorem 4.9] and our assumption that $\theta_{(0)} \neq \omega^{-2}$. $\square$

Let $K = \overline{\mathbb{Q}}^{\ker(\rho)}$ so that $\mathrm{Gal}(K/F_\infty)$ is an abelian pro-p group. The cocycle $\bar{b}$ visibly restricts to a homomorphism of groups on G_{F_∞} and induces a map which we also denote as $\bar{b}$

$$\bar{b} : \mathrm{Gal}(K/F_\infty) \hookrightarrow \mathrm{Hom}_{\mathfrak{h}^*}(Q, P).$$

We find by direct computation that $\bar{b}$ gives a morphism of $\tilde{\Gamma}$-modules with respect to the natural left conjugation action of $G_{\mathbb{Q}}$ on G_{F_∞} and the given left $G_{\mathbb{Q}}$-action on $\mathrm{Hom}(Q,P)$. We further use the isomorphism $Q \cong (\mathfrak{h}^*/I_\theta)^\flat(1)$ induced by Proposition 4.1.16 and identify $\mathrm{Hom}_{\mathfrak{h}^*}(Q,P) \cong P^\iota(-1)$ as $\mathfrak{h}^*[G_{\mathbb{Q}}]$-modules, where the superscript ι indicates a $\tilde{\Lambda}$-module equipped with a Galois action via $G_{\mathbb{Q}} \ni \sigma \mapsto [\kappa_{Np}(\sigma)]^{-1} \in \tilde{\Lambda}$.

Lemma 4.2.3. *The restriction*

$$\bar{b} : G_{F_\infty} \to \mathrm{Hom}_{\mathfrak{h}^*}(Q,P) \cong P^\iota(-1)$$

is a morphism of $\tilde{\Gamma}$-modules. That is, for $\sigma \in \tilde{\Gamma}$, $\tau \in G_{F_\infty}$, and any lift $\tilde{\sigma} \in G_{\mathbb{Q}}$ of σ, we have

$$\bar{b}(\tilde{\sigma}\tau\tilde{\sigma}^{-1}) = \kappa_p^{-1}(\tilde{\sigma})\langle\kappa_{Np}(\tilde{\sigma})\rangle\bar{b}(\tau).$$

We have an isomorphism $\mathcal{O}[[\mathrm{Gal}(F_\infty/F)]] \cong \mathcal{O}[[X]]$ where $1+X$ corresponds to the topological generator of $\mathrm{Gal}(F_\infty/F)$ which maps to $1+p=\gamma$ under the cyclotomic character κ_p. This Galois-theoretic Iwasawa algebra is related to the Hecke-theoretic Iwasawa algebra of adjoint diamond operators $\Lambda_{\mathcal{O}} \cong \mathcal{O}[[T]]$ through their actions on $P^\iota(-1)$ and is given by the above lemma by the isomorphism $1+X \mapsto \gamma^{-1}(1+T)^{-1}$.

Remark 4.2.4. Ohta and Lafferty use the variable T as well for the Galois-theoretic algebra and so view the isomorphism of Iwasawa algebras as an involutive automorphism of $\mathcal{O}[[T]]$. On the other hand, the conventions of [FK12] and [FKS15] for their Hecke-theoretic algebra differ from ours and Ohta's and Lafferty's in that their algebra acts via the usual diamond operators on $\mathcal{T}$ and its subquotients. This leads to an agreement between the Galois-theoretic and Hecke-theoretic Iwasawa module structures on the codomain of Υ, cf. [FKS15, 2.5.6].

Recall from the introduction that the other map ϖ of Sharifi's conjecture was shown to have image contained in $H^2_{\mathrm{Iw},S_p}(F_\infty/F,\mathbb{Z}_p(2))$, the S_p-ramified Iwasawa cohomology group [FK12, Theorem 5.3.5]. We therefore ultimately want to define a map Υ on $H^2_{\mathrm{Iw},S_p}(F_\infty/F,\mathbb{Z}_p(2))$, and so we want to determine when the homomorphism $\bar{b}$ factors through the S-split Iwasawa module $Y_{F,S}$, which is to say that K/F_∞ is completely split at all places, as its twist $Y_{F,S}(1)$ sits inside this cohomology group by Lemma 2.3.3. By the above lemma, we have that necessarily $\bar{b}$ would then factor through $Y_{F,S,\omega^{-1}\theta^{-1}}$, the $\omega^{-1}\theta^{-1}$-eigenspace with respect to the action of $\mathrm{Gal}(F/\mathbb{Q})$. By Hypothesis 4.1.13 and Lemma 2.3.3, we have that the $\omega^{-1}\theta^{-1}$-eigenspaces of $Y_{F,S}$ and $H^2_{\mathrm{Iw},S_p}(F_\infty/F,\mathbb{Z}_p(1))$ agree. By the same hypothesis, we also have that $X_{F,\infty,\omega^{-1}\theta^{-1}} \cong Y_{F,S,\omega^{-1}\theta^{-1}}$, so it is sufficient to identify conditions when the homomorphism $\bar{b}$ is everywhere unramified, i.e., when K/F_∞ is everywhere unramified.

As $\mathcal{T}$ as a $G_\mathbb{Q}$-module is classically known to be unramified outside of Np [Ig59], we need only check places above Np. For places above p, this is implied by the $G_{\mathbb{Q}_p}$-splitting discussed above. To handle (necessarily tame) inertia at places dividing N, we consider for each prime $l \mid N$ the maximal subextension $K(l)$ of K/F_∞ that is unramified at all places of F_∞ above l, of which we remark there are only finitely many. Equivalently, this is the fixed subfield of K corresponding to the subgroup generated by the inertia subgroups in $\mathrm{Gal}(K/F_\infty)$ at places above l. Note that this shows that $\mathrm{Gal}(K/K(l))$ is a $\tilde{\Gamma}$-submodule of $\mathrm{Gal}(K/F_\infty)$.

Lemma 4.2.5. *We have that the image of* $\mathrm{Gal}(K/K(l))$ *inside* $P^\iota(-1)$ *is a cyclic* $\mathrm{Gal}(F_\infty/F)$-

module annihilated by

$$b_l(T) := (1+T)^{i(l)} - \theta_{(0)}^{-1}(l)l^{-2} \in \mathcal{O}[[T]]$$

of the Hecke-theoretic Iwasawa algebra. As a Galois-theoretic Iwasawa module, $\mathrm{Gal}(K/K(l))$ *is annihilated by*

$$b_l(X) := (1+X)^{i(l)} - \theta_{(0)}\omega(l)l \in \mathcal{O}[[X]].$$

Proof. Class field theory tells us that $\mathrm{Gal}(K/K(l))$ is a quotient of the inverse limit along norm maps

$$\varprojlim_r \prod_{S_{F_r} \ni \lambda | l} \mathcal{O}_{F_r,\lambda}^\times$$

where F_r are the intermediate extensions of F_∞/F with $\mathrm{Gal}(F_r/F) \cong \mathbb{Z}/p^r\mathbb{Z}$, the product runs through all primes λ of F_r dividing l, and $\mathcal{O}_{F_r,\lambda}$ is the λ-adic completion of $\mathcal{O}_{F_r}$. Moreover, class field theory tells us that the action of $\tilde{\Gamma}$ on $\mathrm{Gal}(K/K(l))$ is compatible via this quotient map with the natural action of $\tilde{\Gamma}$ on $\varprojlim_r \prod_{S_{F_r} \ni \lambda | l} \mathcal{O}_{F_r,\lambda}^\times$. As $\mathrm{Gal}(K/K(l))$ is pro-p, the quotient map necessarily factors through

$$\varprojlim_r \prod_{S_{F_r} \ni \lambda | l} \kappa(\lambda)^\times$$

where $\kappa(\lambda)$ denotes the residue field of $\mathcal{O}_{F_r,\lambda}$. Thus, $\mathrm{Gal}(K/K(l))$ is unramified at l as a $\mathrm{Gal}(F_\infty/\mathbb{Q})$-module.

A geometric Frobenius $\Phi_l \in \mathrm{Gal}(K/\mathbb{Q})$ acts on the image of $\mathrm{Gal}(K/K(l))$ in $P^\iota(-1)$ by multiplication by $l\theta_{(0)}(l)\langle \kappa_p^{-1}\omega(l)\rangle$ by Lemma 4.2.3 and acts on $\varprojlim_r \prod_{S_{F_r} \ni \lambda | l} \kappa(\lambda)^\times$, written additively, by multiplication by l^{-1}. Therefore, as a $\mathrm{Gal}(F_\infty/\mathbb{Q})$-module, the image of $\mathrm{Gal}(K/K(l))$ is annihilated by $(1+X)^{i(l)} - \theta_{(0)}^{-1}(l)l^{-2}$. Under the isomorphism $1+T \mapsto \gamma^{-1}(1+X)^{-1}$, $b_l(T)$ is sent to a unit-multiple of $b_l(X)$.

Cyclicity follows from pro-cyclicity of the terms of the inverse limit and the transitive action of $\mathrm{Gal}(F_\infty/\mathbb{Q})$ on the places of F_∞ over l. $\square$

The following corollary gives us the conditions we seek.

Corollary 4.2.6. *If $\theta_{(0)}\omega^2(l)$ is not a p-power root of unity, then* $\mathrm{Gal}(K/K(l))$ *is trivial and K/F_∞ is unramified at places above l. In general,* $\mathrm{Gal}(K/K(l))$ *is finite so that $P^\iota(-1)[1/p]$ is everywhere unramified as a G_{F_∞}-module and $\bar{b}$ is unramified as a homomorphism on G_{F_∞}.*

Proof. If $\theta_{(0)}\omega^2(l)$ is not a p-power root of unity, then $b_l(X)$ is a unit in $\mathcal{O}[[X]]$ as its constant term $1-\omega\theta_{(0)}(l)l$ is a unit.

In general, we claim that $b_l(T)$ is coprime to $g^{(1)}_{\theta_{(0)}}(T)$. Suppose that $\theta_{(0)}\omega^2(l)$ is a p-power root of unity. Then the roots of $b_l(T)$ are of the form $\gamma^{-2}\zeta-1$ for ζ a p-power root of unity, as $\gamma^{i(l)} = l\omega^{-1}(l)$. However, for a character $\epsilon \in \widehat{\Gamma}$ such that $\epsilon(\gamma)=\zeta$, we have that

$$g^{(1)}_{\theta_{(0)}}(\gamma^{-2}\zeta-1) = L_p(\theta_{(0)}\omega^2\epsilon, 1)$$

which is nonzero by [Wa97, Corollary 5.30] and our assumption that $\theta_{(0)} \neq \omega^{-2}$.

Thus, for each $l \mid N$ the inclusion $\mathrm{Gal}(K/K(l)) \hookrightarrow P^\iota(-1)$ of $\mathcal{O}[[X]]$-modules factors though a pseudo-null module so that $\mathrm{Gal}(K/K(l))$ must be finite. $\square$

We remark that in fact when $\omega\theta$ is nontrivial as a character on the prime-to-p part of the decomposition subgroup at l of $(\mathbb{Z}/Np\mathbb{Z})^\times$, then sequence 4.2.1 splits as $\mathfrak{h}^*[G_{\mathbb{Q}_l}]$-modules. The splitting of the sequence is a priori stronger than the statement that $\bar{b}$ factors through to $Y_{F,S_p,\omega^{-1}\theta^{-1}}$ and can be used to try to view Υ as a connecting morphism in a long exact sequence of Galois cohomology as in [Sh22] and [FK12, 9.4.4]. For this, one only needs to have splittings at primes $l \mid \mathrm{cond}(\theta)$. However one must also have unramifiedness of $\mathcal{T}/I_\theta$ as a $G_{\mathbb{Q}_l}$-module for all primes, which is a priori stronger than the unramifiedness of $\bar{b}$ as a homomorphism on G_{F_∞} of the corollary. Thus, there is an obstruction to defining Υ as a connecting morphism when there is an $l \nmid \mathrm{cond}(\theta)$ such that $\omega\theta_{(0)}(l)$ is a p-power root of unity or when $\omega\theta$ is trivial on prime-to-p decomposition at l but nontrivial on the p-part of inertia at l. In these cases, we do not obviously have a splitting as $G_{\mathbb{Q}_l}$-modules or unramifiedness of $\mathcal{T}/I_\theta$ at l even after inverting p.

We address the case when $\omega\theta$ is nontrivial on $\Delta_p^{(p)}$. In this case, we may consider the localized representation $\widetilde{\rho} =$ "$\rho[1/p]$" of $G_{\mathbb{Q}}$ induced by the localizations $P \to P[1/p]$ and $Q \to Q[1/p]$ along with the corresponding cocycle $\widetilde{\bar{b}} =$ "$\bar{b}[1/p]$". We may again make sense of $\det(\widetilde{\rho})$ using the identications of $P[1/p]$ and $Q[1/p]$ afforded by Proposition 4.1.18, and we find $F_\infty = \overline{\mathbb{Q}}^{\ker(\det(\widetilde{\rho}))}$ by the same argument as in the proof of Lemma 4.2.2. The splitting field $\widetilde{K} := \overline{\mathbb{Q}}^{\ker(\widetilde{\rho})}$ of $\widetilde{\rho}$ is contained in K in general, with the difference coming from possible ramification at primes above $l \mid N$ in $\widetilde{K}/F_\infty$. The arguments of Lemma 4.2.5 and Corollary 4.2.6 then show that $\widetilde{K}/F_\infty$ is everywhere unramified so that $\widetilde{\bar{b}}$ as a homomormophism on G_{F_∞} factors through $X_{F,S_p,\omega^{-1}\theta^{-1}}$.

Definition 4.2.7. *We say that we are in Case A if neither $\omega\theta_{(0)}(p)$ nor $\omega^2\theta_{(0)}(l)$ for $l \mid N$ are p-power roots of unity, and we say we are in Case B otherwise.*

In Case A, the map $\bar{b} : G_{F_\infty} \to P^\iota(-1)$ induces a morphism of (Galois-theoretic) $\tilde{\Lambda}_{\mathcal{O}}$-modules

$$\Upsilon : X_{F,S_{Np},\omega^{-1}\theta^{-1}}(1) \otimes_{\mathbb{Z}_p[\theta]} \mathcal{O} \to P^\iota.$$

In Case B, the composite $G_{F_\infty} \to P^\iota(-1) \to P^\iota(-1)[1/p]$ induces a morphism of (Galois-theoretic) $\tilde{\Lambda}_{\mathcal{O}}$-modules

$$\Upsilon : X_{F,S_{Np},\omega^{-1}\theta^{-1}}(1) \otimes_{\mathbb{Z}_p[\theta]} \mathcal{O}[1/p] \to P^\iota[1/p]$$

which we also denote Υ.

We consider the domain of Υ.

Lemma 4.2.8. *Write $\chi = \omega^{-1}\theta^{-1}$. Under the non-exceptionality hypothesis 4.1.13, we have isomorphisms*

$$X_{F,\infty,\chi} \cong Y_{F,S_p,\chi} \cong H^2_{\mathrm{Iw},S_p}(F_\infty/F, \mathbb{Z}_p(1))_\chi, \tag{4.2.2}$$

$$X_{\mathbb{Q}(\mu_{Np}),\infty,\chi} \cong Y_{\mathbb{Q}(\mu_{Np}),S_p,\chi} \cong H^2_{\mathrm{Iw},S_p}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}(\mu_{Np}), \mathbb{Z}_p(1))_\chi. \tag{4.2.3}$$

Proof. We have an exact sequence of $\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]$-modules

$$\bigoplus_{v|p} D_v \to X_{F,\infty} \to Y_{F,S_p} \to 0$$

where the sum is over primes v of F_∞ over p and where D_v denotes the corresponding decomposition subgroup of v in $X_{F,\infty}$. We may view the decomposition subgroup Δ_p of p in $\mathrm{Gal}(F/\mathbb{Q})$ as a subgroup of the decomposition group at p of the abelian $\mathrm{Gal}(F_\infty/\mathbb{Q})$, and so we see that the action of Δ_p on $X_{F,\infty}$ leaves each D_v stable. Moreover, the action of Δ_p on each D_v is trivial as H_∞/F_∞ is unramified so that, choosing any place w of H_∞ lying over v, the group $\mathrm{Gal}(H_{\infty,w}/\mathbb{Q})$ is abelian. Thus, taking χ-components (i.e., maximal *submodules* on which Δ acts via χ) followed by taking χ-eigenspaces of the sequence above gives the desired isomorphism between the unramified and S_p-split Iwasawa modules, as Hypothesis 4.1.13 is exactly the statement that $\omega\theta$ is nontrivial on Δ_p.

Next, recall the exact sequence of Lemma 2.3.3

$$0 \to Y_{F,S_p} \to H^2_{\mathrm{Iw},S_p}(F_\infty/F,\mathbb{Z}_p(1)) \to \bigoplus_{w\in S_{F_\infty,p,f}} \mathbb{Z}_p \xrightarrow{\Sigma} \mathbb{Z}_p \to 0,$$

where the direct sum is over places w of F_∞ lying over p with the action of $\mathrm{Gal}(F/\mathbb{Q}) \subset \mathrm{Gal}(F_\infty/\mathbb{Q})$ given by permutation of summands corresponding to the natural action on places. We truncate the sequence on the right to obtain a short exact sequence,

$$0 \to Y_{F,S_p} \to H^2_{\mathrm{Iw},S_p}(F_\infty/F,\mathbb{Z}_p(1)) \to \left(\bigoplus_{w\in S_{F_\infty,p,f}}^{0} \mathbb{Z}_p\right) \to 0$$

where $\bigoplus^0$ denotes the submodule of tuples that sum to 0. As Δ_p lies inside the decomposition subgroup at p of $\mathrm{Gal}(F_\infty/\mathbb{Q})$, we have that Δ_p acts trivially on the direct sum term, and so the non-exceptionality hypothesis tells us that the χ-component $(\bigoplus^0_{w\in S_{F_\infty,p,f}} \mathbb{Z}_p)^\chi = 0$ is trivial. Thus, we have an isomorphism $Y^\chi_{F,S_p} \cong H^2_{\mathrm{Iw},S_p}(F_\infty/F,\mathbb{Z}_p(1))^\chi$, which then gives an isomorphism on χ-eigenspaces.

The same arguments apply with $\mathbb{Q}(\mu_{Np})$ in place of F. $\square$

For brevity, we write $H^2_{\mathrm{Iw},S_{Np}}(\mathbb{Q}(\mu_{Np}))$ for $H^2_{\mathrm{Iw},S_{Np}}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}(\mu_{Np}),\mathbb{Z}_p(1))$ and $H^2_{\mathrm{Iw},S_{Np}}(F)$ for $H^2_{\mathrm{Iw},S_{Np}}(F_\infty/F,\mathbb{Z}_p(1))$.

Corollary 4.2.9. *Write $\chi=\omega^{-1}\theta^{-1}$. Corestriction induces an isomorphism of right exact sequences*

$$\begin{tikzcd}
Y_{\mathbb{Q}(\mu_{Np}),S,\chi} \arrow[r] \arrow[d] & H^2_{\mathrm{Iw},S_{Np}}(\mathbb{Q}(\mu_{Np}))_\chi \arrow[r] \arrow[d] & \left(\bigoplus^0_{w\in S_{\mathbb{Q}(\mu_{Np^\infty}),Np,f}} \mathbb{Z}_p\right)_\chi \arrow[r] \arrow[d] & 0 \\
Y_{F,S,\chi} \arrow[r] & H^2_{\mathrm{Iw},S_{Np}}(F)_\chi \arrow[r] & \left(\bigoplus^0_{w\in S_{F_\infty,Np,f}} \mathbb{Z}_p\right)_\chi \arrow[r] & 0.
\end{tikzcd}$$

We have then that $Y_{F,S_p,\omega^{-1}\theta^{-1}}(1)\cong H^2_{\mathrm{Iw},S_p}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}(\mu_{Np}),\mathbb{Z}_p(2))_{\theta^{-1}}$ so that Υ is a map

$$\Upsilon : H^2_{\mathrm{Iw},S_p}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}(\mu_{Np}),\mathbb{Z}_p(2))_{\theta^{-1}}\otimes_{\mathbb{Z}_p}\mathcal{O}\to P^\iota. \tag{4.2.4}$$

The appropriate generalization of Sharifi's conjecture then is that Υ is an isomorphism.

4.3 Surjectivity of Υ

Having defined the maps Υ, we now explain how Ohta's argument in [Oh20, Part II, §6] combined with Viguié's proof of a main conjecture for imaginary quadratic fields in [Vi16] implies that Υ is surjective, conditioned upon a certain Zariski density result of Hida (see the discussion before Theorem 4.3.4). We will only explicitly address Case A, as Case B may be treated similarly.

Consider the map $b\otimes Q(\mathfrak{h}^*) : G_{\mathbb{Q}}\to \mathrm{Hom}(\mathcal{T}_{\mathrm{sub},\theta,E},\mathcal{T}_{\mathrm{quo},\theta,E})\otimes_{\mathfrak{h}^*}Q(\mathfrak{h}^*)\cong Q(\mathfrak{h}^*)$ of section 4.1.4, where the isomorphism is provided by choosing basis elements $e_-=1\in\mathcal{T}_{\mathrm{sub},\theta,E}\cong\mathfrak{h}^*_{\theta,E}$ and $e_+\in\mathcal{T}_{\mathrm{quo},\theta,E}$. Let B denote the $\mathfrak{h}^*$-span of the image of b inside $Q(\mathfrak{h}^*)$. Then Be_+ is an $\mathfrak{h}^*[G_{\mathbb{Q}}]$-submodule of $\mathcal{T}_{\mathrm{quo},\theta,E}$, and its reduction modulo I_θ is the $\mathfrak{h}^*$-span of the image of the cocycle $\bar{b} : G_{\mathbb{Q}} \to P^{\iota}(-1) \cong \mathcal{T}_{\mathrm{quo}}/I_\theta$. Thus, surjectivity of Υ is equivalent by Nakayama's lemma to the equality of the containment $Be_+ \subseteq \mathcal{T}_{\mathrm{quo},\theta,E}$. Note that it follows that $\mathcal{T}_{\mathrm{quo},\theta,E}/Be_+$ is an $\mathfrak{h}^*/I_\theta[G_{\mathbb{Q}}]$-module. Let $\mathcal{M} \subset \mathcal{T}_{\theta,E}$ be the $\mathfrak{h}^*[G_{\mathbb{Q}}]$-submodule generated by (the $G_{\mathbb{Q}_p}$-submodule) $\mathcal{T}_{\mathrm{sub},\theta,E}$. Then we have $\mathcal{M} = \mathcal{T}_{\mathrm{sub},\theta,E} \oplus Be_+$, and so we equivalently wish to show that $\mathcal{M}$ coincides with $\mathcal{T}$. We do this by considering the quotient by $\langle\gamma\rangle - 1$ and Nakayama's lemma, which brings us to the study of the curve $X_1(Np)$ and its Jacobian.

The argument of [Oh20] uses particular properties of the curve $X_1^\mu(Np)$ of section 3.1, so we first translate from our model to his. One may wish to compare the discussion here to [FK12, §1.4, 1.7.16]. Recall that we have an isomorphism of $\mathfrak{h}^*$-modules

$$v : \mathcal{T} \to \varprojlim_r H^1_{\text{ét}}(X_1^\mu(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))^{\mathrm{ord}} =: \mathcal{T}^\mu(1)$$

which satisfies $\sigma \circ v = \langle \kappa_{Np}(\sigma)\rangle \circ v \circ \sigma$ for $\sigma \in G_{\mathbb{Q}}$, where $\mathcal{T}^\mu(1)$ is given its natural Galois-module structure. This induces an isomorphism of short exact sequences of $\mathfrak{h}^*$-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{T}_{\mathrm{sub}} & \longrightarrow & \mathcal{T} & \longrightarrow & \mathcal{T}_{\mathrm{quo}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle v} & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{T}^\mu_{\mathrm{sub}}(1) & \longrightarrow & \mathcal{T}^\mu(1) & \longrightarrow & \mathcal{T}^\mu_{\mathrm{quo}}(1) & \longrightarrow & 0 \end{array}$$

where $\mathcal{T}^\mu_{\mathrm{sub}}(1)$ is the image of $\mathcal{T}_{\mathrm{sub}}$ under v and $\mathcal{T}^\mu_{\mathrm{quo}}(1)$ is the cokernel.

It follows that $\mathcal{T}^\mu_{\mathrm{sub}}$ may be identified with the inertia-fixed part of $\mathcal{T}^\mu$ as a $G_{\mathbb{Q}_p}$-module. Indeed, if $y \in \mathcal{T}^\mu$ such that $\sigma(y) = y$ for all $\sigma \in I_p \leqslant G_{\mathbb{Q}_p}$, then writing $\mathcal{T}^\mu(1) \ni y = v(x)$ for a unique $x \in \mathcal{T}$, we have that $v(x) = \kappa_p(\sigma)^{-1}\sigma(v(x)) = \kappa_p(\sigma)^{-1}\langle\kappa_{Np}(\sigma)\rangle v(\sigma(x)) = v(\kappa_p(\sigma)^{-1}\langle\kappa_{Np}(\sigma)\rangle\sigma(x))$. Therefore, $\sigma(x) = \kappa_p(\sigma)\langle\kappa_{Np}^{-1}(\sigma)\rangle x$, and so $x \in \mathcal{T}_{\mathrm{sub}}$. We also point out that the determinant of the action of $\sigma \in G_{\mathbb{Q}}$ on $\mathcal{T}^\mu$ is given by $\kappa_p(\sigma)^{-1}\langle\kappa_{Np}(\sigma)\rangle$, which also describes the action of $G_{\mathbb{Q}_p}$ on $\mathcal{T}^\mu_{\mathrm{quo}}/I_\theta$.

We then consider the sequence of $G_{\mathbb{Q}_p}$-modules

$$0 \to \mathcal{T}^\mu_{\mathrm{sub},\theta,E} \to \mathcal{T}^\mu_{\theta,E} \to \mathcal{T}^\mu_{\mathrm{quo},\theta,E} \to 0,$$

which is then necessarily split, and we consider the analogous map $b^\mu : G_{\mathbb{Q}} \to Q(\mathfrak{h}^*)$ with respect to the basis $v(e_-)$ and $v(e_+)$, and denote by B^μ the $\mathfrak{h}^*$-span of its image. We see that the $\mathfrak{h}^*[G_{\mathbb{Q}}]$-module $\mathcal{M}^\mu$ generated by $\mathcal{T}^\mu_{\mathrm{sub},\theta,E}$ coincides with the image of $\mathcal{M}$ under v, which follows from the compatibility relation between v and the action of $G_{\mathbb{Q}}$. Furthermore, the coincidence of $\mathcal{M}$ with $\mathcal{T}_{\theta,E}$ occurs if and only if $\mathcal{M}^\mu$ coincides with $\mathcal{T}^\mu_{\theta,E}$ if and only if $B^\mu v(e_+)$ coincides with $\mathcal{T}^\mu_{\mathrm{quo},\theta,E} \subset Q(\mathfrak{h}^*)$. The takeaway is that we may work with either model, and with any twist of coefficients, in determining the surjectivity of Υ (or even in constructing it for that matter).

4.3.1 Modular Jacobians

We continue with the explanation of Ohta's argument. We have that $\sigma \in G_{\mathbb{Q}}$ acts on $\mathcal{T}^\mu_{\mathrm{quo},\theta,E}/B^\mu v(e_+)$, being a quotient of $\mathcal{T}^\mu_{\mathrm{quo},\theta,E}/I_\theta$, as multiplication by

$$\kappa_p(\sigma)^{-1}\langle \kappa_{Np}(\sigma)\rangle \equiv \omega^{-1}\theta^{-1}(\sigma) \pmod{\mathfrak{m}_\theta}$$

where $\mathfrak{m}_\theta$ is the maximal ideal of $\mathfrak{h}^*/I_\theta$. Recall that we have an isomorphism

$$\mathcal{T}^\mu/(\langle\gamma\rangle - 1) \cong H^1_{\text{ét}}(X_1^\mu(Np)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p)^{\mathrm{ord}}.$$

Let $\mathfrak{m}^0_\theta$ be the maximal ideal of $\mathfrak{h}^*_2(Np;\mathcal{O})$ which pulls back to $\mathfrak{m}_\theta$ under the composition $\mathfrak{h}^* \to \mathfrak{h}^*_2(Np;\mathcal{O})^{\mathrm{ord}} \hookrightarrow \mathfrak{h}^*_2(Np;\mathcal{O})$. Nontriviality of $\mathcal{T}^\mu_{\theta,E}/\mathcal{M}^\mu$ is equivalent by Nakayama's lemma to nontriviality of $\mathcal{T}^\mu_{\theta,E}/\mathcal{M}^\mu \otimes_{\mathfrak{h}^*} \mathfrak{h}^*/\mathfrak{m}_\theta$, and the latter is a quotient of $H^1_{\text{ét}}(X_1^\mu(Np)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p)/\mathfrak{m}^0_\theta$ as $\langle\gamma\rangle - 1 \in \mathfrak{m}_\theta$.

Next, recall the canonical identification of groups

$$H^1_{\text{ét}}(X_1^\mu(Np)_{\overline{\mathbb{Q}}}, \mathcal{O}) \cong \mathrm{Hom}_{\mathcal{O}}(T_p(J_1^\mu(Np))_{\mathcal{O}}, \mathcal{O}) \tag{4.3.1}$$

where $J_1^\mu(Np) := \mathrm{Jac}(X_1^\mu(Np)_{\mathbb{Q}})$ is the Jacobian variety over $\mathbb{Q}$ and where $T_p(J_1^\mu(Np)) := \varprojlim_r J_1^\mu(Np)(\overline{\mathbb{Q}})[p^r]$ is the p-adic Tate module. This isomorphism comes from a combination of Poincaré duality

$$H^1_{\text{ét}}(X_1^\mu(Np)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p) \xrightarrow{\cong} \mathrm{Hom}_{\mathbb{Z}_p}(H^1_{\text{ét}}(X_1^\mu(Np)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1)), \mathbb{Z}_p)$$

which is Galois-equivariant, but exchanges Hecke operators for their adjoints, and the identification

$$H^1_{\text{ét}}(X_1^\mu(Np)_{\overline{\mathbb{Q}}}, \mathbb{G}_m) \cong J_1^\mu(Np)(\overline{\mathbb{Q}})$$

which is Galois-equivariant, but which also exchanges Hecke operators for their adjoints, where we view the Jacobian as a Hecke-module via the covariant/Albanese action of correspondences, cf. Remark 3.2.15. Thus, the isomorphism 4.3.1 is both Hecke- and Galois-equivariant (though note that the Galois action on the dual is by precomposition with the inverse).

Now, assume that $\mathcal{T}^\mu_{\theta,E}/\mathcal{M}^\mu \otimes_{\mathfrak{h}^*} \mathfrak{h}^*/\mathfrak{m}_\theta$ is nontrivial. Then the module $H^1_{\text{ét}}(X_1^\mu(Np)_{\overline{\mathbb{Q}}}, \mathcal{O})/\mathfrak{m}^0_\theta$ admits a nontrivial $\mathfrak{h}_2^*(Np;\mathcal{O})[G_{\mathbb{Q}}]$-module quotient on which $\sigma \in G_{\mathbb{Q}}$ acts as multiplication by $\omega^{-1}\theta^{-1}(\sigma)$, and so the same holds for $\mathrm{Hom}_{\mathcal{O}}(T_p(J_1^\mu(Np))_{\mathcal{O}}, \mathcal{O})/\mathfrak{m}^0_\theta$. Let $\pi \in \mathcal{O}$ be a uniformizer, and let $k_{\mathcal{O}}$ denote the residue field of $\mathcal{O}$. As $T_p(J_1^\mu(Np))$ is finitely generated and free as a $\mathbb{Z}_p$-module, we have

$$\begin{aligned}\mathrm{Hom}_{\mathcal{O}}(T_p(J_1^\mu(Np))_{\mathcal{O}}, \mathcal{O})/(\pi) &\cong \mathrm{Hom}_{\mathcal{O}}(T_p(J_1^\mu(Np))_{\mathcal{O}}/(\pi), k_{\mathcal{O}}) \\ &\cong \mathrm{Hom}_{k_{\mathcal{O}}}(J_1^\mu(Np)[p](\overline{\mathbb{Q}}) \otimes_{\mathbb{F}_p} k_{\mathcal{O}}, k_{\mathcal{O}})\end{aligned}$$

which we may then further quotient to obtain

$$\mathrm{Hom}_{k_{\mathcal{O}}}(J_1^\mu(Np)[p](\overline{\mathbb{Q}}) \otimes_{\mathbb{F}_p} k_{\mathcal{O}}, k_{\mathcal{O}})/m^0_\theta \cong \mathrm{Hom}_{k_{\mathcal{O}}}((J_1^\mu(Np)[p](\overline{\mathbb{Q}}) \otimes_{\mathbb{F}_p} k_{\mathcal{O}})[m^0_\theta], k_{\mathcal{O}})$$

where here we write m^0_θ to also denote the maximal ideal of $\mathfrak{h}^*_{\theta,E}/(\pi)$. We conclude that $(J_1^\mu(Np)[p](\overline{\mathbb{Q}}) \otimes_{\mathbb{F}_p} k_{\mathcal{O}})[m^0_\theta]$ admits a nontrivial $\mathfrak{h}_2^*(Np;\mathcal{O})[G_{\mathbb{Q}}]$-submodule on which $\sigma \in G_{\mathbb{Q}}$ acts as multiplication by $\omega\theta(\sigma)$.

As $J_1^\mu(Np)[p]$ is a finite étale elementary abelian p-group scheme (i.e., of type "$(p, p, \dots, p)$") over $\mathbb{Q}$, we have a bijective correspondence between subgroup schemes of $J_1^\mu(Np)[p]$ and $\mathbb{F}_p[G_{\mathbb{Q}}]$-submodules of $J_1^\mu(Np)[p](\overline{\mathbb{Q}})$. For technical reasons which we will be later explained, we define $A := \ker(\theta|_{(\mathbb{Z}/p\mathbb{Z})^\times})$ and suppose that A is a nontrivial subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. Consider the submodule

$$(\sum_{a \in A} \langle a \rangle) J_1^\mu(Np)[p](\overline{\mathbb{Q}})$$

of $J_1^\mu(Np)[p](\overline{\mathbb{Q}})$. We have observed that under our assumption that $\mathcal{T}^\mu_{\theta,E}/\mathcal{M}^\mu \otimes_{\mathfrak{h}^*} \mathfrak{h}^*/\mathfrak{m}_\theta$ is nontrivial, the $\omega\theta$-isotypic component of the above submodule is nontrivial. Let H be the corresponding subgroup scheme of $J_1^\mu(Np)$, and let k_A be the compositum $\mathbb{Q}(\mu_N)\cdot\mathbb{Q}(\mu_p)^A$. Then the pullback H_{k_A} is a nontrivial μ-type subgroup scheme of $J_1(Np)_{k_A}$ on which $\langle a\rangle$ acts trivially for $a \in A$, where the notion of μ-type is in the sense of [Ma77, §1.3] and [Oh20], which is to say it is finite, flat, and has constant Cartier dual. This contradicts the following theorem, which was proved by Ohta in the case that $p \nmid \varphi(N)$ and $p \nmid [k_0 : \mathbb{Q}]$ [Oh20, Theorem 5.1.4]

Theorem 4.3.1. *Let p be an odd prime, N a positive integer such that $p \nmid N$, and θ a Dirichlet character of modulus Np such that the kernel $\ker(\theta|_{(\mathbb{Z}/p\mathbb{Z})^\times}) =: A$ is nontrivial. Let $k_0/\mathbb{Q}$ be a finite abelian extension in which p is unramified, and set $k_A := k_0\cdot\mathbb{Q}(\mu_p)^A$. Then there are no nontrivial μ-type k_A-subgroup schemes of $J_1^\mu(Np)_{k_A}$ of p-power order on which $\langle a\rangle$ acts trivially for all $a \in A$.*

The remainder of the dissertation is dedicated to the proof of this theorem. We largely follow the proof of [Oh20] and indicate how we may remove the hypothesis that $p \nmid \varphi(N)[k_0 : \mathbb{Q}]$ (we take $k_0 = \mathbb{Q}(\mu_N)$ to prove surjectivity of Υ, so the condition that $p \nmid [k_0 : \mathbb{Q}]$ is equivalent to $p \nmid \varphi(N)$ for us, but in general it is a separate condition that may also be removed). The method of proof is due to Vatsal, who proved a similar claim for the Jacobian of the curve $X_0(Np)$ in [Va05] by showing that the existence of certain nontrivial μ-type subgroups of the Jacobian contradicts Theorem 3.1.5 of Ihara. The connection between μ-type subgroups of the Jacobian $\mathrm{Jac}(X)$ of a smooth, proper curve X and unramified abelian coverings of X is standard geometric class field theory as in [Se88, Ch. VI]. We will describe an instance of the general correspondence below.

We first point out that any μ-type group scheme of type $(p, p, \ldots, p)$ over a number field is simply a product of copies of the group scheme μ_p, as the corresponding Galois module over $\mathbb{F}_p$ decomposes into a product of copies of $\mathbb{F}_p(i)$, where (i) denotes the ith Tate twist, and we must have that $i = 1$ for each copy so that its Cartier dual is constant. Thus, we may assume that we have an embedding $\mu_{p,k_A} \hookrightarrow J_1^\mu(Np)_{k_A}$.

Let $X_1^\mu(Np; A)_\mathbb{Q}$ be the quotient of $X_1^\mu(Np)_\mathbb{Q}$ by the action of A through the diamond operators, and let $J_1^\mu(Np; A)$ be the Jacobian over $\mathbb{Q}$ of this curve. We will work with $J_1^\mu(Np; A)$ and $X_1^\mu(Np; A)_\mathbb{Q}$ as the latter has semi-stable reduction at p over $\mathbb{Q}(\mu_p)^A$ [Oh20, Corollary 5.2.5], and so finite subgroup schemes of p-power order of the former may be compared with finite subgroup schemes of p-power order of the finite characteristic fibers of its Néron model by work of Raynaud when A is nontrivial [Oh20, §II.4.2]. The quotient map induces an isogeny $J_1^\mu(Np; A)_{k_A} \to J_1^\mu(Np)_{k_A}$ of degree prime to p which has μ_p in its image, and by pullback, we then have an embedding $\mu_{p,k_A} \hookrightarrow J_1^\mu(Np; A)_{k_A}$ (alternatively, one may take the image of μ_{p,k_A} under the dual isogeny).

Consider the short exact sequence of commutative group schemes over k_A

$$0 \to \mu_{p,k_A} \to J_1^\mu(Np; A)_{k_A} \to J_1^\mu(Np; A)_{k_A}/\mu_{p,k_A} \to 0 \tag{4.3.2}$$

and its dual sequence

$$0 \to \underline{\mathbb{Z}/p\mathbb{Z}}_{k_A} \to (J_1^\mu(Np; A)_{k_A}/\mu_{p,k_A})^\vee \to J_1^\mu(Np; A)_{k_A} \to 0 \tag{4.3.3}$$

where we have identified $J_1^\mu(Np; A)_{k_A}$ with its dual and have used the fact that kernels of dual isogenies are Cartier dual to one another. Let $S = \mathrm{Spec}(\mathcal{O}_{k_A}[1/Np])$, and define $\mathcal{J}_S$ and $\mathcal{J}_1^\mu(Np; A)_S$ to be the Néron models over S of $(J_1^\mu(Np; A)_{k_A}/\mu_{p,k_A})^\vee$ and $J_1^\mu(Np; A)_{k_A}$, respectively [BLR90, §1.4 Theorem 3], [Oh20, II.5.3]. Note also that $\underline{\mathbb{Z}/p\mathbb{Z}}_S$ is the Néron model of $\underline{\mathbb{Z}/p\mathbb{Z}}_{k_A}$ over S.

As $X_1^\mu(Np; A)_S$ is smooth over S, we have that $\mathcal{J}_1^\mu(Np; A)_S$ is an abelian scheme over S, i.e., it is proper with geometrically connected fibers over S (in addition to being a smooth commutative group scheme over S) [BLR90, §1.4 Proposition 2]. The map $(J_1^\mu(Np; A)_{k_A}/\mu_{p,k_A})^\vee \to J_1^\mu(Np; A)_{k_A}$ extends to an isogeny (a morphism which is fiberwise over S finite and surjective on connected components) of Néron models as p is invertible in

S by [BLR90, §7.3 Proposition 6].[7] Then as $\mathcal{J}_1^{\mu}(Np; A)_S$ is an abelian scheme over S, so must be the isogenous $\mathcal{J}_S$. By [Oh20, Lemma 4.1.5], we then have a short exact sequence of commutative group schemes over S[8]

$$0 \to \underline{\mathbb{Z}/p\mathbb{Z}}_S \to \mathcal{J}_S \to \mathcal{J}_1^{\mu}(Np; A)_S \to 0. \tag{4.3.4}$$

The pullback along the natural map $X_1^{\mu}(Np; A)_S \to \mathcal{J}_1^{\mu}(Np; A)_S$ using the S-rational point ∞ then produces a geometrically irreducible smooth, proper curve Z_S over S and a covering

$$Z_S \to X_1^{\mu}(Np; A)_S \tag{4.3.5}$$

with Galois group $\mathbb{Z}/p\mathbb{Z}$ by [Oh20, Proposition 4.1.6].

We restate Ihara's theorem from section 3.1.2 for convenience. Below, q is a prime not dividing M and $X(M)_{\mathbb{F}_{q^2}}^{\mathrm{Ihara}}$ is a particular twist of $X(M)_{\mathbb{F}_{q^2}}$ such that the supersingular points are all $\mathbb{F}_{q^2}$-rational.

Theorem 4.3.2 ([Ih75, MT 2]). *There is no nontrivial finite abelian covering $Y \to X(M)_{\mathbb{F}_{q^2}}^{\mathrm{Ihara}}$ by a geometrically irreducible, smooth, proper curve Y over $\mathbb{F}_{q^2}$ in which all supersingular points of $X(M)_{\mathbb{F}_{q^2}}^{\mathrm{Ihara}}$ are completely split.*

We remind the reader that we say that a point x of $X(M)_{\mathbb{F}_{q^2}}^{\mathrm{Ihara}}$ is completely split if the fiber of x along the covering map $Y \to X(M)_{\mathbb{F}_{q^2}}^{\mathrm{Ihara}}$ is a disjoint union of copies of the residue field of x.

Our goal then is to find an appropriate rational prime $q \equiv \pm 1 \bmod Np$ for which the fiber at a prime above q of the covering 4.3.5 produces a covering

$$Z_{\mathbb{F}_{q^2}} \to X_1^{\mu}(Np; A)_{\mathbb{F}_{q^2}} \tag{4.3.6}$$

[7]Though [BLR90, §7.3 Proposition 6] works with the local Néron model over a DVR, their proof works for Néron models over Dedekind domains (see [BLR90, §1.2 Definition 1] for the notion of Néron models over a Dedekind base).

[8]We do not need the assumption that A is nontrivial in applying [Oh20, Lemma 4.1.5], as p is invertible on S.

which is completely split at the supersingular points of $X_1^\mu(Np;A)_{\mathbb{F}_{q^2}}$. We would then pull back along the bottom composition of morphisms of the following diagram

$$\begin{tikzcd}
Z''_{\mathbb{F}_{q^2}} \arrow[rr] \arrow[d] & & Z'_{\mathbb{F}_{q^2}} \arrow[r] \arrow[d] & Z_{\mathbb{F}_{q^2}} \arrow[d] \\
X(Np)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}} = X(Np)^{(\zeta_{Np})}_{\mathbb{F}_{q^2}} \arrow[rr] & & X_1^\mu(Np)_{\mathbb{F}_{q^2}} \arrow[r] & X_1^\mu(Np;A)_{\mathbb{F}_{q^2}}
\end{tikzcd} \quad . \tag{4.3.7}$$

to obtain such a cover of $X(Np)^{(\zeta_{Np})}_{\mathbb{F}_{q^2}}$, where we use that in the case that $q \equiv \pm 1 \bmod Np$, we may identify $X(Np)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}} = X(Np)^{(\zeta_{Np})}_{\mathbb{F}_{q^2}}$ as explained in section 3.1.2. Note also that this condition on q tells us that all supersingular points of $X_1^\mu(Np)_{\mathbb{F}_{q^2}}$ and $X_1^\mu(Np;A)_{\mathbb{F}_{q^2}}$ are also $\mathbb{F}_{q^2}$-rational.

Let's see why the pullback of a geometrically irreducible, finite, abelian covering $Z_{\mathbb{F}_{q^2}}$ of $X_1^\mu(Np;A)_{\mathbb{F}_{q^2}}$ in which all supersingular points split completely gives such a covering $Z''_{\mathbb{F}_{q^2}}$ of $X(Np)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}}$ by pullback. The finiteness and abelianness are automatic, so only the other two properties need to be addressed.

Geometric irreducibility holds under pullback along the quotient map $X_1^\mu(Np)_{\mathbb{F}_{q^2}} \to X_1^\mu(Np;A)_{\mathbb{F}_{q^2}}$ as the degree of this morphism is prime to the degree p of the covering, since $A \leqslant (\mathbb{Z}/p\mathbb{Z})^\times$ has order prime to p (recall that geometric disconnectedness arises precisely from the coefficient field $\mathbb{F}_{q^2}$ being non-algebraically closed inside the field of rational functions $K(Z'_{\mathbb{F}_{q^2}})$ of $Z'_{\mathbb{F}_{q^2}}$, and geometric connectedness is equivalent to geometric irreducibility for smooth varieties). It also holds under pullback along the map $X(Np)^{(\zeta_{Np})}_{\mathbb{F}_{q^2}} \to X_1^\mu(Np)_{\mathbb{F}_{q^2}}$ as this covering is totally ramified at the point ∞, so that there is a closed point x of $Z'_{\mathbb{F}_{q^2}}$ for which the preimage in $Z''_{\mathbb{F}_{q^2}}$ consists of a single point y with degree equal to that of $X(Np)^{(\zeta_{Np})}_{\mathbb{F}_{q^2}} \to X_1^\mu(Np)_{\mathbb{F}_{q^2}}$. We may pass to $\overline{\mathbb{F}}_q$ without changing ramification behavior, and we have that the geometric connected component of y must map to $Z'_{\overline{\mathbb{F}}_q}$ with that same degree, proving connectedness of $Z''_{\overline{\mathbb{F}}_q}$.

Finally, the splitting behavior at supersingular points holds as the supersingular points of $X(Np)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}}$ are all $\mathbb{F}_{q^2}$-rational, so the fibers of supersingular points of $X(Np)^{\mathrm{Ihara}}_{\mathbb{F}_{q^2}}$ in $Z''_{\mathbb{F}_{q^2}}$

are isomorphic to those of $X_1^\mu(Np; A)_{\mathbb{F}_{q^2}}$ in $Z_{\mathbb{F}_{q^2}}$.

Determining the structure of the fibers of the covering 4.3.6 at supersingular points is the difficult part of Ohta's and Vatsal's argument. Vatsal had the inspired idea of using the Iwasawa theory at an auxiliary prime $l \neq p$ of an auxiliary imaginary quadratic field K in which prime divisors of Np are totally split to understand the splitting behavior at *CM points* of the modular curve over the ring of integers of the *global* field k_A. He then related this to the splitting behavior at supersingular points of the special fibers using the surjectivity of a reduction map from the CM points defined over the ring class field of K of conductor l^n to the supersingular points in the fiber at particular primes q for sufficiently large n. This latter result was in fact at the time recently obtained by Vatsal and Cornut. Generalizing Vatsal and Cornut's result, who worked only with the curve $X_0(Np)$, Ohta showed that all supersingular points of $X_1^\mu(Np)_{\mathbb{F}_{q^2}}$ are the reductions of certain CM points on $X_1^\mu(Np)_{\mathbb{Q}}$. Let us set up notation to precisely state this result. We will opt to state the results as generally as they appear in [Oh20] and refrain from making particular choices until we are set to apply the result to our case in hand.

4.3.2 Surjection of CM points

Let K be an imaginary quadratic field such that $\mathcal{O}_K = \{\pm 1\}$, and let M be a positive integer for which all prime divisors of M split completely in K. Let $\mathfrak{m}$ be an integral ideal of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{m} \cong \mathbb{Z}/M\mathbb{Z}$. Fix a prime $l \nmid M$ and define H_n to be the ring class field of K of conductor l^n for each $n \geq 0$ (so that $\mathrm{Gal}(H_n/K)$ is naturally isomorphic to the class group of the order $\mathcal{O}_{K,l^n} := \mathcal{O}_K + l^n\mathcal{O}_K$ of conductor l^n of $\mathcal{O}_K$), and define $H_\infty = \bigcup_n H_n$. Fix an elliptic curve $E/\mathbb{C}$ with CM by $\mathcal{O}_K$ and define $\mathcal{L}_l$ to be the set of all subgroups of $E(\overline{\mathbb{Q}})$ of order some power of l. Let $C = E(\mathbb{C})[\mathfrak{m}]$, which is a cyclic subgroup of order M. Then we may define a map producing CM points on $X_0(M)_{H_\infty}$:

$$\mathcal{H} : \mathcal{L}_l \to X_0(M)(H_\infty) \text{ by } \mathcal{H}(X) := [E/X \to E/(X + C)].$$

Let $q \nmid lM$ be any prime that is inert in K. Then class field theory tells us that q splits completely in H_∞/K so that the residue field of any prime $\mathfrak{Q}$ of H_∞ lying over q is isomorphic to $\mathbb{F}_{q^2}$. We thus have a reduction map

$$\mathrm{red}_q : X_0(M)(H_\infty) \hookrightarrow X_0(M)_{\mathbb{Z}[1/M]}(\mathcal{O}_{H_\infty,\mathfrak{Q}}) \to X_0^{\mathrm{ss}}(M)_{\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}) \subset X_0(M)_{\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}),$$

where $\mathcal{O}_{H_\infty,\mathfrak{Q}}$ is the ring of integers of the completion of H_∞ at $\mathfrak{Q}$ and where the inclusion follows from the valuative criterion of properness (whence our need to base change to $\mathbb{Z}[1/M]$), which lands in the subset of points of the supersingular locus $X_0^{\mathrm{ss}}(M)$ as q is inert in K, by a classical result of Deuring [La87a, Ch. 13 Theorem 12]. Let $\overline{\mathfrak{m}}$ denote the conjugate ideal in $\mathcal{O}_K$ of $\mathfrak{m}$, and let $K(\overline{\mathfrak{m}})$ denote the ray class field of K of modulus $\overline{\mathfrak{m}}$. Then any point of $X_1^\mu(Np)$ lying over a point in the image of $\mathrm{red}_q \circ \mathcal{H}$ is defined over the field $H'_\infty := H_\infty \cdot K(\overline{\mathfrak{m}})$ by [Oh20, Lemma 3.2.1]. Define $X_0(M)(H_\infty)^{\mathrm{CM}}$ to be the image of $\mathcal{H}$ in $X_0(M)(H_\infty)$, and define $X_1^\mu(M)(H'_\infty)^{\mathrm{CM}}$ to be the preimage of $X_0(M)(H_\infty)^{\mathrm{CM}}$ induced by the natural map $X_1^\mu(M) \to X_0(M)$ which on points sends $(E/T, \beta\colon \mu_{M,T} \hookrightarrow E[M])$ to $(E/T, \mathrm{im}(\beta))$. For any prime $q \nmid Ml$ inert in K and completely split in $K(\overline{\mathfrak{m}})/K$, we may similarly define the reduction map

$$\mathrm{red}'_q : X_1^\mu(M)(H'_\infty) \to X_1^{\mu,\mathrm{ss}}(M)_{\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}).$$

We state Ohta's result for the map red'_q together with the original result of Vatsal and Cornut for red_q.

Theorem 4.3.3 ([Co02, Theorem 3.1], [Oh20, Proposition 3.2.5])**.** *The composite map*

$$\mathrm{red}_q \circ \mathcal{H} : \mathcal{L}_l \to X_0(M)^{\mathrm{ss}}_{\mathbb{F}_{q^2}}(\mathbb{F}_{q^2})$$

is surjective. The supersingular points of $X_1^\mu(M)_{\mathbb{F}_{q^2}}$ are all $\mathbb{F}_{q^2}$-rational, and the map red'_q induces a surjection

$$X_1^\mu(M)(H'_\infty)^{\mathrm{CM}} \to X_1^{\mu,\mathrm{ss}}(M)_{\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}).$$

4.3.3 Anticyclotomic analog of Washington's theorem

Finally, we look at the anticyclotomic Iwasawa theory of imaginary quadratic fields in order to control the splitting behavior of the CM points $X_1^\mu(Np)(H'_\infty)^{\mathrm{CM}}$ in the covering 4.3.5 over $S = \mathrm{Spec}(\mathcal{O}_{k_A}[1/Np])$. The key is to prove and use an anticyclotomic analog of Washington's result on the boundedness of the p-parts of class groups up a cyclotomic $\mathbb{Z}_l$-tower of an abelian number field for $l \neq p$. The proof of this requires Hida's result on the non-vanishing mod p of special values of L-functions associated with Hecke characters of the imaginary quadratic field (with certain conditions imposed on the characters) and (an affirmative answer to) the single-variable $\mathfrak{p}$-ramified main conjecture for the imaginary quadratic field, the latter of which was addressed in Theorem 2.4.6 of section 2.4.2.

As we did with the previous theorem, we continue to work generally, though we reuse notation in a manner that indicates how we intend to apply the results. Let K be an imaginary quadratic field with $\mathcal{O}_K = \{\pm 1\}$, and let p be an odd prime which splits as $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in K. Let $l \neq p$ be an odd prime unramified in K such that

$$\begin{cases} p \nmid (l-1) & \text{if } l \text{ splits in } K, \\ p \nmid (l+1) & \text{if } l \text{ is inert in } K. \end{cases}$$

Denote by H_n the ring class field of K of conductor l^n and set $H_\infty = \bigcup_n H_n$. The conditions on K and l imply that restriction $\mathrm{Gal}(H_n/K) \to \mathrm{Gal}(H_m/K)$ induces an isomorphism on the p-parts for $n \geq m \geq 0$ by Lemma 2.4.2. Let $\widetilde{H}_0/H_0$ be a finite abelian extension such that $\widetilde{H}_0/K$ is unramified at primes above l and such that primes that ramify in $\widetilde{H}_0/K$ are split in $K/\mathbb{Q}$, and set $\widetilde{H}_n = \widetilde{H}_0 \cdot H_n$ for $1 \leq n \leq \infty$.

We have the following result which was proved by Ohta under the assumption that $p \nmid [\widetilde{H}_0 : H_0]$ [Oh20, Theorem 2.1.6] and Vatsal under the assumption that $\widetilde{H}_0 = H_0$ [Va05, Proposition 3.1.9].

Theorem 4.3.4. *Let $\widetilde{H}_n^{\mathrm{ur}}$ be the maximal unramified abelian pro-p extension of $\widetilde{H}_n$ for $0 \leq n \leq \infty$. Then conditioned upon [Hi04, Propositions 2.7, 2.8], there exists an n_0 such* *that* $\widetilde{H}_n^{\mathrm{ur}} = \widetilde{H}_{n_0}^{\mathrm{ur}} \cdot \widetilde{H}_n$ *for* $n \geq n_0$*. In particular,* $\widetilde{H}_\infty^{\mathrm{ur}}$ *is a finite extension of* $\widetilde{H}_\infty$*.*

Proof. We remark that the results [Hi04, Propositions 2.7, 2.8] were fundamentally used in the arguments of Ohta [Oh20, pg. 381] and Vatsal [Va05, Theorem 3.13], and at the time the results were believed to be true. A preprint [Hi23] of Hida explains a hole in the argument pointed out by Venkatesh and proves a result which is weaker than that which is required by Ohta and Vatsal.

Let A_n denote the p-part of the class group of $\widetilde{H}_n$ and let $\mathfrak{X}_{\mathfrak{p},n}$ denote the $\mathfrak{p}$-ramified Iwasawa module of $\widetilde{H}_n$ as in Definition 2.4.5. Denote by $\mathcal{P}$ the prime ideal of $\mathcal{O}_{\bar{\mathbb{Q}}_p}$. For $\chi \in \widehat{\mathrm{Gal}(\widetilde{H}_n/K)}$ a character which is nontrivial modulo $\mathcal{P}$, we have that the vanishing of $\mathfrak{X}_{\mathfrak{p},n,\chi}$ implies the vanishing of $A_{n,\chi}$. Indeed, a nontrivial abelian unramified extension of F_n on which $\mathrm{Gal}(F_n/K)$ acts via χ would be linearly disjoint from $\widetilde{H}_n \cdot K^{\mathfrak{p}}$, where $K^{\mathfrak{p}}$ is the $\mathbb{Z}_p$-extension of K unramified outside of $\mathfrak{p}$, as $\mathrm{Gal}(\widetilde{H}_n \cdot K^{\mathfrak{p}}/\widetilde{H}_n)$ carries the trivial action of $\mathrm{Gal}(\widetilde{H}_n/K)$.

Corollary 2.2.6 tells us that $\mathfrak{X}_{\mathfrak{p},n,\chi} \cong \mathfrak{X}_{\mathfrak{p},m,\chi}$ and $A_{n,\chi} \cong A_{m,\chi}$ for any $n \geq m \geq \mathrm{cond}(\chi)$ (viewing χ as an element of both $\widehat{\mathrm{Gal}(\widetilde{H}_n/K)}$ and $\widehat{\mathrm{Gal}(\widetilde{H}_m/K)}$ by inflation). We may then view $\chi \in \varinjlim_n \widehat{\mathrm{Gal}(\widetilde{H}_n/K)}$, and as we wish to show that A_n stabilizes as n increases, we may consider $A_{n,\chi}$ and try to show that these vanish for all but finitely many χ (viewed inside the direct limit). By the above paragraph, our goal then is to show that $\mathfrak{X}_{\mathfrak{p},n,\chi}$ vanishes for all but finitely many χ (cf. [Va05, 3.3]).

We show that $\mathfrak{X}_{\mathfrak{p},n,\chi}$ is trivial by showing that the χ-component $\mathfrak{X}_{\mathfrak{p},n}^{\chi}$ is trivial. This would follow from the vanishing of the characteristic ideal of $\mathfrak{X}_{\mathfrak{p},n,\chi'}$ for each $\chi' \equiv \chi \bmod \mathcal{P}$ together with the fact that $\mathfrak{X}_{\mathfrak{p},n}^{\chi}$ contains no nontrivial finite $\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{H}_n \cdot K^{\mathfrak{p}}/\widetilde{H}_n)]]$-submodules [Gr78, §4].

Suppose that the prime-to-$\mathfrak{p}$ part of the conductor of χ is nontrivial. Then by Corollary 2.4.11, the characteristic ideal of $\mathfrak{X}_{\mathfrak{p},n,\chi} \otimes_{\mathbb{Z}_p} R$ in $R[[T]] \cong R[[\mathrm{Gal}(\widetilde{H}_n \cdot K^{\mathfrak{p}}/\widetilde{H}_n)]]$ is given by the p-adic Hecke L-function $f_\chi \in R[[T]]$, where R is the integer ring of the completion of

$\mathbb{Q}_p^{\mathrm{ur}}(\chi)$ and the isomorphism is given by $[\gamma_0] - 1 \leftrightarrow T$ for a choice of topological generator $\gamma_0 \in \mathrm{Gal}(\widetilde{H}_n \cdot K^{\mathfrak{p}}/\widetilde{H}_n)$.

Note that as $\widetilde{H}_0/H_0$ is linearly disjoint from H_n/H_0, characters of $\mathrm{Gal}(\widetilde{H}_n/K)$ may be written as products of characters of $\mathrm{Gal}(\widetilde{H}_0/K)$ with those of $\mathrm{Gal}(H_n/K)$. We now shift viewpoints and vary over characters of the latter groups. Let $\widehat{\mathfrak{g}}_\infty$ denote the direct limit of the character groups of $\mathrm{Gal}(H_n/K)$ along the dual of restriction maps. Let φ be any character of $\mathrm{Gal}(\widetilde{H}_0/K)$, and note that under the assumptions on $\widetilde{H}_0/K$, the conductor of φ is prime to l and is comprised of primes which split in $K/\mathbb{Q}$.

By our assumption that $\mathcal{O}_K^\times = \{\pm 1\}$, there exists a Hecke character of K of conductor $\mathcal{O}_K$ and infinity type $(2, 0)$ [Oh20, proof of Theorem II.2.3.5]. We take a large enough power ξ of this character so that the associated character $\xi^{\mathfrak{p}}$ of $\mathrm{Gal}(K(\mathfrak{p}^\infty)/K)$ factors through $\mathrm{Gal}(K^{\mathfrak{p}}/K)$. This auxiliary ξ allows us to consider p-adic Hecke L-functions as in Theorem 2.4.8. Finally, Corollary 2.4.9, [Oh20, Proposition II.1.2.3], and [Oh20, Theorem I], the latter of which is conditioned upon the veracity of [Hi04, Propositions 2.7, 2.8], tell us that for all but finitely many characters $\varepsilon \in \widehat{\mathfrak{g}}_\infty$ of nontrivial conductor, the constant term

$$f_{\varphi\varepsilon}(\xi^{\mathfrak{p}}(\gamma_0) - 1)$$

is a p-adic unit, so that $f_{\varphi\varepsilon}$ is a unit power series.

$\square$

Corollary 4.3.5 ([Oh20, Corollary 2.1.7])**.** *Let Σ be a finite set of primes of K which are split in $K/\mathbb{Q}$ and which do not divide p. Let $M_{\infty,\Sigma}$ be the maximal Σ-ramified abelian pro-p extension of $\widetilde{H}_\infty$. Then $\mathrm{Gal}(M_{\infty,\Sigma}/\widetilde{H}_\infty)$ is finitely generated as a $\mathbb{Z}_p$-module.*

Proof. The group $\mathrm{Gal}(M_{\infty,\Sigma}/\widetilde{H}_\infty)$ surjects onto $\mathrm{Gal}(\widetilde{H}_\infty^{\mathrm{ur}}/\widetilde{H}_\infty)$, which is finite by Theorem 4.3.4, and has kernel generated by the inertia subgroups of primes of $\widetilde{H}_\infty$ lying above those in Σ. We will show that the kernel is also finitely generated as a $\mathbb{Z}_p$-module.

Any prime of K which is split over $\mathbb{Q}$ cannot split completely in the anticyclotomic

$\mathbb{Z}_l$-extension of K [Br07, Theorem 2], and therefore it only finitely splits in $\widetilde{H}_\infty/K$. Let $\tilde{\mathfrak{q}}$ be a prime of $\widetilde{H}_\infty$ lying over a prime of Σ. The inertia subgroup of $\tilde{\mathfrak{q}}$ in $\mathrm{Gal}(M_{\infty,S}/\widetilde{H}_\infty)$ arises from tame inertia and so is at most rank 1 as a $\mathbb{Z}_p$-module. There are only finitely many such primes $\tilde{\mathfrak{q}}$, so $\mathrm{Gal}(M_{\infty,S}/\widetilde{H}_\infty)$ has finite $\mathbb{Z}_p$-rank. $\square$

The following allows us to choose an appropriate prime q in order to contradict Ihara's theorem 4.3.2.

Corollary 4.3.6 ([Oh20, Corollary 2.1.8])**.** *Let the notation be as in the above theorem. Fix an $r \geq 1$, and let $\widetilde{L}_n$ be the compositum of all Σ-ramified abelian extensions of $\widetilde{H}_n$ of degree dividing p^r. Then each $\widetilde{L}_n/\widetilde{H}_n$ is a finite extension, and there exists an n_1 such that $\widetilde{L}_n = \widetilde{L}_{n_1} \cdot \widetilde{H}_n$ for all $n \geq n_1$.*

Proof. The groups $\mathrm{Gal}(\widetilde{L}_n/\widetilde{H}_n)$ for $n \geq 0$ are quotients of $\mathrm{Gal}(M_{\infty,\Sigma}/\widetilde{H}_\infty)$ of Corollary 4.3.5 of exponent dividing p^r. Thus, they must eventually stabilize as n increases. $\square$

We now return to our covering

$$Z_S \to X_1^\mu(Np; A)_S, \tag{4.3.8}$$

where $S = \mathrm{Spec}(\mathcal{O}_{k_A}[1/Np])$, and make our choices of auxiliary field K and prime l. We fix an imaginary quadratic field K in which all primes which ramify in $k_A/\mathbb{Q}$ are split in $K/\mathbb{Q}$, all primes dividing Np are split in $K/\mathbb{Q}$, and $\mathcal{O}_K = \{\pm 1\}$. We then fix an odd prime $l \nmid Np$ unramified in K and in k_A such that $p \nmid (l-1)$ if l is split in K and $p \nmid (l+1)$ if l is inert in K, and as before we denote by H_n and H_∞ the fields occuring in the tower of ring class fields of conductor l^n of K. Let $\mathfrak{m}$ be an integral ideal of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{m} \cong \mathbb{Z}/Np\mathbb{Z}$. With this we may then consider the set of CM points $X_0^\mu(M)(H_\infty)^{\mathrm{CM}}$ as above. We set $\widetilde{H}_0 := k_A \cdot K(\overline{\mathfrak{m}})$ and define $\widetilde{H}_n := \widetilde{H}_0 \cdot H_n$ so that the points of $X_1^\mu(Np)$ and $X_1^\mu(Np; A)$ lying over $X_0^\mu(M)(H_\infty)^{\mathrm{CM}}$ are all rational over $\widetilde{H}_\infty$. We let

$$X_1^\mu(Np)(\widetilde{H}_\infty)^{\mathrm{CM}} \text{ and } X_1^\mu(Np; A)(\widetilde{H}_\infty)^{\mathrm{CM}}$$

denote the inverse images of $X_0^\mu(Np)(\tilde{H}_\infty)^{\mathrm{CM}}$ in $X_1^\mu(Np)$ and $X_1^\mu(Np;A)$, respectively.

Let $\widetilde{L}_n$ denote the compositum of all S_N-ramified abelian extensions of degree p of $\widetilde{H}_n$ for each $0 \leq n \leq \infty$. Then $\widetilde{L}_n/\widetilde{H}_n$ is finite by the above corollary.

Lemma 4.3.7 ([Oh20, Lemma 5.3.8])**.** *For any $x \in X_1^\mu(Np;A)(\widetilde{H}_\infty)^{\mathrm{CM}}$, the points in the fiber of $Z_{k_A} \to X_1^\mu(Np;A)_{k_A}$ over x are rational over $\widetilde{L}_\infty$.*

Note that in particular the residue fields occuring in the fiber of x are unramified over x at places above p. The proof of this critically uses the technical hypothesis that the group $A \leqslant (\mathbb{Z}/p\mathbb{Z})^\times$ is nontrivial in order to invoke the fact that one can extend an exact sequence of abelian varieties over a p-adic local field to an exact sequence of Néron models over a DVR provided that the absolute ramification index over $\mathbb{Z}_p$ is strictly less than $p-1$; see [Oh20, Proposition 4.2.1] and [BLR90, §7.5 Theorem 4] for more precise statements.

We may now choose a prime $q \nmid Npl$ which is inert in K and splits completely in $\widetilde{L}_{n_1}$, where n_1 is as in Corollary 4.3.6. Then as q is inert in $K/\mathbb{Q}$, by class field theory it must split completely in the union of ring class fields H_∞ [Br07, pg. 2132] and so it splits completely in $\widetilde{L}_\infty$. Fixing a place $\mathfrak{Q}$ of $\widetilde{H}_\infty$ over q, we may pullback $Z_S \to X_1^\mu(Np;A)_S$ along the residue field of $\mathfrak{Q}$ to obtain a geometrically irreducible covering (cf. the discussion after equation 4.3.7)

$$Z_{\mathbb{F}_{q^2}} \to X_1^\mu(Np;A)_{\mathbb{F}_{q^2}}$$

in which we claim all supersingular points of $X_1^\mu(Np;A)_{\mathbb{F}_{q^2}}$ are completely split. Indeed, we have surjections

$$X_1^\mu(Np)(\widetilde{H}_\infty)^{\mathrm{CM}} \to X_1^{\mu,\mathrm{ss}}(Np)_{\mathbb{F}_{q^2}}(\mathbb{F}_{q^2})$$

and

$$X_1^\mu(Np;A)(\widetilde{H}_\infty)^{\mathrm{CM}} \to X_1^{\mu,\mathrm{ss}}(Np;A)_{\mathbb{F}_{q^2}}(\mathbb{F}_{q^2})$$

onto the supersingular loci from Theorem 4.3.3 so that $x \in X_1^{\mu,\mathrm{ss}}(Np;A)_{\mathbb{F}_{q^2}}(\mathbb{F}_{q^2})$ occurs as the special fiber of a $\mathrm{Spec}(\mathcal{O}_{\widetilde{H}_n,\mathfrak{Q}})$-point $\tilde{x}$ of $X_1^\mu(Np;A)_S$ for some n. Lemma 4.3.7 tells us that the fiber along $\tilde{x}$ of $Z_S \to X_1^\mu(Np;A)_S$ is the spectrum of a valuation ring of a subfield of $\widetilde{L}_\infty$ at a place over q, and thus its residue field is isomorphic to $\mathbb{F}_{q^2}$.

Finally, note that $K(\overline{\mathfrak{m}}) \subset \widetilde{H}_0$ so that the condition that q is inert in K and split in $\widetilde{L}_{n_1}$ forces $q \equiv \pm 1 \bmod Np$. For such q, we have an identification of models $X(Np)_{\mathbb{F}_{q^2}} = X(Np)_{\mathbb{F}_{q^2}}^{\mathrm{Ihara}}$ as explained in section 3.1.2. As $X(Np)_{\mathbb{F}_{q^2}}^{\mathrm{Ihara}}$ has all supersingular points rational over $\mathbb{F}_{q^2}$ by construction, we may pull back the covering $Z_{\mathbb{F}_{q^2}} \to X_1^\mu(Np;A)_{\mathbb{F}_{q^2}}$ along $X(Np)_{\mathbb{F}_{q^2}} \to X_1^\mu(Np;A)_{\mathbb{F}_{q^2}}$ to obtain a geometrically connected $\mathbb{Z}/p\mathbb{Z}$-covering of $X(Np)_{\mathbb{F}_{q^2}}^{\mathrm{Ihara}}$ in which all supersingular points are completely split, as explained in the discussion following equation 4.3.7. This contradicts Ihara's theorem, Theorem 4.3.2.

Recall that our goal at the start of section 4.3 was to show that Υ is surjective. We explained in section 4.3.1 that this would follow from Theorem 4.3.1, and that our strategy to prove Theorem 4.3.1 was to assume otherwise and to arrive at a contradiction of Ihara's theorem with $M = Np$ and an appropriately chosen q. The above contradiction therefore concludes the proof of Theorem 4.3.1 and the proof of surjectivity of Υ (conditioned upon the veracity of the claims of [Hi04, Propositions 2.7, 2.8], which as of now is still an open question).

We remark that Ohta proves Υ is an isomorphism in [Oh20] by invoking the main conjecture. Surjectivity of Υ tells us that $(\xi_{\theta_{(0)}}) \supseteq \mathrm{char}(P^\iota)$ inside $\Lambda_{\mathcal{O}}$, or $\Lambda_{\mathcal{O}}[1/p]$ in Case B, but as we have only defined Υ for non-exceptional characters, we cannot use the class number formula to deduce the main conjecture from these divisibilities alone. However, we have the following, conditioned upon the veracity of the claims of [Hi04, Propositions 2.7, 2.8].

Theorem 4.3.8. *If $p \nmid \varphi(N)$, then Υ is an isomorphism. In general, the map $\Upsilon[1/p]$ is an isomorphism.*

Proof. We have already shown that Υ is surjective in both Case A and Case B in the terminology of Definition 4.2.7. The main conjecture, Theorem 2.2.8, tells us that Υ is a pseudo-isomorphism. In general, by the vanishing of the μ-invariant of $Y_{F,S_{Np},\omega^{-1}\theta^{-1}}$ [FW79], one has that there are no nontrivial finite $\Lambda_{\mathcal{O}}$-submodules of $Y_{F,S_{Np},\omega^{-1}\theta^{-1}}(1) \otimes_{\mathbb{Z}_p[\theta]} \mathcal{O}[1/p]$. Thus, $\Upsilon[1/p]$ is an isomorphism. In the case that $p \nmid \varphi(N)$, we may use the fact that $Y_{F,S_{Np},\omega^{-1}\theta^{-1}}$ has no p-torsion, which follows from [Wa97, Propositions 13.26, 13.28] and Lemma 4.2.8, to conclude that Υ is an isomorphism.

$\square$

REFERENCES

[AS95] A. Ash, G. Stevens, "p-adic deformations of cohomology classes of subgroups of $\mathrm{GL}(n, \mathbb{Z})$", *Collectanea Mathematica*, Vol. 48, 1997, pp. 1–30.

[Ar73] J. Arnold, "Krull dimension in power series rings", *Transactions of the American Mathematical Society*, Vol. 177 (1973), pp. 299–304.

[Bl05] W. Bley, "On the equivariant Tamagawa number conjecture for abelian extensions of a quadratic imaginary field", *Documenta Mathematica*, Vol. 11 (2005), pp. 73–118.

[BLR90] S. Bosch, W. Lütkebohmert, M. Raynaud, "Néron Models", *A Series of Modern Surveys in Mathematics*, Vol. 21, Springer-Verlag, 1990.

[Br07] D. Brink, "Prime decomposition in the anti-cyclotomic extension", *Mathematics of Computation*, Vol. 76 (2007), pp. 2127–2138.

[Br67] A. Brumer, "On the units of algebraic number fields", *Mathematika*, Vol. 14 (1967), pp. 113–233.

[Ca16] B. Cais, "The geometry of Hida families I: Λ-adic de Rham cohomology", *Mathematische Annalen*, Vol. 372 (2018), pp. 781–844.

[Ca18] B. Cais, "The geometry of Hida families II: Λ-adic (φ, Γ)-modules and Λ-adic Hodge theory", *Compositio Mathematica*, Vol. 154 (2018), pp. 719–769.

[Ce17] K. Cĕsnavičius, "A modular description of $\mathcal{X}_1(n)$", *Algebra & Number Theory*, Vol. 11 (2017), pp. 2001–2089.

[Co05] B. Conrad, "The Keel-Mori theorem via stacks", `https://math.stanford.edu/~conrad/papers/coarsespace.pdf`, 2005.

[Co07] B. Conrad, "Arithmetic moduli of generalized elliptic curves", *Journal of the Inst. of Math. Jussieu*, Vol. 6 (2007), pp. 209–278.

[Co02] C. Cornut, "Mazur's conjecture on higher Heegner points", *Inventiones Mathematicae*, Vol. 148 (2002), pp. 495–523.

[Co13] D. Cox, "Primes of the form $x^2 + ny^2$", 2nd edition, John Wiley & Sons Inc., 2013.

[De69] P. Deligne, "Formes modulaires et représentations ℓ-adiques" in *Séminaire Bourbaki*, Exposé 355 (1969), pp. 139–172.

[DR73] P. Deligne, M. Rapoport, "Les schémas de modules de courbes elliptiques", *Lecture Notes in Mathematics*, Vol. 349, Springer, pp. 143–316, 1973.

[DI95] F. Diamond, J. Im, "Modular forms and modular curves", *Canadian Mathmematical Society Conference Proceedings*, Vol. 17 (1995), pp. 39–133.

[DS05] F. Diamond, J. Shurman, "A first course in modular forms" 1st edition, *Graduate Texts in Mathematics*, Vol. 228, Springer-Verlag, 2005.

[Ei57] M. Eichler, "Eine verallgemeinerungder abelschen integrale", *Mathematische Zeitschrift*, Vol. 67. (1957), pp. 267–298.

[El90] R. Elkik, "La Théorm̀e de Manin-Drinfeld", *Astérisque*, tome 183. (1990), pp. 59–67.

[FW79] B. Ferrero, L. Washington, "The Iwasawa invariant μ_p vanishes for abelian number fields", *Annals of Mathematics*, Vol. 109 (1979), pp. 377–395.

[FK12] T. Fukaya, K. Kato, "On conjectures of Sharifi", preprint, version August 15, 2012.

[FKS15] T. Fukaya, K. Kato and R. Sharifi, "Modular symbols in Iwasawa theory" in *Iwasawa Theory 2012: State of the Art and Recent Advances*, Springer, (2015).

[Gi85] R. Gillard, "Fonctions L p-adiques des corps quadratiques imaginaires et de leurs extensions abéliennes", *Journal f̀ur die reine und angewandte Mathematik*, Vol. 138 (1985), pp. 76–91.

[Gr71] R. Greenberg, "On some questions concerning the Iwasawa invariants", Ph.D. dissertation, Princeton University.

[Gr78] R. Greenberg, "On the structure of certain Galois groups", *Inventiones Mathematicae*, Vol. 47 (1978), pp. 85–99.

[Gr90] B. Gross, "A tameness criterion for Galois representations associated with modular forms (mod p)", *Duke Mathematical Journal*, Vol. 61 (1990), pp. 445–517.

[SGA4.3] A. Grothendieck, "Théorie des topos et cohomologie étale des schémas" tome 3, *Lecture Notes in Mathematics*, Vol. 305, Springer-Verlag, 1972.

[SGA5] A. Grothendieck, "Cohomologie ℓ-adique et fonctions L", *Lecture notes in Mathematics*, Vol. 569, Springer-Verlag, 1977.

[SGA7] A. Grothendieck, "Modèls de Néron et monodromie" in SGA 7 I, *Lecture notes in Mathematics*, Vol. 288, Springer-Verlag, 1972, pp. 313-523.

[HP92] G. Harder and R. Pink, "Modular konstruierte unverzweigte abelsche p-Erweiterungen von $\mathbb{Q}(\zeta_p)$ und die Strukturihrer Galoisgruppen", *Mathematische Nachrichten*, Vol. 159 (1992), pp. 83–99.

[Hi85] H. Hida, "A p-adic measure attached to zeta functions associated with two elliptic modular forms. I", *Inventiones Mathematica*, Vol. 79 (1985), pp. 159–195.

[Hi86a] H. Hida, "Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms", *Inventiones mathematicae*, Vol. 85 (1986), pp. 545–613.

[Hi86b] H. Hida, "Iwasawa modules attached to congruences of cusp forms", *Annales Scientifiques de l'École Normale Supérieure*, Vol. 19 (1986), pp. 231–273.

[Hi88a] H. Hida, "Modules of congruence of Hecke algebras and L-functions associated with cusp forms", *American Journal of Mathematics*, Vol. 110, No. 2 (1988), pp. 323–382.

[Hi88b] H. Hida, "On p-adic Hecke algebras for GL_2 over totally real fields", *Annals of Mathematics*, Vol. 128, No. 2 (1988), pp. 295–384.

[Hi93] H. Hida, "Elementary theory of L-functions and Eisenstein series", *Mathematical Society Student Books*, Vol. 26, Cambridge University Press, 1993.

[Hi00] H. Hida, "Modular forms and Galois cohomology", *Cambridge Studies in Advanced Mathematics*, Vol. 69, Cambridge University Press, 2000.

[Hi04] H. Hide, "Non-vanishing modulo p of Hecke L-values", in *Geometric Aspects of Dwork Theory*, Walter de Gruyter, 2004, pp. 735–784.

[Hi22] H. Hida, "Elementary Modular Iwasawa theory", *Series on Number Theory and its Applications*, Vol. 16, World Scientific Publishing Co., 2022.

[Hi23] H. Hida, "Non-vanishing of integral of a mod p modular form, preliminary version", preprint, version August 27, 2022.

[Ig59] J. Igusa "Kroneckerian model of fields of elliptic modular functions", *American Journal of Mathematics*, Vol. 81 (1959), pp. 561–577.

[Ih75] Y. Ihara, "On modular curves over finite fields" in *Discrete Subgroups of Lie Groups and Applications to Moduli*, Oxford University Press, 1975, pp. 161–202.

[Iw59a] K. Iwasawa, "On Γ-extensions of algebraic number fields", *Bulletin of the American Mathematical Society*, Vol. 65 (1959), pp. 182–226.

[Iw59b] K. Iwasawa, "On the theory of cyclotomic fields", *Annals of Mathematics*, Vol. 70 (1959)., pp. 530–561.

[Iw69] K. Iwasawa, "On p-adic L-functions", *Annals of Mathematics*, Vol. 89 (1969), pp. 198–205.

[Iw73] K. Iwasawa, "On $\mathbb{Z}_l$-extensions of algebraic number fields", *Annals of Mathematics*, Vol. 98 (1973), pp. 246–326.

[Ka04] K. Kato, "p-adic Hodge theory and values of zeta functions of modular forms", *Astérisque*, tome 295 (2004), pp. 117–290.

[Ka72] N. Katz, "p-adic properties of modular schemes and modular forms", *Springer Lecture Notes in Mathematics*, Vol. 350 (1973), pp. 70–189.

[Ka76] N. Katz, "p-adic interpolation of real analytic Eisenstein series", *Annals of Mathematics*, Vol. 104, No. 3 (1976), pp. 459–571.

[KM85] N. Katz and B. Mazur, "Arithmetic moduli of elliptic curves", *Annals of Mathematics studies*, Vol. 108, Princeton University Press, 1985.

[Ku93] M. Kurihara, "Ideal class groups of cyclotomic fields and modular forms of level 1", *Journal of Number Theory*, Vol. 45 (1993), 281–294.

[La15a] M. Lafferty, "Eichler-Shimura cohomology groups and the Iwasawa main conjecture", Ph.D. dissertation, The University of Arizona.

[La15b] M. Lafferty, "Hida duality and the Iwasawa main conjecture", *Mathematische Annalen*, Vol. 375 (2019), pp. 737–776.

[La87a] S. Lang, "Elliptic Functions", Second edition, *Graduate Texts in Mathematics*, Vol. 112, Springer-Verlag, 1987.

[La87b] S. Lang, "Introduction to Modular Forms", *A Series of Comprehensive Studies in Mathematics*, Springer-Verlag, 1987.

[Li02] Q. Liu, "Algebraic Geometry and Arithmetic Curves", *Oxford Graduate Tests in Mathematics*, Vol. 6, Oxford University Press, Oxford, 2002.

[Ma77] B. Mazur, "Modular curves and the Eisenstein ideal", *Publications Mathématiques I.H.E.S.*, tome 47 (1977), pp. 33–186.

[MW84] B. Mazur and A. Wiles, "Class fields of abelian extensions of $\mathbb{Q}$", *Inventiones Mathematicae*, Vol. 76 (1984), pp. 179–330.

[MW86] B. Mazur and A. Wiles, "On p-adic analytic families of Galois representations", *Compositio Mathematica*, Vol. 59, No. 2 (1986), pp. 231–264.

[Mi06] J. Milne, "Arithmetic duality theorems", 2nd edition, BookSurge LLC., 2006.

[NP00] J. Nekovář and A. Plater, "On the parity of ranks of Selmer groups", *Asian Journal of Mathematics*, Vol. 4 (2000), pp.437–498.

[Ne99] J. Neukirch, "Algebraic Number Theory", English translation by N. Schappacher, *Grundlehren der mathematischen Wissenschaften*, Vol. 322, 1999.

[NSW13] J. Neurkich, A. Schmidt, K. Wingberg, "Cohomology of Number Fields", 2nd ed., corrected second printing, *Grundlehren der mathematischen Wissenschaften* , Vol. 323, Springer, 2013.

[Oh93] M. Ohta, "On cohomology groups attached to towers of algebraic curves", *Journal of the Mathematical Society of Japan*, Vol. 45, No. 1 (1993), pp. 131–183.

[Oh95] M. Ohta, "On the p-adic Eichler-Shimura isomorphism for $\tilde{\Lambda}$-adic cusp forms", *Journal f̀ur die reine und angewandte Mathematik*, Vol. 463 (1995), pp. 49–98.

[Oh99] M. Ohta, "Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves", *Compositio Mathematica*, Vol. 115 (1999), pp. 241–301.

[Oh00] M. Ohta, "Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves II", *Mathematische Annalen*, Vol. 318 (2000), pp. 557–583.

[Oh03] M. Ohta, "Congruence modules related to Eisenstein series", *Annales scientifiques de l'École Normale Supérieure, Quatrième Série*, Vol. 36 (2003), pp. 225–269.

[Oh20] M. Ohta, "μ-type subgroups of $J_1(N)$ and applications to cyclotomic fields", *Journal of the Mathematical Society of Japan*, Vol. 72, No. 2 (2020), pp. 333–412.

[OV16] H. Oukhaba, S. Viguié, "On the μ-invariants of Katz p-adic L-functions attached to imaginary quadratic fields", *Forum Mathematicum*, Vol. 28 (2016), pp. 507–525.

[Pr09] K. Prasanna, "Arithmetic properties of the Shimura-Shintani-Waldspurger correspondence", *Inventiones Mathematica*, Vol. 176 (2009), pp. 521–600.

[RZ10] L. Ribes, P. Zalesskii, "Profinite Groups", 2nd edition, *A Series of Modern Surveys in Mathematics*, Vol. 40, Springer, 2010.

[Ri76] K. Ribet, "A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$", *Inventiones mathematicae*, Vol. 34 (1976), pp. 151–162.

[Ri90] K. Ribet, "On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms", *Inventiones mathematicae*, Vol. 100 (1990), pp. 431–476.

[Ru91] K. Rubin, "The "main conjectures" of Iwasawa theory for imaginary quadratic fields", *Inventiones Mathematicae*, Vol. 103 (1991), pp. 25–68.

[Ru94] K. Rubin, "More "main conjectures" for imaginary quadratic fields", *Centre de Recherches Mathématiques Proceedings and Lecture Notes*, Vol. 4 (1994), pp. 23–28.

[Sc85] L. Schneps, "On the μ-invariant of p-adic L-functions attached to elliptic curves with complex multiplication", *Journal of Number Theory*, Vol. 25 (1985), pp. 20–33.

[Se60] J. P. Serre, "Classes des corps cyclotomiques", *Séminaire Bourbaki*, Exposé 174 (1960), pp. 83–93.

[Se72] J. P. Serre, "Formes modulaires et fonctions zeta p-adiques", *Springer Lecture Notes in Mathematics*, Vol. 350 (1973), pp. 191–268.

[Se88] J. P. Serre, "Algebraic Groups and Class Fields", *Graduate Texts in Mathematics*, Vol. 117, Springer-Verlag, 1988.

[dS87] E. de Shalit, "Iwasawa Theory of Elliptic Curves with Complex Multiplication", *Perspectives in Mathematics*, Vol. 3, Academic Press, 1987.

[Sh11] R. Sharifi, "A reciprocity map and the two-variable p-Adic L-Function", *Annals of Mathematics*, Vol. 173 (2011), pp. 251–300.

[Sh22] R. Sharifi, "Reciprocity maps with restricted ramification", *Transactions of the American Mathematical Society*, Vol. 375 (2022), pp. 5361–5392.

[Sh59] G. Shimura, "Sur les intégrales atachées aux formes automorphs", *Journal of the Mathematical Society of Japan*, Vol. 11, No. 4, (1959), pp. 291–311.

[Sh71] G. Shimura, "Introduction to the arithmetic theory of automorphic functions", *Publications of the Mathematical Society of Japan*, Vol. 11, Princeton University Press, 1971.

[SP] Authors, The Stacks Project, "Stacks Project", `https://stacks.math.columbia.edu/`.

[Ti87] J. Tilouine, "Un sous-groupe p-divisible de la jacobienne de $X_1(Np^r)$", *Bulletin de la Société Mathématique de France*, tome 115 (1987), pp. 329–360.

[Va05] V. Vatsal, "Multiplictive subgroups of $J_0(N)$ and applications to elliptic curves", *Journal of the Institute of Mathemetics of Jussieu*, Vol. 4 (2005), pp. 281–316.

[Vi16] S. Viguié, "On the classical main conjecture for imaginary quadratic fields", *Pioneer Journal of Algebra, Number Theory, and its Applications*, Vol. 12. (2016), pp. 1–27.

[WWE17] P. Wake and C. Wang-Erickson, "Pseudo-modularity and Iwasawa Theory", *American Journal of Mathematics*, Vol. 140 (2018), pp. 977–1040.

[Wa97] L. Washington, "Introduction to Cyclotomic Fields", *Graduate Texts in Mathematics*, Vol. 83, Springer-Verlag, 1997.

[Wi86] A. Wiles, "On p-adic representations for totally real fields", *Annals of Mathematics*, Vol. 123, No. 3 (1986), pp. 407–456.

[Wi88] A. Wiles, "On ordinary $\tilde{\Lambda}$-adic representations associated with modular forms", *Inventiones mathematicae*, Vol. 94 (1988), pp. 529–573.

[Wi90] A. Wiles, "The Iwasawa conjecture for totally real fields", *Annals of Mathematics*, Vol. 131, No. 3 (1990), pp. 493–540.