HIDA THEORY

R. SCOTT WILLIAMS

Contents

1. Introduction

Hida first began developing his theory of the ordinary part of a module in the 1980's and subsequently refined it over the next decade to describe the properties of the ordinary part of spaces of modular forms. In this work we seek to give a broad overview of Hida Theory, beginning with the construction of ordinary parts and ending with a discussion of ordinary Λ-adic Galois representations.

We will first present, as a reminder, some basic background information on several topics which will be used, directly or indirectly, throughout. Then we will move on to discuss the basics of Hida Theory and Λ-adic forms so that we can conclude with the construction and properties of ordinary Λ-adic Galois representations to the extent in which they were used in Wiles' proof of the Iwasawa main conjecture.

It must be added that none of this work is new. Most of it being taken or paraphrased from several standard Hida Theory references, and briefly expanded upon when necessary in an effort to present well rounded and clear descriptions of the theory.

2. Preliminaries

Before presenting the main topics, in an effort to make this paper more self-contained, let us briefly recall some basic definitions and results that will be central to our work.

We would like to set some notation. Let N be a positive integer. Fix algebraic closures of $\mathbb{Q}$ and $\mathbb{Q}_p$, denoting them by $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}_p}$. Let $\mathbb{C}_p$ denote the completion of $\overline{\mathbb{Q}_p}$ with respect to the normalized p-adic absolute value, $|\cdot|_p$, i.e., $|p|_p = 1/p$. We also fix embeddings $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_p}$ and $\overline{\mathbb{Q}_p} \to \mathbb{C}_p$. Finally, let K be a fixed finite extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}$.

2.1. Characters.

In general, a character is simply a function from a group to a field. Obviously, more conditions can be imposed on the function to obtain certain types of characters. Three characters of importance to us will be: Dirichlet, Teichmüller and cyclotomic characters. The following definitions come mostly from [DiSh07], [Coh07] and [RS11].

Definition 2.1.1. *A **Dirichlet character** modulo N is a homomorphism of multiplicative groups*

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times.$$

The set of Dirichlet characters modulo N is a multiplicative group which, in fact, is the dual group of $(\mathbb{Z}/N\mathbb{Z})^\times$. Since $(\mathbb{Z}/N\mathbb{Z})^\times$ is a finite group, it follows that $\chi(k)$ must be a root of unity for any $k \in (\mathbb{Z}/N\mathbb{Z})^\times$, i.e., $\chi\left((\mathbb{Z}/N\mathbb{Z})^\times\right) \subset \bigcup_{n=1}^N \mu_n$ where μ_n denotes the group of nth roots of unity.

If d is a positive divisor of N then every Dirichlet character χ modulo d lifts to a Dirichlet character χ_N modulo N given by

$$\chi_N(n \pmod N) = \chi(n \pmod d)$$

for every $n \in \mathbb{Z}$ with $(n, N) = 1$. However, going the other direction is not always possible. Let $\pi_{N,d} : (\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$ be the natural projection map, then we have the following definition:

Definition 2.1.2. *The **conductor** of a Dirichlet character χ modulo N is the smallest positive divisor d of N such that $\chi = \chi_d \circ \pi_{N,d}$ for some Dirichlet character χ_d modulo d. A Dirichlet character is said to be **primitive** if its conductor is N.*

We can extend a Dirichlet character χ modulo N to a function $\chi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ by defining $\chi(k) = 0$ for $k \notin (\mathbb{Z}/N\mathbb{Z})^\times$. We may then extend this further to a function $\chi : \mathbb{Z} \to \mathbb{C}$ given by $\chi(k) = \chi(n \pmod N)$, so that $\chi(n) = 0$ for all $n \in \mathbb{Z}$ such that $(n, N) > 1$. One should, however, notice that this extension is no longer a homomorphism.

If χ is a Dirichlet character then, via our fixed embedding $\overline{\mathbb{Q}} \to \mathbb{C}_p$, we may regard the values of χ as lying in $\mathbb{C}_p$. Then the character χ may be regarded as a p-adic object, or more precisely, a map $\mathbb{Z}_p \to \mathbb{C}_p$ multiplicative in $\mathbb{Z}_p^\times$. Such a function is then called a p-adic Dirichlet character. One particular p-adic character is the Teichmüller character which we now define.

Definition 2.1.3. *The **Teichmüller character** ω at a prime p is a $\mathbb{Z}_p^\times$-valued character of $(\mathbb{Z}/q\mathbb{Z})^\times$, where $q = p$ if p is odd and $q = 4$ if $p = 2$. If $x \in \mathbb{Z}_p$, then $\omega(x)$ is the unique solution in $\mathbb{Z}_p^\times$ of $\omega(x)^p = \omega(x) \equiv x \pmod p$, or equivalently we could define*

$$\omega(x) = \lim_{n\to\infty} x^{p^n}.$$

Finally, we want to discuss the last character of importance for us, the cyclotomic character. Let μ_ℓ denote the group of ℓth roots of unity in $\overline{\mathbb{Q}}$, then the action of $\mathrm{G}_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on μ_ℓ gives rise to a continuous homomorphism

$$\chi_\ell : \mathrm{G}_\mathbb{Q} \to \mathrm{Aut}(\mu_\ell) \cong (\mathbb{Z}/\ell\mathbb{Z})^\times = \mathbb{F}_\ell^\times.$$

Let ζ_n be a primitive p^nth root of unity. If $g \in \mathrm{G}_\mathbb{Q}$, g sends ζ_n to another primitive p^nth root of unity, say $g(\zeta_n) = \zeta_n^{a_{g,n}}$ for some $a_{g,n} \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. For a fixed g, as n varies, the $a_{g,n}$ form a compatible system, inducing an element in the inverse limit

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

Hence, $\chi_p(g) = (a_{g,n})_n \in \mathbb{Z}_p^\times$ encodes the action of g on p-power roots of unity.

Definition 2.1.4. *The map χ_ℓ given above, considered as a map $\chi_\ell : \mathrm{G}_\mathbb{Q} \to \mathbb{F}_\ell^\times$, is the mod-$\ell$ **cyclotomic character**. If p is a prime, then the **p-adic cyclotomic character** is $\chi_p : \mathrm{G}_\mathbb{Q} \to \mathbb{Z}_p^\times$.*

2.2. **Congruence Subgroups.** Much of our work will be based upon modular forms, which will be discussed in the next section, but before we discuss them we should first understand the notion of a congruence subgroup – essentially spaces where the modular forms will be invariant. Most of the following is taken from the exposition found in [DiSh07], but could also be found in any book on modular forms.

Definition 2.2.1. *The **principal congruence subgroup** of level N is*

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\}.$$

*A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a **congruence subgroup** if $\Gamma(N) \subset \Gamma$ for some N, and taking the minimal N, Γ is said to be a congruence subgroup of **level** N.*

Two very important congruence subgroups are

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\}.$$

2.3. **Modular Forms.** We are now at a point where we can describe modular forms. Obviously, the theory of modular forms is much richer than what is presented below, but we seek only to provide a reminder of the basics from which much of the remainder of this paper will be built upon. Again, much of the following information is taken from the exposition found in [DiSh07].

Definition 2.3.1. *For any matrix*

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

the ***factor of automorphy***, *$j(\gamma,\tau) \in \mathbb{C}$ for any $\tau \in \mathcal{H}$ (the upper half-plane), is given by $j(\gamma,\tau) = c\tau + d$, and for any integer k define the* ***weight-k*** *operator $[\gamma]_k$ on $f : \mathcal{H} \to \mathbb{C}$ by*

$$(f[\gamma]_k)(\tau) = j(\gamma,\tau)^{-k} f(\gamma(\tau)) \quad \text{for all } \tau \in \mathcal{H}.$$

Definition 2.3.2. *Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let k be an integer. A function $f : \mathcal{H} \to \mathbb{C}$ is a* ***modular form*** *of weight k with respect to Γ if*

(1) *f is holomorphic,*
(2) *f is weight-k invariant under Γ, i.e., $f[\gamma]_k = f$ for each $\gamma \in \Gamma$,*
(3) *$f[\alpha]_k$ is holomorphic at ∞ for each $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.*

If, in addition,

4. *$a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for each $\alpha \in \mathrm{SL}_2(\mathbb{Z})$,*

then f is a ***cusp form*** *of weight k with respect to Γ.*

The space of modular forms of weight k with respect to Γ is denoted $\mathcal{M}_k(\Gamma)$, and the space of weight k cusp forms is $\mathcal{S}_k(\Gamma)$. Of particular interest to us will be modular (and cusp) forms with respect to $\Gamma_1(N)$. For notation's sake, we will write $\mathcal{M}_k(N)$ (and $\mathcal{S}_k(N)$) for $\mathcal{M}_k(\Gamma_1(N))$ (and $\mathcal{S}_k(\Gamma_1(N))$).

We should take a moment to explain some parts of the above definition of a modular form. For one, we state that $f[\gamma]_k$ must be holomorphic at ∞ but do not explain what it means to be so; and second, we have claimed without proof that $f[\alpha]_k$ indeed has a Fourier expansion.

It is not hard to see that each congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ contains a translation matrix of the form

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} : \tau \mapsto \tau + h,$$

for some minimal $h \in \mathbb{Z}^+$. Then, if f is weight-k invariant under Γ, i.e., f satisfies (2) in the above definition, we will have $f(\tau + h) = f(\tau)$ so that f is $h\mathbb{Z}$-periodic. Let $D = \{q \in \mathbb{C} : |q| < 1\}$ be the open complex unit disk with $D' = D \backslash \{0\}$. Recall from complex analysis that the $h\mathbb{Z}$-periodic holomorphic map $\tau \mapsto e^{2\pi i\tau/h} = q_h$ takes $\mathcal{H}$ to D'. Thus, corresponding to f, the function $g : D' \to \mathbb{C}$ where $g(q) = f(h\log(q)/(2\pi i))$ is well defined and $f(\tau) = g(q_h)$.

If f is holomorphic on the upper half-plane, then the composition g is holomorphic on the punctured disk since the logarithm can be defined holomorphically about each point. Hence, g has a Laurent expansion $g(q) = \sum_{n\in\mathbb{Z}} a_n q^n$ for $q \in D'$. The relation $|q| = e^{-2\pi \mathrm{Im}(\tau)}$ shows that $q \to 0$ as $\mathrm{Im}(\tau) \to \infty$. We now define f to be holomorphic at ∞ if g extends holomorphically to $q = 0$, i.e., if the Laurent series sums over $n \in \mathbb{N}$. This means that f has a Fourier expansion

$$f(\tau) = \sum_{n=0}^{\infty} a_n q_h^n, \quad \text{where } q_h = e^{2\pi i\tau/h}.$$

As mentioned above, we are particularly interested in the congruence subgroup $\Gamma_1(N)$, and since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)$ our $h = 1$. Thus we write the expansion as

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f) q^n,$$

known as the ***q*-expansion** of f.

One of the reasons we introduced Dirichlet characters above is that they provide us with a way to decompose the vector spaces $\mathcal{M}_k(N)$ and $\mathcal{S}_k(N)$ into a direct sum of eigenspaces, each of which can then be studied independently.

Definition 2.3.3. *For each Dirichlet character χ modulo N, the **χ-eigenspace** of $\mathcal{M}_k(N)$ is given by*

$$\mathcal{M}_k(N, \chi) = \left\{ f \in \mathcal{M}_k(N) : f[\gamma]_k = \chi(d) f \text{ for each } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \right\},$$

and similarly for $\mathcal{S}_k(N, \chi)$.

With this the vector spaces $\mathcal{M}_k(N)$ and $\mathcal{S}_k(N)$ decompose as

$$\mathcal{M}_k(N) = \bigoplus_{\chi} \mathcal{M}_k(N, \chi) \quad \text{and} \quad \mathcal{S}_k(N) = \bigoplus_{\chi} \mathcal{S}_k(N, \chi).$$

We can define yet another subspace of modular forms based upon where the coefficients of the q-expansion lie. For any subring $A \subset \mathbb{C}$ we define

$$\mathcal{M}_k(N; A) = \{ f \in \mathcal{M}_k(N) : a_n(f) \in A \text{ for all } n \geq 0 \},$$

and

$$\mathcal{S}_k(N; A) = \mathcal{M}_k(N; A) \cap \mathcal{S}_k(N).$$

With this, the spaces $\mathcal{M}_k(N, \chi; A)$ and $\mathcal{S}_k(N, \chi; A)$ are defined in the obvious way.

Finally, one can see from the definitions that $\Gamma_1(N) \subset \Gamma_0(N)$, so it follows that the smaller group has more modular forms (since there are fewer γ for which a modular form must remain invariant under), i.e., $\mathcal{M}_k(\Gamma_1(N)) \supset \mathcal{M}_k(\Gamma_0(N))$.

As one last note, it is not hard to see that the map

$$\begin{array}{ccc} \Gamma_0(N) & \longrightarrow & (\mathbb{Z}/N\mathbb{Z})^\times \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & d \ (\mathrm{mod}\ N) \end{array}$$

is a surjective homomorphism with kernel $\Gamma_1(N)$. Hence, there exists an isomorphism

$$\begin{array}{ccc} \Gamma_0(N)/\Gamma_1(N) & \xrightarrow{\sim} & (\mathbb{Z}/N\mathbb{Z})^\times \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & d \ (\mathrm{mod}\ N). \end{array}$$

2.4. **Eisenstein Series.** One of the most standard examples of a modular form is given by the Eisenstein series, which is a 2-dimensional analogue of the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ with $\Re(s) > 1$.

Definition 2.4.1. *For any even integer $k > 2$ we define the weight k **Eisenstein series** to be the absolutely convergent infinite series*

$$E'_k(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^k}.$$

We may also consider a slightly more general version. For any nontrivial primitive Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$,

$$E'_{k,\chi}(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{\chi^{-1}(n)}{(mNz+n)^k}.$$

Since

$$\chi^{-1}(-n)(-mNz-n)^{-k} = \chi(-1)(-1)^k\chi^{-1}(n)(mNz+n)^{-k}$$

the series $E'_{k,\chi}$ is nontrivial only when $\chi(-1) = (-1)^k$. In this case, we have $E'_{k,\chi} \in \mathcal{M}_k(N,\chi)$ as seen in [Hid93, Sec. 5.1].

Before we can state the q-expansion of $E'_{k,\chi}$, we first want to recall the definitions of a few functions which will appear in the expansion. The Dirichlet L-function is given by

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

and satisfies (see [Hid93, Thm. 2.4.2])

$$L(1-k,\chi) = \frac{2N^k(k-1)!}{g(\chi^{-1})(-2\pi i)^k} L(k,\chi^{-1}),$$

where g denotes the Gauss sum which is given by

$$g(\chi) = \sum_{a=1}^{N} \chi(a) e^{2\pi i a/N}.$$

With these functions in hand, the q-expansion of $E'_{k,\chi}$ is given by

$$E'_{k,\chi} = 2L(k,\chi^{-1}) + 2\frac{(-2\pi i)^k g(\chi^{-1})}{N^k(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1,\chi}(n) q^n$$

where

$$\sigma_{k-1,\chi}(n) = \sum_{d|n} \chi(d) d^{k-1}.$$

To obtain a series with a 'nicer' expansion we now define

$$E_{k,\chi}(z) = \frac{N^k(k-1)!}{2g(\chi^{-1})(-2\pi i)^k} E'_{k,\chi}(z) = \frac{L(1-k,\chi)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1,\chi}(n) q^n.$$

We may also consider a slightly more general series for a now not necessarily primitive Dirichlet character χ modulo N given by

$$G'_{k,\chi}(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{\chi(m)}{(mz+n)^k}.$$

As with $E'_{k,\chi}$, if $k > 2$ is even and $\chi(-1) = (-1)^k$, we will have that $G'_{k,\chi} \in \mathcal{M}_k(N,\chi)$.

We also see that $G'_{k,\chi}$ has a slightly simpler q-expansion than that of $E'_{k,\chi}$, which is given by

$$G'_{k,\chi}(z) = 2\frac{(-2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma'_{k-1,\chi}(n)q^n,$$

where

$$\sigma'_{k-1,\chi}(n) = \sum_{d|n}\chi(n/d)d^{k-1}.$$

Again, we may scale this to obtain a cleaner expansion; let

$$G_{k,\chi}(z) = \frac{(k-1)!}{2(-2\pi i)^k}G'_{k,\chi}(z) = \sum_{n=1}^{\infty}\sigma'_{k-1,\chi}(n)q^n.$$

By [Hid93, Thm. 5.2.2] we know that $L(1-k,\chi) \in \mathbb{Q}(\chi)$ for all χ, so it follows that for every even $k > 2$ and for all Dirichlet characters χ modulo N,

$$G_{k,\chi} \in \mathcal{M}_k(N,\chi;\mathbb{Z}[\chi]),$$

and if χ is primitive,

$$E_{k,\chi} \in \mathcal{M}_k(N,\chi;\mathbb{Q}[\chi]).$$

2.5. ***p*-adic Modular Forms.** We have seen above that conventional modular forms are defined over a finite extension of $\mathbb{Q}$. A natural question would now be whether equivalent objects exist over the p-adics which also manage to reflect the p-adic topology. It was shown by Serre in the 1970's that such objects do indeed exist, and these have since been greatly generalized by Katz, Dwork, Hida and Coleman.

We present here only the most basic of definitions, which for our purposes will suffice. For a more detailed definition one should see [Ser73] or [Kat83].

Definition 2.5.1. *Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be an arbitrary Dirichlet character. For every integer $k \geq 2$ and every subring $A \subset \mathbb{C}_p$ such that $\mathbb{Z}[\chi] \subset A$, we define the* ***space of p-adic modular forms over A with respect to χ*** *by*

$$\mathcal{M}_k(N,\chi;A) = \mathcal{M}_k(N,\chi;\mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A,$$

and the ***space of p-adic cusp forms over A with respect to χ*** *by*

$$\mathcal{S}_k(N,\chi;A) = \mathcal{S}_k(N,\chi;\mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A.$$

By considering q-expansions the space $\mathcal{M}_k(N,\chi;\mathbb{Z}[\chi])$ is naturally embedded in the power series ring $\mathbb{Z}[\chi][[q]]$, and hence we may consider $\mathcal{M}_k(N,\chi;A)$ as the A-linear span of $\mathcal{M}_k(N,\chi;\mathbb{Z}[\chi])$ in $A[[q]]$; doing so allows us to consider the q-expansions of p-adic modular forms.

2.6. **Hecke Operators.** It can be shown that for any congruence subgroups Γ_1 and Γ_2 of $\mathrm{SL}_2(\mathbb{Z})$ there exists a special family of operators, known as the double coset operators (we will avoid providing a detailed definition of these operators in general), which are linear and take $\mathcal{M}_k(\Gamma_1)$ to $\mathcal{M}_k(\Gamma_2)$ (and also take cusp forms to cusp forms). Of particular interest to us is the case $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$, where the double coset operators are known as the Hecke operators. The following is based upon the exposition found in [DiSh07].

Definition 2.6.1. *Let $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. The Hecke operator known as the* ***diamond operator*** *is given by the map*

$$\begin{aligned} \langle d\rangle : \mathcal{M}_k(\Gamma_1(N)) &\longrightarrow \mathcal{M}_k(\Gamma_1(N)) \\ \langle d\rangle f &= f[\alpha]_k \end{aligned}$$

for any $\alpha = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N)$ with $\delta \equiv d \pmod N$.

For any character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}$ we have that $\mathcal{M}_k(N,\chi)$ is the χ-eigenspace of the diamond operators, i.e.,

$$\mathcal{M}_k(N,\chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)) : \langle d\rangle f = \chi(d) f \text{ for each } d \in (\mathbb{Z}/N\mathbb{Z})^\times\}.$$

Definition 2.6.2. *Let p be a prime. The Hecke operator $\boldsymbol{T_p}$ is given by the map*

$$T_p : \mathcal{M}_k(\Gamma_1(N)) \longrightarrow \mathcal{M}_k(\Gamma_1(N))$$

with

$$T_p f = \begin{cases} \displaystyle\sum_{j=0}^{p-1} f\left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}\right]_k & \text{if } p \mid N \\ \displaystyle\sum_{j=0}^{p-1} f\left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}\right]_k + f\left[\begin{pmatrix} m & n \\ N & p \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right]_k & \text{if } p \nmid N \end{cases}$$

where m, n are chosen such that $mp - nN = 1$.

One can then show that these Hecke operators commute:

Proposition 2.6.3. *Let $d, e \in (\mathbb{Z}/N\mathbb{Z})^\times$ and let p, q be primes. Then*

1. $\langle d\rangle T_p = T_p \langle d\rangle$,
2. $\langle d\rangle\langle e\rangle = \langle e\rangle\langle d\rangle$,
3. $T_p T_q = T_q T_p$.

Proof. See [DiSh07, Prop. 5.2.4]. □

We may further extend the definitions of $\langle d\rangle$ and T_p to ones without the requirements that $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ and p be a prime.

Let $n \in \mathbb{Z}^+$, if $(n, N) = 1$ then we set $\langle n\rangle = \langle n \pmod N\rangle$, and if $(n, N) > 1$, $\langle n\rangle = 0$. The mapping $n \mapsto \langle n\rangle$ is totally multiplicative, i.e., $\langle nm\rangle = \langle n\rangle\langle m\rangle$ for all $n, m \in \mathbb{Z}^+$.

Now we set $T_1 = 1$ (the identity operator), and since T_p is already defined we may inductively define

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}\langle p\rangle T_{p^{r-2}} \text{ for } r \geq 2.$$

One should note that by induction and Proposition 2.6.3 it follows $T_{p^r} T_{q^s} = T_{q^s} T_{p^r}$ for distinct primes p and q.

With this, we may multiplicatively extend to T_n for any $n \in \mathbb{Z}^+$,

$$T_n = \prod T_{p_i^{e_i}} \quad \text{where } n = \prod p_i^{e_i},$$

and hence it follows that $T_{nm} = T_n T_m$ if $(n, m) = 1$.

Of more interest to us will be the manner in which Hecke operators act on the spaces of p-adic modular and cusp forms, so we will now provide a simple description. As discussed above, as with classical modular forms, we may consider the q-expansions of p-adic modular forms, and using this we will obtain our description of the Hecke action.

Proposition 2.6.4. *Let $f \in \mathcal{M}_k(N, \chi; A)$ with*

$$f = \sum_{n=0}^{\infty} a_n(f) q^n.$$

For all integers $m > 0$, we define $T_m f$ by

$$T_m f = \sum_{n=0}^{\infty} a_n(T_m f) q^n$$

where

$$a_n(T_m f) = \sum_{d|(m,n)} \chi(d) d^{k-1} a_{mn/d^2}(f)$$

for each $n \geq 0$.

Proof. See [DiSh07, Prop. 5.3.1] □

2.7. **Hecke Eigenforms.** The space $\mathcal{M}_k(N, \chi)$ is naturally a $\mathbb{C}$-vector space, and we know from above that the Hecke operators T_n are linear, so it makes sense to discuss their corresponding eigenvectors and eigenforms. Since, in this case, our eigenvectors will be modular forms, we instead refer to them as eigenforms.

Definition 2.7.1. *A modular form $f \in \mathcal{M}_k(N, \chi)$ is a **Hecke eigenform** if $T_n f = c_n f$ for some $c_n \in \mathbb{C}$ for each $n > 0$. If, in addition, $a_1(f) = 1$ we say that f is a **normalized Hecke eigenform**.*

One should note here that if $f = \sum_{n=0}^{\infty} a_n(f) q^n$ is a normalized Hecke eigenform then $T_i f = a_i(f) f$ for each i (See [RS11, Def. 3.5.9].)

Theorem 2.7.2. *Let $k \geq 1$ and $N > 0$. If $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is a primitive character, or $N = 1$ with $\chi = 1$, then $\mathcal{M}_k(N, \chi)$ has a basis of normalized Hecke eigenforms.*

Proof. See [Miy89, Thm. 4.7.2, Thm. 7.2.18]. □

In the previous theorem we saw that $\mathcal{M}_k(N, \chi)$ has a basis of normalized Hecke eigenforms; we now want to construct an explicit basis for sufficiently large k. Recall that the Eisenstein series $E_{k,\chi}$ and $G_{k,\chi}$ were defined in Section 2.4.

Theorem 2.7.3. *Let $a \geq 2$ be an integer and let ψ be a character modulo p^r with $\psi(-1) = (-1)^a$. Suppose further that $k > 2a+2$, then for any primitive character χ modulo p^r $(r \geq 1)$ with $\chi(-1) = (-1)^k$ there exists finitely many positive integers $n_1, \ldots, n_r$ such that $T_{n_j}(G_{a,\psi^{-1}} E_{k-1,\psi\chi})$ for $i = 1, \ldots, r$ together with $G_{k,\chi}$ and $E_{k,\chi}$ span $\mathcal{M}_k(p^r, \chi)$ over $\mathbb{C}$.*

Proof. See [Hid93, Sec. 5.4]. □

Definition 2.7.4. *Let $f \in S_k(N)$ be a normalized Hecke eigenform. The* ***number field associated to f****, denoted K_f, is the field generated over $\mathbb{Q}$ by the Fourier coefficients of f.*

With this definition we now have the following corollary.

Corollary 2.7.5. *Let $k \geq 0$ and let $f \in \mathcal{S}_k(N, \chi)$ be a normalized Hecke eigenform. Then $[K_f : \mathbb{Q}] < \infty$ and $a_n(f) \in \mathcal{O}_{K_f}$ for all positive integers n (where $\mathcal{O}_{K_f}$ denotes the ring of integers of K_f).*

Proof. See [Hid93, Cor. 5.4.2]. □

2.8. **The Hecke Algebra.** In this section we would like to define an algebra generated by the Hecke operators T_n and $\langle n \rangle$. To begin, let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be an arbitrary Dirichlet character.

Definition 2.8.1. *Let $k > 0$ and A be an arbitrary subalgebra of $\mathbb{C}$. For any A-submodule V of $\mathcal{M}_k(N; A)$ which is stable under the action of T_n and $\langle n \rangle$ for each $n \in \mathbb{N}$, we define the* ***Hecke algebra*** *$\mathcal{H}(V; A)$ to be the A-subalgebra of $\mathrm{End}_A(V)$ generated by $\{T_n, \langle n \rangle : n \in \mathbb{N}\}$.*

By Proposition 2.6.3 and the definitions of T_n and $\langle n \rangle$ it follows that $\mathcal{H}(V; A)$ is a commutative algebra; and since $T_1 \in \mathcal{H}(V; A)$ it is actually a commutative algebra with unity.

To set some notation we denote

$$\begin{aligned} \mathcal{H}_k(N; A) &= \mathcal{H}(\mathcal{M}_k(N; A); A), \\ h_k(N; A) &= \mathcal{H}(\mathcal{S}_k(N; A); A), \\ \mathcal{H}_k(N, \chi; A) &= \mathcal{H}(\mathcal{M}_k(N, \chi; A); A), \\ h_k(N, \chi; A) &= \mathcal{H}(\mathcal{S}_k(N, \chi; A); A), \end{aligned}$$

and we note that A will be omitted above whenever $A = \mathbb{C}$.

One should also take note that while the Hecke algebra is generated by both the operators T_n and $\langle n \rangle$, since $\langle n \rangle$ acts on $\mathcal{M}_k(N, \chi; A)$ and $\mathcal{S}_k(N, \chi; A)$ as multiplication by a constant, it follows that $\mathcal{H}_k(N, \chi; A)$ and $h_k(N, \chi; A)$ are generated by only $\{T_n\}_{n \in \mathbb{N}}$.

Further, as with p-adic modular forms (see Def. 2.5.1 above), we have

$$\mathcal{H}_k(N, \chi; A) \cong \mathcal{H}_k(N, \chi; \mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A$$

and

$$h_k(N, \chi; A) \cong h_k(N, \chi; \mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A.$$

We will see in Theorem 2.8.3 that there is a duality between these Hecke algebras and the spaces of modular and cusp forms. However, before describing it we first need a definition.

Definition 2.8.2. *Let A be a subalgebra of $\mathbb{C}$ with $\mathbb{Z}[\chi] \subset A$, and let $K = \operatorname{Frac} A$. Then we define*

$$\mathcal{M}_{k,0}(N,\chi;A) = \{f \in \mathcal{M}_k(N,\chi;K) : a_n(f) \in A \text{ for all } n \geq 1\}.$$

Theorem 2.8.3. *Let $k \geq 2$ and let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be an arbitrary character. For any subalgebra A of $\mathbb{C}$ containing $\mathbb{Z}[\chi]$, the pairing*

$$\begin{array}{rcl} \mathcal{H}_k(N,\chi;A) \times \mathcal{M}_{k,0}(N,\chi;A) & \longrightarrow & A \\ (H,f) & \longmapsto & a_1(fH) \end{array}$$

induces the following A-module isomorphisms

$$\begin{array}{rcl} \operatorname{Hom}_A(\mathcal{H}_k(N,\chi;A),A) & \cong & \mathcal{M}_{k,0}(N,\chi;A), \\ \operatorname{Hom}_A(h_k(N,\chi;A),A) & \cong & \mathcal{S}_k(N,\chi;A), \\ \operatorname{Hom}_A(\mathcal{M}_{k,0}(N,\chi;A),A) & \cong & \mathcal{H}_k(N,\chi;A), \\ \operatorname{Hom}_A(\mathcal{S}_k(N,\chi;A),A) & \cong & h_k(N,\chi;A). \end{array}$$

Proof. Our proof will consist of two parts; first, we will consider the case that either $N = 1$ or $A = \mathbb{C}$; then we will handle the general case where $N = qp^r$ for some $r \geq 0$.

By Theorem 2.7.3 we know that $\mathcal{M}_{k,0}(N,\chi;\mathbb{C})$, and hence $\operatorname{End}_{\mathbb{C}}(\mathcal{M}_{k,0}(N,\chi;\mathbb{C}))$, are of finite dimension. Since $\mathcal{H}_k(N,\chi;\mathbb{C})$ is a subspace of $\operatorname{End}_{\mathbb{C}}(\mathcal{M}_{k,0}(N,\chi;\mathbb{C}))$ we know that $\mathcal{H}_k(N,\chi;\mathbb{C})$ is also of finite dimension. Therefore, it suffices to prove the non-degeneracy of the pairing. If $\langle H, f\rangle = 0$ for each $H \in \mathcal{H}_k(N,\chi;A)$ then, in particular, $0 = a_1(T_n f) = a_n(f)$ for all $n \geq 0$; thus f must be constant. Since $k > 0$ it then follows that f must be 0. Now, if $\langle H, f\rangle = 0$ for each $f \in \mathcal{M}_{k,0}(N,\chi;A)$ then

$$a_n(Hf) = \langle T_n, Hf\rangle = a_1(HT_nf) = \langle H, T_nf\rangle = 0$$

using the fact that Hecke operators commute. Thus, $Hf = 0$ for each f and so we have that $H = 0$. Thus, if $A = \mathbb{C}$, the pairing is non-degenerate, as desired.

One should note that the above is true for any field A as long as $\mathcal{H}_k$ and $\mathcal{M}_{k,0}$ are finite dimensional over A. From [Hid93, Thm. 5.2.1] this is the case for $A = \mathbb{Q}$ with $\mathcal{M}_{k,0}(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Q})$, so we want to show that the theorem holds for $A = \mathbb{Z}$ with $\mathcal{M}_{k,0}(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z})$.

Since $A = \mathbb{Z}$ is a principal ideal domain, it then suffices to prove one of the following:

$$\operatorname{Hom}_A(\mathcal{H}_k(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z}),\mathbb{Z}) \cong \mathcal{M}_{k,0}(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z})$$

or

$$\operatorname{Hom}_A(\mathcal{M}_{k,0}(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z}),\mathbb{Z}) \cong \mathcal{H}_k(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z}).$$

We will show the first isomorphism. As shown above, if $\langle H, f\rangle = 0$ for each H, then $f = 0$ which tells us that the natural map from $\mathcal{M}_{k,0}(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z})$ into $\operatorname{Hom}_A(\mathcal{H}_k(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z}),\mathbb{Z})$ is injective.

Now, if $\phi : \mathcal{H}_k(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z}) \to \mathbb{Z}$ is a linear form we can extend it to a linear form $\mathcal{H}_k(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Q}) \to \mathbb{Q}$ by linearity. Then, we can find a $f \in \mathcal{M}_{k,0}(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Q})$ such that $\langle H, f\rangle = \phi(H)$ for each H. Thus, $a_n(f) = \langle T_n, f\rangle = \phi(T_n) \in \mathbb{Z}$ and so $f \in \mathcal{M}_{k,0}(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z})$; thus proving surjectivity.

Returning to the case of general A we see then see that

$$\begin{aligned}\mathrm{Hom}_A(\mathcal{H}_k(\mathrm{SL}_2(\mathbb{Z}),\chi;A),A) &\cong \mathrm{Hom}_{\mathbb{Z}}(\mathcal{H}_k(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z}),\mathbb{Z})\otimes A\\ &\cong \mathcal{M}_{k,0}(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z})\otimes A\\ &\cong \mathcal{M}_{k,0}(\mathrm{SL}_2(\mathbb{Z}),\chi;A)\end{aligned}$$

and

$$\begin{aligned}\mathrm{Hom}_A(\mathcal{M}_{k,0}(\mathrm{SL}_2(\mathbb{Z}),\chi;A),A) &\cong \mathrm{Hom}_{\mathbb{Z}}(\mathcal{M}_{k,0}(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z}),\mathbb{Z})\otimes A\\ &\cong \mathcal{H}_k(\mathrm{SL}_2(\mathbb{Z}),\chi;\mathbb{Z})\otimes A\\ &\cong \mathcal{H}_k(\mathrm{SL}_2(\mathbb{Z}),\chi;A);\end{aligned}$$

thus completing the first case.

Now we move on to the general case where $N = qp^r$ for some $r \geq 0$. Again, by Theorem 2.7.3, we can find a basis, say $\{f_i\}_{i=1}^r$ of $\mathcal{M}_k(qp^r,\chi)$ in $\mathcal{M}_k(qp^r,\chi;\mathbb{Z}[\chi])$. If ψ is a character modulo qp^r with $\psi(-1) = -1$, then taking $a = 2$ in Theorem 2.7.3 we find $\{f_i'\}_{i=1}^n$ among $T_{n_i}(G_1(\psi^{-1})E_{k-1}(\psi\chi)), G_k(\chi)$ and $E_k(\chi)$ which forms a basis of $\mathcal{M}_k(pq^r,\chi;K)$ where $K = \mathbb{Q}(\chi,\psi)$. After choosing suitable $a_i \in K$ we can show that $f_i = \mathrm{Tr}(a_i f_i') = \sum_\sigma \sigma(a_1)\sigma(f_i)$, where σ runs through all elements of $\mathrm{Gal}(K/\mathbb{Q}(\chi))$, forms a basis with coefficients in $\mathbb{Z}[\chi]$.

By the construction of the f_i we can find $n_1,\dots,n_r$ such that $\det((a_{n_i}(f_j))_{i,j=1}^r) \neq 0$. Then, for any $\phi \in \mathcal{M}_k(qp^r,\chi;\mathbb{Q}[\chi])$, we can simultaneously solve the system $\sum_j x_j a_{n_i}(f_j) = a_{n_i}(\phi)$ in $\mathbb{Q}(\chi)$. Doing so shows that ϕ is a linear combination of the f_i's with coefficients in $\mathbb{Q}(\chi)$. Thus, $\dim_{\mathbb{Q}(\chi)} M_k(qp^r,\chi;\mathbb{Q}[\chi]) \leq \dim_{\mathbb{C}}(\mathcal{M}_k(qp^r,\chi))$. Hence, $\mathcal{M}_k(qp^r,\chi;\mathbb{Z}[\chi])\otimes\mathbb{C} = \mathcal{M}_k(qp^r,\chi)$ and $\mathcal{M}_k(qp^r,\chi;\mathbb{Z}[\chi])\otimes\mathbb{C} \cong \mathcal{M}_q(qp^r,\chi)$.

Thus, using the same methods as in the first case ($N = 1$ or $A = \mathbb{C}$) we can see that

$$\mathrm{Hom}_{\mathbb{Z}[\chi]}(\mathcal{M}_k(qp^r,\chi;\mathbb{Z}[\chi]),\mathbb{Z}[\chi]) \cong \mathcal{H}_k(qp^r,\chi;\mathbb{Z}[\chi]),$$

and

$$\mathrm{Hom}_{\mathbb{Z}[\chi]}(\mathcal{H}_k(qp^r,\chi;\mathbb{Z}[\chi])) \cong \mathcal{M}_k(qp^r,\chi;\mathbb{Z}[\chi]).$$

Finally, we want to show that $\mathcal{H}_k(qp^r,\chi;A) \cong \mathcal{H}_k(qp^r,\chi;\mathbb{Z}[\chi])\otimes_{\mathbb{Z}} A$. It should be clear that $\mathcal{H}_k(qp^r,\chi;A)$ is a surjective image of $\mathcal{H}_k(qp^r,\chi;\mathbb{Z}[\chi])\otimes_{\mathbb{Z}} A$, so now suppose that the image of H in $\mathcal{H}_k(qp^r,\chi;\mathbb{Z}[\chi])\otimes_{\mathbb{Z}} A$ vanishes in $\mathcal{H}_k(qp^r,\chi;A)$. Extending scalars to $\mathbb{C}$, it then also vanishes in $\mathcal{H}_k(qp^r,\chi;\mathbb{C})$. Since $\mathcal{M}_k(qp^r,\chi) = \mathcal{M}_k(qp^r,\chi;\mathbb{Z}[\chi])\otimes\mathbb{C}$, it then follows that $H = 0$; showing injectivity. Thus we have that

$$\begin{aligned}\mathcal{M}_{k,0}(qp^r,\chi;A) &\cong \mathcal{M}_k(qp^r,\chi;\mathbb{Z}[\chi])\otimes_{\mathbb{Z}[\chi]} A\\ &\cong \mathrm{Hom}_{\mathbb{Z}[\chi]}(H_k(qp^r,\chi;\mathbb{Z}[\chi]),\mathbb{Z}[\chi])\otimes_{\mathbb{Z}} A\\ &\cong \mathrm{Hom}_A(H_k(qp^r,\chi;A),A),\end{aligned}$$

as desired. The other isomorphisms follow in a similar manner.

□

3. Ordinary Parts

One of the most important theorems of complex analysis is that every complex holomorphic function is also complex analytic. This is, however, not the case for real holomophic functions; in the real case holomophic functions are a subset of holomorphic functions. Since holomophic functions are "better behaved" than their analytic counterparts it makes sense to concentrate on the properties of just the holomorphic ones. Hida realized that something similar is true if we move away from an analytic setting and into an algebraic one. In the p-adic numbers so-called ordinary forms are better behaved than standard algebraic holomorphic forms. Thus we now develop the notion of an ordinary modular form which will be used extensively in the remaining sections.

We present here a general definition (as described in [Eme99]) of ordinary parts, then later introduce Hida's original definition as developed in [Hid81].

Let U be an indeterminate and let $\mathscr{C}$ denote the full subcategory of $\mathbb{Z}_p[U]$-modules which are finitely generated as $\mathbb{Z}_p$-modules. Finally, let $M \in \mathscr{C}$, then there exists a $\mathbb{Z}_p$-module morphism

$$\mathbb{Z}_p[U] \longrightarrow \mathrm{End}_{\mathbb{Z}_p}[M].$$

Since M is finitely generated as a $\mathbb{Z}_p$-module it follows that $\mathrm{End}_{\mathbb{Z}_p}(M)$ is a finite $\mathbb{Z}_p$-algebra, and thus the image of $\mathbb{Z}_p[U]$ in $\mathrm{End}_{\mathbb{Z}_p}(M)$ is also a finite $\mathbb{Z}_p$-algebra; let us denote it by A.

Now, any finite $\mathbb{Z}_p$-algebra factors as a product of local rings, and hence $A = \prod A_i$ where each A_i is local. One may project U onto these local factors of A; some of these projections will be contained in the maximal ideal, while others won't – and will hence be a unit. Let A^{ord} denote the product of local factors of A in which the image of U is a unit.

Definition 3.0.1. *The **ordinary part** of M is defined to be*

$$M^{\mathrm{ord}} = M \otimes_A A^{\mathrm{ord}}.$$

One may show that A^{ord} is a flat A-algebra and hence it will follow that taking ordinary parts is an exact functor.

For the most part we will be discussing the ordinary parts of $\mathcal{M}_k$ and $\mathcal{S}_k$, the spaces of weight k modular and cusp forms, respectively. In doing so we will take our indeterminate U to be the Hecke operator T_p.

Now we will present Hida's original construction (as in [Hid81] and later refined in [Hid93]) of the ordinary parts of $\mathcal{M}_k$ and $\mathcal{S}_k$.

Lemma 3.0.2. *Let K be a finite extension of $\mathbb{Q}_p$ with $\mathcal{O}_K$ its p-adic ring of integers. For any commutative $\mathcal{O}_K$-algebra A of finite rank over $\mathcal{O}_K$ and for any $x \in A$, the limit $\lim_{n\to\infty} x^{n!}$ exists in A and is an idempotent of A.*

Proof. See [Hid93, Lem. 7.2.1]. □

With this in hand, let K now be a finite extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}$ and let $\chi : (\mathbb{Z}/qp^r\mathbb{Z})^\times \to \mathcal{O}^\times$ be an arbitrary character with $r \geq 0$.

Definition 3.0.3. *The **ordinary projector**, e, of the Hecke algebra $\mathcal{H}_k(qp^r, \chi; \mathcal{O})$ is given by*

$$e = \lim_{n\to\infty} T_p^{n!}.$$

From Lemma 3.0.2 it follows that e exists in both $\mathcal{H}_k(qp^r, \chi; \mathcal{O})$ and $h_k(qp^r, \chi; \mathcal{O})$ and is an idempotent in each.

If $f \in \mathcal{M}_k(qp^r, \chi\,\mathcal{O})$ is an eigenform of T_p with eigenvalue c_p then

$$f|_e = \begin{cases} f & \text{if } |c_p|_p = 1, \\ 0 & \text{if } |c_p|_p < 1, \end{cases}$$

where $|\cdot|_p$ denotes the p-adic absolute value. One should further note that if f is a normalized eigenform then the eigenvalue will be $a_p(f)$, and hence the above becomes

$$f|_e = \begin{cases} f & \text{if } |a_p(f)|_p = 1, \\ 0 & \text{if } |a_p(f)|_p < 1. \end{cases}$$

Definition 3.0.4. *We say $f \in \mathcal{M}_k(qp^r, \chi; \mathcal{O})$ is **ordinary** if $f|_e = f$.*

It is clear that since e is an idempotent, $f|_e$ is ordinary for every $f \in \mathcal{M}_k(qp^r, \chi; \mathcal{O})$.

Definition 3.0.5. *For every $k \geq 0$ the spaces of weight k, level qp^r **ordinary modular forms** and **ordinary cusp forms** are given by*

$$\mathcal{M}_k^{\text{ord}}(qp^r, \chi; \mathcal{O}) = \mathcal{M}_k(qp^r, \chi; \mathcal{O})|_e = \{f|_e : f \in \mathcal{M}_k(qp^r, \chi; \mathcal{O})\},$$

and

$$\mathcal{S}_k^{\text{ord}}(qp^r, \chi; \mathcal{O}) = \mathcal{S}_k(qp^r, \chi; \mathcal{O})|_e = \{f|_e : f \in \mathcal{S}_k(qp^r, \chi; \mathcal{O})\},$$

respectively.

*Their corresponding **ordinary Hecke algebras** are then*

$$\mathcal{H}_k^{\text{ord}}(qp^r, \chi; \mathcal{O}) = e\mathcal{H}_k(qp^r, \chi; \mathcal{O}) = \{eH : H \in \mathcal{H}_k(qp^r, \chi; \mathcal{O})\},$$

and

$$h_k^{\text{ord}}(qp^r, \chi; \mathcal{O}) = eh_k(qp^r, \chi; \mathcal{O}) = \{eH : H \in h_k(qp^r, \chi; \mathcal{O})\},$$

respectively.

Now, similar to Proposition 2.8.3, we see that the duality between modular and cusp forms and their corresponding Hecke algebras still holds when we restrict to ordinary parts.

Proposition 3.0.6. *For every $k \geq 0$ we have*

$$\begin{aligned} \text{Hom}_{\mathcal{O}}(\mathcal{H}_k^{\text{ord}}(qp^r, \chi; \mathcal{O}), \mathcal{O}) &\cong \mathcal{M}_{k,0}^{\text{ord}}(qp^r, \chi; \mathcal{O}), \\ \text{Hom}_{\mathcal{O}}(h_k^{\text{ord}}(qp^r, \chi; \mathcal{O}), \mathcal{O}) &\cong \mathcal{S}_{k,0}^{\text{ord}}(qp^r, \chi; \mathcal{O}), \\ \text{Hom}_{\mathcal{O}}(\mathcal{M}_{k,0}^{\text{ord}}(qp^r, \chi; \mathcal{O}), \mathcal{O}) &\cong \mathcal{H}_k^{\text{ord}}(qp^r, \chi; \mathcal{O}), \\ \text{Hom}_{\mathcal{O}}(\mathcal{S}_k^{\text{ord}}(qp^r, \chi; \mathcal{O}), \mathcal{O}) &\cong h_k^{\text{ord}}(qp^r, \chi; \mathcal{O}). \end{aligned}$$

Proof. We will show only the $\mathcal{M}_{k,0}^{\text{ord}}(qp^r, \chi; \mathcal{O})$ case, since an identical argument will hold for $\mathcal{S}_k^{\text{ord}}(qp^r, \chi; \mathcal{O})$. Recall the pairing introduced in Theorem 2.8.3,

$$\begin{aligned} \mathcal{H}_k(qp^r, \chi; A) \times \mathcal{M}_{k,0}(qp^r, \chi; A) &\longrightarrow A \\ (H, f) &\longmapsto a_1(Hf). \end{aligned}$$

We see that for any $f \in \mathcal{M}_{k,0}(qp^r, \chi; A)$,

$$(H, ef) = a_1(Hef) = a_1(eHf) = (eH, f),$$

and thus the isomorphisms provided by Theorem 2.8.3 clearly restrict to ordinary parts; giving the desired isomorphisms.

□

We close this section by presenting one of the fundamental theorems in the theory of ordinary forms.

Theorem 3.0.7. *Suppose that $k \geq 2$, then we have*

$$\begin{aligned}\operatorname{rank}_{\mathcal{O}} \mathcal{H}_k^{\mathrm{ord}}(qp^r, \chi\omega^{-k}; \mathcal{O}) &= \operatorname{rank}_{\mathcal{O}} \mathcal{M}_k^{\mathrm{ord}}(qp^r, \chi\omega^{-k}; \mathcal{O}) \\ &= \operatorname{rank}_{\mathcal{O}} \mathcal{M}_2^{\mathrm{ord}}(qp^r, \chi\omega^{-2}; \mathcal{O}),\end{aligned}$$

and

$$\begin{aligned}\operatorname{rank}_{\mathcal{O}} h_k^{\mathrm{ord}}(qp^r, \chi\omega^{-k}; \mathcal{O}) &= \operatorname{rank}_{\mathcal{O}} \mathcal{S}_k^{\mathrm{ord}}(qp^r, \chi\omega^{-k}; \mathcal{O}) \\ &= \operatorname{rank}_{\mathcal{O}} \mathcal{S}_2^{\mathrm{ord}}(qp^r, \chi\omega^{-2}; \mathcal{O}),\end{aligned}$$

where ω denotes the Teichmüller character.

Proof. See [Hid93, Thm. 7.2.1]. □

4. Λ-adic Forms

With the basics of p-adic modular forms and their corresponding Hecke algebras now under our belt we move on to discuss certain families of p-adic modular forms, known as Λ-adic forms; which are the way much of the theory ordinary forms is proved. In fact, Λ-adic forms and their Galois representations play a fundamental role in Wiles' approach (in [Wil90]) to his proof of the Iwasawa main conjecture.

Much of the following is taken directly from [Hid93, Ch. 7] and [BCG08].

Let p be an odd prime and N an integer prime to p. Recalling now a bit of algebraic number theory, the units of $\mathbb{Z}_p$ may be decomposed as

$$\begin{gathered}\mathbb{Z}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times \times U_{(1)} \\ x = \omega(x) \times \langle x \rangle\end{gathered}$$

where ω is a Dirichlet character of conductor p and $U_{(1)}$ denotes the principal units of $\mathbb{Z}_p$, i.e., $U_{(1)} = 1 + p\mathbb{Z}_p$. We also let u be a topological generator of $U_{(1)}$.

For use throughout this section we would like to fix some characters:

- χ will denote a fixed Dirichlet character of level Np.
- χ_ζ is a Dirichlet character of conductor p^r associated to a p-power root of unity as follows: If ζ has exact order p^{r-1} with $r \geq 1$ define χ_ζ by mapping the image of $u \in U_{(1)}$ in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ to ζ.
- ν_p is the p-adic cyclotomic character defined by $\zeta^g = \zeta^{\nu_p(g)}$ for all $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and all p-power roots of unity ζ.

We will also let $\Lambda = \mathbb{Z}_p[[X]]$ be the power series ring over $\mathbb{Z}_p$ – this is the usual Iwasawa algebra. In addition, let K be a finite field extension of the quotient field of Λ, and let I denote the integral closure of Λ in K.

Lemma 4.0.1. *If $z \in U_{(1)}$, then $z = u^{s(z)}$ where $s(z) = \frac{\log(z)}{\log(u)} \in \mathbb{Z}_p$.*

Proof. Let $\exp_p$ denote the p-adic exponential map, $\exp_p(z) = \sum_{n=0}^\infty \frac{z^n}{n!}$, which converges on $|z|_p < p^{-1/p-1}$. Then

$$u^{s(z)} = \exp_p(s(z)\log(u)) = \exp_p\left(\frac{\log(z)}{\log(u)}\log(u)\right) = \exp_p(\log(z)) = z.$$

□

Proposition 4.0.2. *If $s \in \mathbb{Z}_p$ then $\binom{s}{m} \in \mathbb{Z}_p$ for any integer $m \geq 0$.*

Proof. It's not hard to check that if $P(s) \in \mathbb{Q}_p[s]$ is a polynomial in s, then $P(s)$ will be a continuous function from $\mathbb{Z}_p$ to $\mathbb{Q}_p$; so, in particular, the map $s \mapsto \binom{s}{m}$ is a continuous map from $\mathbb{Z}_p$ to $\mathbb{Q}_p$. Obviously, this map takes $\mathbb{N}$ to $\mathbb{N}$, and since $\mathbb{N}$ is dense in $\mathbb{Z}_p$, it induces a continuous map from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. Thus $\binom{s}{m} \in \mathbb{Z}_p$ if $s \in \mathbb{Z}_p$.

□

Corollary 4.0.3. *If $s \in \mathbb{Z}_p$, then $(1+X)^s \in \Lambda$.*

Proof. To show that $(1+X)^s \in \Lambda$ we simply need to show that the coefficients of the expansion

$$(1+X)^s = \sum_{m=0}^{s} \binom{s}{m} X^m$$

are elements of $\mathbb{Z}_p$, but this follows immediately from Proposition 4.0.2.

□

Now, defining one final character, let $\kappa : U_{(1)} \to \Lambda^\times$ be the character which maps u to $1+X$, i.e., for each $s \in \mathbb{Z}_p$

$$\kappa(u^s) = (1+X)^s = \sum_{m=0}^{s} \binom{s}{m} X^m \in \Lambda^\times.$$

One should note that the character κ may also be viewed as a Galois character via the natural map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = U_{(1)}$ where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We will see that κ plays a central role in the subject of Λ-adic forms, e.g., it plays the role of the Λ-adic analogue of the cyclotomic character ν_p.

We are now ready to give the main definition of this section.

Definition 4.0.4. *A **Λ-adic form** F of level N and character $\chi : (\mathbb{Z}/Np\mathbb{Z})^\times \to \mathbb{C}^\times$ is a formal q-expansion*

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

such that for all specializations $\nu : I \to \overline{\mathbb{Q}_p}$ extending the usual specializations

$$\nu_{k,\zeta} : \Lambda \to \overline{\mathbb{Q}_p}$$
$$x \mapsto \zeta u^k - 1$$

where $k > 1$ and $\zeta \in \mu_p^{r-1}$ with $r \geq 1$, the specialized q-expansion

$$f_\nu = \nu(F) = \sum_{n=0}^{\infty} \nu(a_n(F)) q^n \in \overline{\mathbb{Q}_p}[[q]]$$

is the image under a fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$ of the q-expansion in $\overline{\mathbb{Q}_p}[[q]]$ of a classical modular form of weight k, level Np^r and character $\chi_\nu = \chi\omega^{-k}\chi_\zeta$, i.e., it is an element of $\mathcal{M}_k(Np^r, \chi_\nu)$.

Thus, a Λ-adic form is a family of classical modular forms of varying weights and level divisible by Np, with identical residual q-expansions.

It may be beneficial for one to think of the specializations $\nu(F) = f_\nu$ as $F(\zeta u^k - 1)$ for some $k > 1$, so that $f_\nu = F(\zeta u^k - 1) \in \mathcal{M}_k(Np^r, \chi_\nu)$; both notations will now be used throughout.

One should note that while we have assumed p to be odd throughout this section, Λ-adic forms can still be defined for $p = 2$ with some slight modifications, which we omit here.

Additionally, some authors have chosen different normalizations in the specialized q-expansions in the definition of a Λ-adic form; however, it can be shown that all of these normalizations result in equivalent forms (see [BCG08] for detals).

Definition 4.0.5. *A Λ-adic form with q-expansion in $I[[q]]$ referred to as an **I-adic form**.*

We will write $\mathcal{M}(N, \chi, I)$ for the space of I-adic forms of tame level N and character χ. We also will let

$$\mathcal{M}(N, I) = \bigoplus_{\chi} \mathcal{M}(N, \chi, I)$$

denote the space of all I-adic forms.

Definition 4.0.6. *A Λ-adic form, F, is **cuspidal** if all the specializations f_ν are cusp forms.*

With this definition we have the following obvious decomposition,

$$\mathcal{S}(N, I) = \bigoplus_{\chi} \mathcal{S}(N, \chi, I)$$

of the space of I-adic cusp forms.

We would now like to introduce a Hecke operator on $\mathcal{M}(N, \Lambda)$ and $\mathcal{S}(N, \Lambda)$. First, recall that the character κ was defined so that

$$\kappa(u^s) = (1 + X)^s \in \Lambda^\times.$$

If we let $\langle n \rangle := \omega(n)^{-1} n = u^{s(n)}$ where, as in Lemma 4.0.1, $s(n) = \log(\langle n \rangle)/\log(u)$, then we have for all integers n prime to p,

$$\kappa(\langle n \rangle)(u^k - 1) = \kappa(u^{s(n)})(u^k - 1) = u^{ks(n)} = \omega(n)^{-k} n^k.$$

Then we define for each Λ-adic form $F \in \mathcal{M}(N, \Lambda)$ the coefficients of a formal q-expansion for $T_n F$ by

$$a_n(T_n F)(X) = \sum_{b|(m,n)} \kappa(\langle b \rangle)(X) \chi(b) b^{-1} a_{mn/b^2}(F)(X).$$

We may now evaluate the above equation at $u^k - 1$, and we see

$$\begin{aligned} a_n(T_n F)(u^k - 1) &= \sum_{b|(m,n)} \kappa(\langle b \rangle)(u^k - 1) \chi(b) b^{-1} a_{mn/b^2}(F(u^k - 1)) \\ &= \sum_{b|(m,n)} \chi\omega^{-k}(b) b^{k-1} a_{mn/b^2}(F(u^k - 1)) \\ &= a_m(T_n F(u^k - 1)), \end{aligned}$$

noting that $F(u^k-1)$ is a classical modular form. Hence we have $(T_nF)(u^k-1) = T_n(F(u^k-1))$; therefore, T_n is well defined, and so we have Hecke operators T_n acting on $\mathcal{M}(N,\Lambda)$ and $\mathcal{S}(N,\Lambda)$.

5. Λ-adic Eisenstein Series

Let $k > 2$ and $\chi : (\mathbb{Z}/Np^r\mathbb{Z})^\times \to \mathbb{C}^\times$ be a primitive character of level N extended trivially to Np^r, i.e., χ has trivial p-part. Recall in Section 2.4 we defined the Eisenstein series $E_{k,\chi}$ and saw that its q-expansion was given by

$$E_{k,\chi}(z) = \frac{L(1-k,\chi)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1,\chi}(n)q^n.$$

Since χ has level N we saw that $E_{k,\chi} \in \mathcal{M}_k(N,\chi)$, i.e., $E_{k,\chi}$ also has level N. As described in the previous section, Λ-adic forms are families of classical modular forms with weights divisible by Np. Clearly, N is not divisible by Np, so a Λ-adic form will not interpolate a standard Eisenstein series, but rather interpolate its so-called p-stabilization.

Definition 5.0.1. *The* ***p-stabilization*** *of an Eisenstein series $E_{k,\chi}$ is given by*

$$E^{(p)}_{k,\chi}(z) = E_{k,\chi}(z) - \chi(p)p^{k-1}E_{k,\chi}(pz),$$

which has q-expansion

$$E^{(p)}_{k,\chi}(z) = \frac{L^{(p)}(1-k,\chi)}{2} + \sum_{n=1}^{\infty} \sigma^{(p)}_{k-1,\chi}(n)q^n,$$

where

$$\sigma^{(p)}_{k-1,\chi}(n) = \sum_{\substack{d|n \\ (d,p)=1}} \chi(d)d^{k-1}$$

and

$$L^{(p)}(s,\chi) = (1-\chi(p)p^{-s})L(s,\chi),$$

and is of level divisible by Np.

5.1. Kubota-Leopoldt p-adic L-functions.

Recall in Section 2.4 we briefly discussed the Dirichlet L-function

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

We now would like to introduce analogous functions whose domain and range lie in the p-adics; known as p-adic L-functions.

There are two main constructions for p-adic L-functions, the first coming from Kubota and Leopoldt in 1964 ([KL64]) via the p-adic interpolation of special values of Dirichlet L-functions. These p-adic L-functions are typically referred to as *analytic p-adic L-functions*. The second construction is due to Iwasawa in 1972 ([Iwa72]) which stems from the arithmetic of cyclotomic fields, and are hence referred to as *arithmetic p-adic L-functions*. The Iwasawa main conjecture, proved by Mazur and Wiles, states that the analytic and arithmetic L-functions are essentially the same.

Our focus will be only on the analytic L-functions of Kubota and Leopoldt, which we now define.

Definition 5.1.1. *The **Kubota-Leopoldt p-adic L-function** $L_p(s,\chi)$ attached to χ is a continuous function for $s \in \mathbb{Z}_p \backslash \{1\}$ (and still continuous for $s = 1$ if χ is nontrivial) which satisfies*

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

for $k \geq 1$.

Recall from Section 4 that $U_{(1)} = 1 + p\mathbb{Z}_p$ denotes the principal units of $\mathbb{Z}_p$, and $u = 1 + p$ is a topological generator of $U_{(1)}$. We say that χ is of type $U_{(1)}$ if χ factors through $U_{(1)}$ with the assumption that the trivial character is of type $U_{(1)}$. Set

$$H_\chi(X) = \begin{cases} \chi(u)(1-X) - 1 & \text{if } \chi \text{ is of type } U_{(1)} \\ 1 & \text{otherwise.} \end{cases}$$

Iwasawa showed that there exists a unique power series $G_\chi(X) \in I = \mathbb{Z}_p[\chi][[X]]$ such that

$$L_p(1-s,\chi) = \frac{G_\chi(u^s - 1)}{H_\chi(u^s - 1)}. \tag{5.1}$$

Moreover, if ρ is a character of type $U_{(1)}$, then

$$G_{\chi\rho}(X) = G_\chi(\rho(u)(1+X) - 1). \tag{5.2}$$

5.2. **Λ-adic Eisenstein Series.** Now we may describe (as detailed in [BCG08, Sec. 4.3]) a Λ-adic form which interpolates the p-stabilization of the Eisenstein series. Fix an even character χ of conductor Np. For each $k > 1$ and $\zeta \in \mu_{p^{r-1}}$ with $r \geq 1$ we let $\psi = \chi_\nu = \chi\omega^{-k}\chi_\zeta$ be the character of level Np^r. Then the p-stabilized Eisenstein series $E_{k,\psi}^{(p)}$ is a modular form in $\mathcal{M}_k(Np^r, \chi)$.

Proposition 5.2.1. *Set $I = \mathcal{O}[[X]]$ with $\mathcal{O} = \mathbb{Z}_p[\chi]$. If $\chi \neq 1$, then there is a Λ-adic form*

$$\mathcal{E}_\chi = \sum_{n=0}^{\infty} A_{n,\chi}(X)q^n \in I[[q]]$$

which specializes to $E_{k,\psi}^{(p)}$, with $\psi = \chi\omega^{-k}\chi_\zeta$, under the homomorphism of I to $\overline{\mathbb{Q}_p}$ induced by $\nu_{k,\zeta}$ for $k > 1$ and $\zeta \in \mu_{p^{r-1}}$ for $r \geq 1$.

If $\chi = 1$ then $\mathcal{E}_\chi$ still exists, but is, strictly speaking, not a Λ-adic form since its constant term will have denominator X.

Proof. First, we want to interpolate the non-constant terms of $\mathcal{E}_\chi$, i.e., $A_{n,\chi}(X)$ for $n > 0$. From Corollary 4.0.3 we know that if $s \in \mathbb{Z}_p$ then

$$(1+X)^s = \sum_{m=0}^{\infty} \binom{s}{m} X^m \in \Lambda^\times.$$

By Lemma 4.0.1, if $d \in \mathbb{Z}$ with $d \equiv 1 \pmod{p}$ then $d = u^{s(d)} \in \mathbb{Z}_p$. Thus, if we set

$$A_d(X) = \frac{1}{d}(1+X)^{s(d)} \in \Lambda$$

then

$$A_d(u^k - 1) = \frac{u^{s(d)k}}{d} = d^{k-1}.$$

Recall, at the start of Section 4 saw that any $x \in \mathbb{Z}_p^\times$ can be written as $x = \omega(x) \cdot \langle x \rangle$. So now, given d with $(d,p) = 1$, we know that $\langle d \rangle \in U_{(1)}$ and hence we define

$$A_d(X) = \frac{1}{d}(1+X)^{s(\langle d \rangle)}. \tag{5.3}$$

We then see that

$$A_d(\zeta u^k - 1) = \frac{\zeta^{s(\langle d \rangle)} u^{ks(\langle d \rangle)}}{d} = \frac{\chi_\zeta(\langle d \rangle)\langle d \rangle^k}{d} = \omega^{-k}(d)\chi_\zeta(d)d^{k-1},$$

recalling that χ_ζ was defined at the start of Section 4.

Now, we introduce the character χ of level Nq into our coefficient. For $n \geq 1$ we set

$$A_{n,\chi}(X) = \sum_{\substack{d|n \\ (d,p)=1}} \chi(d) A_d(X).$$

With this, we then have

$$A_{n,\chi}(\zeta u^k - 1) = \sum_{\substack{d|n \\ (d,p)=1}} \psi(d) d^{k-1} = \sigma_{k-1,\psi}^{(p)}(n),$$

where $\psi = \chi\omega^{-k}\chi_\zeta$. Hence, with $A_{n,\chi}(X)$ defined in this way we have successfully interpolated the non-constant terms of $E_{k,\chi}^{(p)}$.

Next, we need to interpolate the constant terms, $A_{0,\chi}$; i.e., we need to find $A_{0,\chi}(X) \in I$ such that

$$A_{0,\chi}(\zeta u^k - 1) = \frac{L^{(p)}(1-k,\psi)}{2}.$$

Here we will use the Kubota-Leopoldt p-adic L-function described in Section 5.1. Define

$$A_{0,\chi}(X) = \frac{G_\chi(X)}{2H_\chi(X)}.$$

If either the N-part or p-part of χ is nontrivial, then χ will not be of type $U_{(1)}$, and so if χ is nontrivial we know $H_\chi(X) = 1$. Again, we always assume that trivial characters are of type $U_{(1)}$, so in this case $H_\chi(X) = X$. Thus, $A_{0,\chi}(X) \in I$ if $\chi \neq 1$, and $XA_{0,\chi}(X) \in I$ if $\chi = 1$.

Hence we now have that

$$\begin{aligned} A_{0,\chi}(\zeta u^k - 1) &= \frac{G_\chi(\zeta u^k - 1)}{2H_\chi(\zeta u^k - 1)} \\ &= \frac{G_{\chi\chi_\zeta}(u^k - 1)}{2H_{\chi\chi_\zeta}(u^k - 1)} \quad \text{by (5.2)} \\ &= \frac{L_p(1-k,\chi\chi_\zeta)}{2} \quad \text{by (5.1)} \\ &= \frac{(1-(\chi\omega^{-k}\chi_\zeta)(p)p^{k-1})L(1-k,\chi\omega^{-k}\chi_\zeta)}{2} \\ &= \frac{L^{(p)}(1-k,\psi)}{2}; \end{aligned} \tag{5.4}$$

interpolating the constant terms.

Thus, define

$$\mathcal{E}_\chi = \sum_{n=0}^{\infty} A_{n,\chi}(X) q^n$$

with $A_{n,\chi}(X)$ as above and we have $\mathcal{E}_\chi \in I[[q]]$ if $\chi \neq 1$, $X\mathcal{E}_\chi \in I[[q]]$ if $\chi = 1$, and $\mathcal{E}_\chi$ interpolates the terms of the p-stabilized Eisenstein series, as desired.

□

6. Ordinary Λ-adic Forms

Using the methods presented in Section 3 we may define the spaces of ordinary Λ-adic modular forms and ordinary Λ-adic cusp forms,

$$\mathcal{M}^{\mathrm{ord}}(N, I) \quad \text{and} \quad \mathcal{S}^{\mathrm{ord}}(N, I),$$

each of which have a decomposition

$$\mathcal{M}^{\mathrm{ord}}(N, I) = \bigoplus_{\chi} \mathcal{M}^{\mathrm{ord}}(N, \chi, I) \quad \text{and} \quad \mathcal{S}^{\mathrm{ord}}(N, I) = \bigoplus_{\chi} \mathcal{S}^{\mathrm{ord}}(N, \chi, I).$$

We now have a few definitions.

Definition 6.0.1. *A Λ-adic form is a* ***newform*** *if each specialization f_ν is N-new.*

Definition 6.0.2. *A Λ-adic form F is an* ***eigenform*** *if it is an eigenfunction of the Hecke operators. Equivalently, F is an eigenform if each specialization f_ν is an eigenform for the Hecke operators.*

Definition 6.0.3. *A Λ-adic form is* ***primitive*** *if it is an eigenform, a newform, and normalized such that $a_1(F) = 1$.*

Definition 6.0.4. *A Λ-adic form F is* ***ordinary*** *if each specialization f_ν is ordinary, i.e., if $a_p(f_\nu)$ is a p-adic unit for each ν.*

Finally, before discussing the properties of ordinary Λ-adic forms we state a theorem with summarizes the main results of Hida theory.

Theorem 6.0.5 (Hida,Wiles)**.** *Let p be an odd prime.*

(1) *There are finitely many primitive, ordinary Λ-adic forms F of tame level N.*
(2) *Each classical, p-stabilized, primitive, ordinary form is a member of some primitive ordinary Λ-adic form F.*
(3) *The form F from (2) is unique up to Galois conjugacy.*
(4) *Given a normalized, ordinary, Λ-adic eigenform F, one may associate a Galois representation ρ_F to it, with several natural properties.*

The natural properties of ρ_F mentioned in (4) will be described in further detail in Section 7. One should note that parts (2) and (3) follow from what is usually referred to as Hida's Control Theorem.

Next, we present a property of ordinary Λ-adic forms which does not hold for their classical counterparts. We begin with a lemma which will aid in the proof of Theorem 6.0.7

Lemma 6.0.6 (Weierstrass Preparation Theorem)**.** *Any power series $F(X)$ in Λ can be decomposed into a product of a unit power series $U(X)$, some power of a prime element in $\mathcal{O}$, and a distinguished polynomial $P(X) \in \mathcal{O}X$, where a polynomial $P(X) = a_0 + a_1X + \cdots + X^n$ is called* distinguished *if $|a_i|_p < 1$ for each i.*

Proof. This proof can be found in any commutative ring theory or p-adic number theory text, e.g., [Was80, Thm. 7.3]. □

For notation we let $\mathcal{M}^{\mathrm{ord}} = \mathcal{M}^{\mathrm{ord}}(\chi, \Lambda)$ denote the Λ-module of all Λ-adic modular forms, and denote the Λ-module of all Λ-adic cusp forms similarly as $\mathcal{S}^{\mathrm{ord}}$.

Theorem 6.0.7 (Wiles)**.** *The space of ordinary Λ-adic modular forms (resp. ordinary Λ-adic cusp forms) of character χ is free of finite rank over Λ; i.e., $\mathcal{M}^{\mathrm{ord}}(N, \chi, I)$ and $\mathcal{S}^{\mathrm{ord}}(N, \chi, I)$ are free of finite rank over Λ.*

Proof. The proof will be the same for $\mathcal{M}^{\mathrm{ord}}$ and $\mathcal{S}^{\mathrm{ord}}$, so we only present the $\mathcal{M}^{\mathrm{ord}}$ case. First, we will show that $\mathcal{M}^{\mathrm{ord}}$ is finitely generated and Λ-torsion free.

Since, by definition, $\mathcal{M}^{\mathrm{ord}}$ is a Λ-submodule of $\Lambda[[q]]$ it is Λ-torsion free. Now, we want to show that the rank of any finitely generated free Λ-submodule M of $\mathcal{M}^{\mathrm{ord}}$ is bounded. To this end, let $\{F_1, F_2, \ldots, F_r\}$ be a basis of M over Λ; which exists by Theorem 2.7.3. Since the F_i are linearly independent over Λ there exist $n_i \in \mathbb{N}$ such that $D(x) = \det((a_{n_i}(F_j))_{i,j}) \neq 0 \in \Lambda$. By the Weierstrass Preparation Theorem (6.0.6) we can choose the weight k so that $D(u^k - 1) \neq 0$ and $F_i(u^k - 1) \in \mathcal{M}_k^{\mathrm{ord}}(qp^r, \chi\omega^{-k}; \mathcal{O})$ for each i.

Write $f_i = F_i(u^k-1)$, then $D(u^k-1) = \det((a_{n_i}(f_j))_{i,j}) \neq 0$ and so the f_i span a free module of rank r in $\mathcal{M}_k^{\mathrm{ord}}(qp^r, \chi\omega^{-k}; \mathcal{O})$ whose rank is bounded independently of the weight k. Hence, r is bounded by a positive number independent of M. Therefore, if $F_1, \ldots, F_r$ is a maximal set of linearly independent elements in $\mathcal{M}^{\mathrm{ord}}$ any element in $\mathcal{M}^{\mathrm{ord}}$ can be expressed as a linear combination of the F_i's if we allow coefficients in the quotient field I of Λ, e.g., if $F \in \mathcal{M}^{\mathrm{ord}}$, then $F, F_1, \ldots, F_r$ are linearly dependent and so

$$a_0F + a_1F_1 + \cdots a_rF_r = 0$$

for some $a_i \in \Lambda$ and thus it follows

$$F = \frac{a_1}{a_0}F_1 + \cdots \frac{a_r}{a_0}F_r,$$

where $\frac{a_i}{a_0} \in I$. We thus consider $V = \mathcal{M}^{\mathrm{ord}} \otimes_\Lambda L$, which is a finite dimensional space over L embedded in $L[[q]]$.

For each $F \in \mathcal{M}^{\mathrm{ord}}$ write $F = \sum x_iF_i$ with $x_i \in L$, then x_i is the solution of $a_{n_i}(F_j)x = a_{n_i}F \in \Lambda^r$. Thus, $Dx_i \subset \Lambda$ and so $D\mathcal{M}^{\mathrm{ord}} \subset \Lambda F_1 + \cdots + \Lambda F_r$. Since Λ is Noetherian and $D\mathcal{M}^{\mathrm{ord}}$ is a submodule of a finitely generated Λ-module we have that $D\mathcal{M}^{\mathrm{ord}}$ is finitely generated. Now, since $\mathcal{M}^{\mathrm{ord}}$ is Λ-torsion free, the map $\mathcal{M}^{\mathrm{ord}} \to D\mathcal{M}^{\mathrm{ord}}$ is an isomorphism and therefore $\mathcal{M}^{\mathrm{ord}}$ is finitely generated.

Next, we want to prove that $\mathcal{M}^{\mathrm{ord}}$ is free over Λ, so first note that Λ is both a unique factorization domain and a compact ring (see [Hid93, Thm. 7.3.1] and [Lan02, Thm. 9.4]). Since $\mathcal{M}^{\mathrm{ord}}$ is finitely generated we can find k such that $F(u^k - 1)$ is meaningful, i.e., is an element of $\mathcal{M}_k^{\mathrm{ord}}(qp^r, \chi\omega^{-k}; \mathcal{O})$, for all F in $\mathcal{M}^{\mathrm{ord}}$. If $F(u^k - 1) = 0$ then $a_n(F)(u^k - 1)$ is divisible by $P = P_k = X - (u^k - 1)$

for all n. Hence, $(F/P_k)(u^j-1)=F(u^j-1)/(u^j-u^k)\in\mathcal{M}_k^{\mathrm{ord}}(qp^r,\chi\omega^{-k};\mathcal{O})$ for all $j\neq k$. So, $F/P_k\in\mathcal{M}^{\mathrm{ord}}$ and thus,

$$P\mathcal{M}^{\mathrm{ord}}=\{F\in\mathcal{M}^{\mathrm{ord}}:F(u^k-1)=0\}.$$

Therefore, $\mathcal{M}^{\mathrm{ord}}/PM^{\mathrm{ord}}$ embeds into $\mathcal{M}_k^{\mathrm{ord}}(qp^r,\chi\omega^{-k};\mathcal{O})$. With $\mathcal{O}$ being a principle ideal domain and $\mathcal{M}_k^{\mathrm{ord}}(qp^r,\chi\omega^{-k};\mathcal{O})$ a free $\mathcal{O}$-module, we know that each $\mathcal{O}$-submodule of $\mathcal{M}_k^{\mathrm{ord}}(qp^r,\chi\omega^{-k};\mathcal{O})$ is free and, in particular, $M^{\mathrm{ord}}/P\mathcal{M}^{\mathrm{ord}}$ is $\mathcal{O}$-free of finite rank.

Now, take $F_i\in\mathcal{M}^{\mathrm{ord}}$ for $i=1,\ldots,r$ such that $\{F_i \pmod{P\mathcal{M}^{\mathrm{ord}}}\}_i$ forms an $\mathcal{O}$-basis of $\mathcal{M}^{\mathrm{ord}}/P\mathcal{M}^{\mathrm{ord}}$. If $\lambda_1F_1+\cdots+\lambda_rF_r=0$ for some $\lambda_i\in\Lambda$ with at least one λ_i not divisible by P then, reducing modulo P, there would be a nontrivial linear relation between the F_i modulo P, which is impossible. Thus, there can be no such equation, so that F_i must be linearly independent over Λ.

Let $M=\Lambda F_1+\cdots\Lambda F_r$, then M is Λ-free of rank r, and M/PM coincides with $\mathcal{M}^{\mathrm{ord}}/P\mathcal{M}^{\mathrm{ord}}$; e.g., if $F\in\mathcal{M}^{\mathrm{ord}}$ there exists a finite linear combination G_0 of the F_i's such that $F-G_0$ is divisible by P. Repeating this with $F-G_0/P$ there exists a linear combination G_1 of the F_i's such that $F-G_0/P-G_1$ is divisible by P. Continuing this process, we can find G_j's which are linear combinations of the F_i's such that $F\equiv G_0+G_1P_1+\cdots+G_{i-1}P^{i-1} \pmod{P^i}$.

Let $G_i=\alpha_{1,i}F_1+\cdots+\alpha_{r,i}F_r$ for some $\alpha_{j,i}\in\Lambda$. Since Λ is a compact ring we know that

$$\alpha_n=\lim_{i\to\infty}\sum_{k=0}^{i}\alpha_{n,k}P^k\in\varprojlim_k\Lambda/P^k\Lambda=\Lambda$$

for all $1\le n\le r$. Thus, $G=\alpha_1F_1+\cdots+\alpha_rF_r\in M$. Further, $F-G\in\mathcal{M}^{\mathrm{ord}}$ is divisible by P^i for each i, and so $G=F$. Hence, it follows that $M=\mathcal{M}^{\mathrm{ord}}$, and since M is Λ-free, so is $\mathcal{M}^{\mathrm{ord}}$.

□

From the above we have that for sufficiently large k, if $P=X-(u^k-1)$ then $\mathcal{M}^{\mathrm{ord}}/P\mathcal{M}^{\mathrm{ord}}$ is naturally embedded into $\mathcal{M}_k^{\mathrm{ord}}(qp^r,\chi\omega^{-k};\mathcal{O})$, and in particular,

$$\mathrm{rank}_\Lambda(\mathcal{M}^{\mathrm{ord}})\le\mathrm{rank}_{\mathcal{O}}(\mathcal{M}_k^{\mathrm{ord}}(qp^r,\chi\omega^{-k};\mathcal{O})).$$

Corollary 6.0.8. *$\mathcal{M}^{\mathrm{ord}}(N,I)$ is finitely generated as an I-module.*

6.1. **The Universal Ordinary Hecke Algebra.** In this section we introduce the Hecke algebra which acts on the space of ordinary Λ-adic forms.

Definition 6.1.1. *The **universal ordinary Hecke algebra**, $\mathcal{H}^{\mathrm{ord}}(N;\Lambda)$ (resp. $h^{\mathrm{ord}}(N;\Lambda)$) is the subalgebra of $\mathrm{End}_\Lambda(\mathcal{M}^{\mathrm{ord}}(N,\Lambda))$ (resp. $\mathrm{End}_\Lambda(\mathcal{S}^{\mathrm{ord}}(N,\Lambda))$) generated by all of the Hecke operators T_n over Λ.*

For any Λ-algebra A we can further define

$$\begin{aligned}\mathcal{H}^{\mathrm{ord}}(N;A)&=\mathcal{H}^{\mathrm{ord}}(N;\Lambda)\otimes_\Lambda A,\\ h^{\mathrm{ord}}(N;A)&=h^{\mathrm{ord}}(N;\Lambda)\otimes_\Lambda A,\\ \mathcal{M}^{\mathrm{ord}}(N,A)&=\mathcal{M}^{\mathrm{ord}}(N,\Lambda)\otimes_\Lambda A,\\ \mathcal{S}^{\mathrm{ord}}(N,A)&=\mathcal{S}^{\mathrm{ord}}(N,\Lambda)\otimes_\Lambda A,\\ \mathcal{M}(N,A)&=\mathcal{M}(N,\Lambda)\otimes_\Lambda A,\\ \mathcal{S}(N,A)&=\mathcal{S}(N,\Lambda)\otimes_\Lambda A.\end{aligned}$$

Theorem 6.1.2. *$\mathcal{H}^{\mathrm{ord}}(N;\Lambda)$ (resp. $h^{\mathrm{ord}}(N;\Lambda)$) is reduced; i.e., $\mathcal{H}^{\mathrm{ord}}(N;L)$ (resp. $h^{\mathrm{ord}}(N;L)$) is semisimple, where L is the quotient field of Λ.*

Proof. Using Theorem 6.0.7 we may choose a basis $\{F_i\}_{i=1}^r$ of $\mathcal{M}^{\mathrm{ord}}$. Now we may identify $\mathrm{End}_\Lambda(\mathcal{M}^{\mathrm{ord}})$ with the matrix ring $M_r(\Lambda) \in \mathrm{Mat}_{r\times r}(\Lambda)$. For $k \geq 2$, $\mathrm{End}_\Lambda(\mathcal{M}^{\mathrm{ord}}) \otimes_\Lambda \Lambda/P_k\Lambda \cong \mathrm{End}_{\mathcal{O}}(\mathcal{M}^{\mathrm{ord}}/P_k\mathcal{M}^{\mathrm{ord}})$ where recall, as in the proof of Theorem 6.0.7, $P_k = X - (u^k - 1)$.

Suppose that $h \in \mathcal{H}^{\mathrm{ord}}(\chi;\Lambda)$ is nilpotent. Since

$$\mathcal{M}^{\mathrm{ord}}/P_k\mathcal{M}^{\mathrm{ord}} \otimes_{\mathcal{O}} K \cong \mathcal{M}_k^{\mathrm{ord}}(qp^r, \chi\omega^{-k}; K),$$

where $K = \mathbb{Q}(\chi,\psi)$ with ψ defined as in 2.7.3, it follows that the image of h in $\mathrm{End}_{\mathcal{O}}(\mathcal{M}^{\mathrm{ord}}/P_k\mathcal{M}^{\mathrm{ord}})$ gives an element of $\mathcal{H}_k^{\mathrm{ord}}(qp^r, \chi\omega^{-k}; \mathcal{O})$. Now, as seen in [Hid93, Cor. 2.1, Thm. 5.3.2], $\mathcal{H}_k^{\mathrm{ord}}(qp^r, \chi\omega^{-k}; \mathcal{O})$ has no nontrivial nilpotent elements, and this the image of h must be trivial. Hence, h is divisible by P_k. Since $h \in \bigcap_{k\geq 2} P_k M_r(\Lambda) = \{0\}$ the desired result then follows.

□

Similar to Theorem 2.8.3, we now define the pairing

$$\langle\cdot,\cdot\rangle : \mathcal{H}^{\mathrm{ord}}(N;A) \times \mathcal{M}^{\mathrm{ord}}(N,A) \to A$$
$$\langle H, F\rangle = a_1(HF) \in A$$

and we also define, as in Definition 2.8.2, the space

$$m^{\mathrm{ord}}(N,A) = \{f \in \mathcal{M}^{\mathrm{ord}}(N,K) : a_n(F) \in A \text{ for } n > 0\},$$

where K is the quotient field of A. With this, we have the following dualities.

Theorem 6.1.3. *For any extension A of Λ, the above pairing induces the isomorphisms*

$$\mathrm{Hom}_A(\mathcal{H}^{\mathrm{ord}}(N;A), A) \cong m^{\mathrm{ord}}(N,A),$$
$$\mathrm{Hom}_A(m^{\mathrm{ord}}(N,A), A) \cong \mathcal{H}^{\mathrm{ord}}(N;A),$$
$$\mathrm{Hom}_A(h^{\mathrm{ord}}(N;A), A) \cong \mathcal{S}^{\mathrm{ord}}(N,A),$$
$$\mathrm{Hom}_A(\mathcal{S}^{\mathrm{ord}}(N,A), A) \cong h^{\mathrm{ord}}(N;A).$$

In particular, $\mathcal{H}^{\mathrm{ord}}(N;A)$ and $h^{\mathrm{ord}}(N;A)$ are free of finite rank over A.

Proof. See [Hid93, Thm. 7.3.5] □

7. Ordinary Λ-adic Galois Representations

Recall that in Theorem 6.0.5 it was stated that one may associate a Galois representation having natural properties to normalized, ordinary, Λ-adic eigenforms. In this section we seek to construct this representation and describe its properties. Much of the following is taken from the exposition found in [BCG08].

We begin by stating the theorem that summarizes the natural properties of the associated Galois representation and we will use most of the remainder of the section developing the tools needed to give its proof.

Theorem 7.0.1 (Hida,Wiles)**.** *Let F be a normalized, i.e. $a_1(F) = 1$, I-adic eigenform of level N in $\mathcal{S}^{\mathrm{ord}}(N, \chi, I)$, and let λ denote the corresponding I-algebra homomorphism $\lambda : h^{\mathrm{ord}}(N, \chi, I) \to I$. Then there exists a unique Galois representation $\rho_F : \mathrm{G}_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K)$ such that*

(1) *ρ_F is continuous and absolutely irreducible,*
(2) *ρ_F is unramified outside Np,*
(3) *for each prime $q \nmid Np$, we have*

$$\det(1 - \rho_F(\mathrm{Frob}_q)T) = 1 - \lambda(T_q)T + (\chi\kappa\nu_p^{-1})(q)T^2,$$

where Frob_q is the Frobenius element at q.

For reference, recall that κ and $\langle n \rangle$ were defined in Section 4.

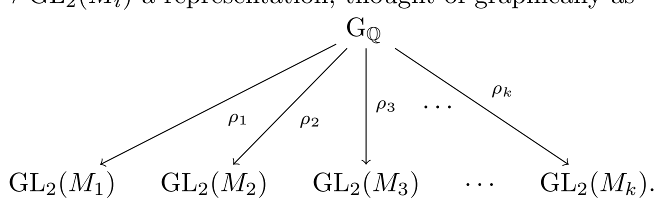
While it won't be used directly, we would like to comment on what it means for a Λ-adic Galois representation to be continuous.

Definition 7.0.2. *A Galois representation $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(K)$ is said to be continuous if there is an I-submodule $\mathcal{L}$ of K^2 (called a lattice) such that $\mathcal{L}$ is of finite type over I, $\mathcal{L} \otimes_I K = K^2$, $\mathcal{L}$ is stable under ρ, and as a map $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}_I(\mathcal{L})$, ρ is continuous, where $\mathrm{Aut}_I(\mathcal{L})$ is equipped with the projective limit topology*

$$\mathrm{Aut}_I(\mathcal{L}) = \varprojlim_n \mathrm{Aut}_I(\mathcal{L}/\mathfrak{m}^i\mathcal{L})$$

for the unique maximal ideal $\mathfrak{m}$ of I.

Theorem 7.0.1 will be proved over the next several sections but, as motivation, let us briefly describe the strategy for the proof. Let M_i be a finite extension of $\mathbb{Q}_p$ and $\rho_i : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(M_i)$ a representation, thought of graphically as



We then wish to patch these representations together to form a Λ-adic representation $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(K)$ such that the 'reductions' of ρ at certain prime ideals provide an isomorphism to ρ_i. However, it is generally hard to patch together representations, so Wiles (in [Wil88]) introduced the notion of a pseudo-representation for which the patching is much simpler to perform.

As stated in Theorem 7.0.1, the representation ρ_F is absolutely irreducible. However (in [Wil88]), Wiles was able to show that the local representation obtained by restricting ρ_F to a decomposition group D_p at the prime p is reducible.

Theorem 7.0.3 (Wiles)**.** *With the same notation as above, the restriction of ρ_F to D_p is given, up to equivalence, by*

$$\rho_F|_{D_p} \sim \begin{pmatrix} \epsilon_1 & * \\ 0 & \epsilon_2 \end{pmatrix}$$

where ϵ_2 is unramified and $\epsilon_2(\mathrm{Frob}_p) = \lambda(T_p)$.

Before constructing our representation ρ_F let us briefly explain what we mean by the reduction of ρ_F modulo P. For any prime ideal P of I, let $Q(I/P)$ denote the field of fractions of I/P.

Definition 7.0.4. *A Galois representation $\rho_F(P)$ into $\mathrm{GL}_2(Q(I/P))$ is called a **residual representation** of ρ_F at P if $\rho_F(P)$ is continuous under the $\mathfrak{m}$-adic topology of $Q(I/P)$, it is semi-simple, and it satisfies the following properties:*

1. *$\rho_F(P)$ is unramified outside Np,*
2. *For any prime $q \nmid Np$,*

$$\det(1 - \rho_F(P)(\mathrm{Frob}_q)T) = 1 - \lambda(T_q)(P)T + ((\chi\kappa\nu_p^{-1})(q))(P)T^2.$$

A priori, it's not clear that such a residual representation does indeed exist; however, its existence is guaranteed by the following theorem.

Theorem 7.0.5. *For every prime ideal P of height 1, the residual representation $\rho_F(P)$ of ρ_F exists and it is unique up to an isomorphism over $Q(I/P)$.*

Proof. (Sketch) Let $\mathcal{L}$ be a lattice such that the image of ρ_F is a subset of $\mathrm{Aut}_I(\mathcal{L})$. We know that I is a noetherian integrally closed domain of dimension 2. Let P denote a prime ideal of height 1, and let I_P denote the localization of I at P. It is easy to see that I_P is a discrete valuation ring, and since I_P is then a principal ideal domain we have that $\mathcal{L}_P = \mathcal{L} \otimes_I I_P$ becomes a free module of rank 2 over I_P.

Now, identify $\mathcal{L}_P$ with I_p^2 so we that can view the representation ρ_F as $\rho_F : \mathrm{G}_\mathbb{Q} \to \mathrm{GL}_2(I_P)$. Reducing ρ_F modulo P, and noting that $I_P/PI_P = Q(I/P)$ we have

$$\rho_P : \mathrm{G}_\mathbb{Q} \to \mathrm{GL}_2(Q(I/P)).$$

Let $\rho_F(P) = \rho_P^{\mathrm{ss}}$, the semi-simplification of ρ_P, then it can be checked that this $\rho_F(P)$ is the desired residual representation of ρ_F at P.

□

Lemma 7.0.6. *Let G be a group, K be a field of characteristic 0 and let ρ_1 and ρ_2 be two finite dimensional linear representations of G over K. If ρ_1 and ρ_2 are semi-simple and $\mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(\rho_2(g))$ for all $g \in G$, then ρ_1 and ρ_2 are isomorphic over K.*

We now define a family of height one prime ideals of I were we will be constructing our residual representations $\rho_F(P)$.

Definition 7.0.7. *The set of **arithmetic primes** is given by*

$$\Xi(I) = \{P : P = \ker(\nu_{k,\zeta} : \Lambda \to \overline{\mathbb{Q}}_p) \textit{ for some } k > 1 \textit{ and } \zeta \in \mu_{p^{r-1}} \textit{ with } r \geq 1\}.$$

If P is an arithmetic prime, then $F(P)$ is, by definition, a classical cuspidal eigenform of weight at least 2, and Deligne then showed that there is a classical Galois representation $\rho_{F(P)}$ attached to $F(P)$.

Let f be a normalized eigenform in $S_k(\Gamma_0(Np^r), \psi; K_f)$ where, recall, K_f denotes the number field generated by $\{a_n(f)\}_{n=1}^\infty$. Let λ_f denote the corresponding algebra homomorphism $h_k(\Gamma_0(Np^r), \psi; K_f) \to K_f$, then we have the following theorem due to Eichler-Shimura for $k = 2$ (see [Eic54],[Shi71]), Deligne for $k \geq 2$ (see [Del68]) and finally Deligne-Serre for $k = 1$ (see [DeSe74]).

Theorem 7.0.8. *For each maximal ideal $\wp$ of $\mathcal{O}_{K_f}$ lying over P, there exists a unique 2-dimensional Galois representation $\rho_{f,\wp} : \mathrm{G}_\mathbb{Q} \to \mathrm{GL}_2(K_{f,\wp})$ such that*

(1) *$\rho_{f,\wp}$ is continuous and absolutely irreducible,*
(2) *$\rho_{f,\wp}$ is unramified outside Np,*
(3) *for each prime $q \nmid Np$, we have*

$$\det(1 - \rho_{f,\wp}(\mathrm{Frob}_q)T) = 1 - \lambda_f(T_q)T + \psi(q)q^{k-1}T^2.$$

Let P be an arithmetic prime, $f = f_\nu = F(P)$ and let $\wp$ be the prime of K_f induced by the fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. It will follow from our work below that $K_{f,\wp} \subseteq Q(I/P)$ and hence $\mathcal{O}_{K_{f,\wp}} \subseteq \widetilde{I/P}$, where $\widetilde{I/P}$ is the integral closure of I/P in $Q(I/P)$. With this we can state a refined version of the previous theorem for $f = F(P)$:

Corollary 7.0.9. *There exists a unique, odd, Galois representation $\rho_{F(P)} : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(Q(I/P))$, and hence into $\mathrm{GL}_2(\widetilde{I/P})$, with the same properties as in Theorem 7.0.8.*

We can now show that the residual representation $\rho_F(P)$ attached to ρ_F is the same as Deligne's representation, $\rho_{F(P)}$, described above, as Galois representations into $\mathrm{GL}_2(Q(I/P))$.

Lemma 7.0.6 and the fact that the Frobenius elements outside Np are dense in $\mathrm{G}_{\mathbb{Q}}$ allow us to only show that the characteristic polynomials of the Frobenius elements outside Np coincide for our two residual representations. Recall the trace polynomials from Definition 7.0.4 and Theorem 7.0.8 are given by

$$\det(1 - \rho_F(P)(\mathrm{Frob}_q)T) = 1 - \lambda(T_q)(P)T + ((\chi\kappa\nu_p^{-1})(q))(P)T^2,$$

and

$$\det(1 - \rho_{f,\wp}(\mathrm{Frob}_q)T) = 1 - \lambda_f(T_q)T + \psi(q)q^{k-1}T^2,$$

respectively.

Now,

$$\begin{aligned} \kappa(\langle n\rangle)(\zeta u^k - 1) = \kappa(u^{s(\langle n\rangle)})(\zeta u^k - 1) = (\zeta u^k)^{s(\langle n\rangle)} &= \zeta^{s(\langle n\rangle)}(u^{s(\langle n\rangle)})^k \\ &= \zeta^{s(\langle n\rangle)}\omega^{-k}n^k \\ &= \chi_\zeta(\langle n\rangle)\omega^{-k}n^k \\ &= \chi_\zeta(n)\omega^{-k}n^k. \end{aligned}$$

Hence, if $P|_\Lambda = \ker(\nu_{k,\zeta})$, then

$$\lambda(T_q)(P) = a_q(F)(P) = a_q(F(P)) = a_q(f_\nu) = \lambda_{f_\nu}(T_q) = \lambda_f(T_q), \tag{7.1}$$

and

$$((\chi\kappa\nu_p^{-1})(q))(P) = (\chi\omega^{-1}\chi_\zeta)(q)q^{k-1} = \chi_\nu(q)q^{k-1}, \tag{7.2}$$

as desired.

7.1. **Pseudo-Representations.** As eluded to above, it is difficult to patch together Galois representations, so to remedy this Wiles developed the notion of a pseudo-representation. Let B be a commutative topological ring with unity and assume that 2 is invertible in B. Further, if B is an integral domain, let $Q(B)$ denote the field of fractions of B.

Definition 7.1.1. *Let G be a profinite group with an identity e, and a special element c of order 2. A pseudo-representation $\pi : G \to B$ is a triple $\pi = \{A, D, X\}$ of continuous maps*

$A : G \to B$
$D : G \to B$, and,
$X : G \times G \to B$,

satisfying the following axioms:

(1) $A(\sigma\tau) = A(\sigma)A(\tau) + X(\sigma,\tau)$,
(2) $D(\sigma\tau) = D(\sigma)D(\tau) + X(\tau,\sigma)$,
(3) $X(\sigma\tau,\gamma) = A(\sigma)X(\tau,\gamma) + D(\tau)X(\sigma,\gamma)$,
(4) $X(\sigma,\tau\gamma) = A(\gamma)X(\sigma,\tau) + D(\tau)X(\sigma,\gamma)$,
(5) $A(e) = D(e) = A(c) = 1, D(c) = -1$,
(6) $X(\sigma,e) = X(e,\sigma) = X(\sigma,c) = X(c,\sigma) = 0$,
(7) $X(\sigma,\tau)X(\gamma,\eta) = X(\sigma,\eta)X(\gamma,\tau)$.

When we need to specify π we denote A, D, X by A_π, D_π, X_π.

Note that (1) above shows that X is determined by A, so we could leave the X requirement out of the definition of a pseudo-representation; however, it will be important whether or not $X(\sigma,\tau) = 0$ so we leave it in for convenience.

Clearly, every odd 2-dimensional representation $\rho : G \to \mathrm{GL}_2(B)$ with $\rho(c) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ induces a pseudo-representation in the following manner. Let

$$\rho(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix},$$

then define $\pi = (A, D, X)$ by

$$A(\sigma) = a(\sigma),\ D(\sigma) = d(\sigma),\ X(\sigma,\tau) = b(\sigma)c(\tau),$$

and it is easily checked that π is a pseudo-representation from G to B.

Also, if $\pi : G \to B$ is defined as above, then we say that π is the *pseudo-representation associated to* ρ, or that π *comes from* ρ.

Definition 7.1.2. *The **trace** and **determinant** of a pseudo-representation π are defined to be*

- $\mathrm{Tr}(\pi)(\sigma) := A(\sigma) + D(\sigma)$,
- $\mathrm{Det}(\pi)(\sigma) := A(\sigma)D(\sigma) - X(\sigma,\sigma)$.

With these definitions we have the following two identities which will be used in the forthcoming proofs:

$$A(\sigma) = \frac{\mathrm{Tr}(\pi)(\sigma) + \mathrm{Tr}(\pi)(c\sigma)}{2},$$

and

$$D(\sigma) = \frac{\mathrm{Tr}(\pi)(\sigma) - \mathrm{Tr}(\pi)(c\sigma)}{2}.$$

We have seen that representations induce pseudo-representations, however, given a pseudo-representation it would be nice to know whether it came from a representation or not. The following theorem gives us a criteria for determining exactly this.

Theorem 7.1.3. *Let π be a pseudo-representation from G to B such that either X is identically zero or $X(h_1,h_2) \in B^\times$ for some $h_1, h_2 \in G$. Then π comes from a 2-dimensional odd representation $\rho : G \to \mathrm{GL}_2(B)$.*

Proof. First, suppose that X is identically zero. Then we can define for every $g \in G$,

$$\rho(g) = \begin{pmatrix} A_\pi(g) & 0 \\ 0 & D_\pi(g) \end{pmatrix}.$$

Since $X \equiv 0$, ρ is clearly a representation from $G \to \mathrm{GL}_2(B)$.

Alternatively, if there exist $h_1, h_2 \in G$ such that $X(h_1, h_2) \in B^\times$ then we define for each $g \in G$

$$\rho(g) = \begin{pmatrix} A(g) & X(g, h_2)/X(h_1, h_2) \\ X(h_1, g) & D(g) \end{pmatrix}.$$

Using the defining properties of a pseudo-representation it is then easy to check that ρ is a representation.

$\square$

Corollary 7.1.4. *If B is a field, then the pseudo-representation π always comes from a 2-dimensional, odd, representation.*

Let us now return our focus to the situation where $G = \mathrm{G}_{\mathbb{Q}}$ and I is a finite extension of Λ. Our goal is to patch together pseudo-representations to obtain the desired representation which has the proper reductions. So we begin with a lemma on how to patch two pseudo-representations and then expand upon that.

Lemma 7.1.5. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of I. Let $\pi(\mathfrak{a})$ and $\pi(\mathfrak{b})$ be pseudo-representations of G into $I/\mathfrak{a}$ and $I/\mathfrak{b}$. Suppose that they are compatible, i.e., there exists two functions T and D on a dense subset Σ of G, with values in I, such that*

$$\mathrm{Tr}(\pi(\mathfrak{a}))(\sigma) \equiv T(\sigma) \ (mod\ \mathfrak{a}) \quad \text{and} \quad \mathrm{Tr}(\pi(\mathfrak{b}))(\sigma) \equiv T(\sigma) \ (mod\ \mathfrak{b}),$$

and

$$\mathrm{Det}(\pi(\mathfrak{a}))(\sigma) \equiv D(\sigma) \ (mod\ \mathfrak{a}) \quad \text{and} \quad \mathrm{Det}(\pi(\mathfrak{b}))(\sigma) \equiv D(\sigma) \ (mod\ \mathfrak{b}),$$

for any $\sigma \in \Sigma$. Then, there exists a pseudo-representation $\pi(\mathfrak{a} \cap \mathfrak{b})$ of G into $I/(\mathfrak{a} \cap \mathfrak{b})$, such that

$$\mathrm{Tr}(\pi(\mathfrak{a} \cap \mathfrak{b}))(\sigma) \equiv T(\sigma) \ (mod\ \mathfrak{a} \cap \mathfrak{b}) \quad \text{and} \quad \mathrm{Det}(\pi(\mathfrak{a} \cap \mathfrak{b}))(\sigma) \equiv D(\sigma) \ (mod\ \mathfrak{a} \cap \mathfrak{b}),$$

on Σ.

Proof. (Sketch.) We have the following short exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I/(\mathfrak{a} \cap \mathfrak{b}) & \longrightarrow & I/\mathfrak{a} \oplus I/\mathfrak{b} & \longrightarrow & I/(\mathfrak{a} + \mathfrak{b}) & \longrightarrow & 0 \\ & & \overline{a} & \longmapsto & (\overline{a}, \overline{a}) & & & & \\ & & & & (\overline{a}, \overline{b}) & \longmapsto & a - b(\mathfrak{a} + \mathfrak{b}). & & \end{array}$$

Consider the map $\pi = \pi(\mathfrak{a}) \oplus \pi(\mathfrak{b}) : G \to I/\mathfrak{a} \oplus I/\mathfrak{b}$. Since $\pi(\mathfrak{a})$ and $\pi(\mathfrak{b})$ are pseudo-representations, it's not hard to check that π is also a pseudo-representation into $I/\mathfrak{a} \oplus I/\mathfrak{b}$.

By Lemma 6.22, $\mathrm{Tr}(\pi)$ (mod $\mathfrak{a} + \mathfrak{b}$) vanishes identically on Σ and hence

$$\mathrm{Tr}(\pi)(\sigma) \equiv T(\sigma) \ (\mathrm{mod}\ \mathfrak{a} \cap \mathfrak{b}) \quad \text{for all } \sigma \in \Sigma.$$

Thus, π is a candidate for our $\pi(\mathfrak{a} \cap \mathfrak{b})$, but we need to show that π takes values in $I/\mathfrak{a} \cap \mathfrak{b}$ first.

Since $\mathrm{Tr}(\pi)$ is continuous and Σ is dense in G it follows that $\mathrm{Tr}(\pi)$ (mod $\mathfrak{a} + \mathfrak{b}$) vanishes on G, and hence $\mathrm{Tr}(\pi)$ has values in $I/\mathfrak{a} \cap \mathfrak{b}$. By our trace formulas for $A(\sigma)$ and $D(\sigma)$ mentioned above it is clear that A_π, D_π, X_π take values in $I/\mathfrak{a} \cap \mathfrak{b}$, and so we call this π our desired $\pi(\mathfrak{a} \cap \mathfrak{b})$.

□

Now, using induction and a few results from commutative algebra one can generalize Lemma 7.1.5 for a countable collection of ideals.

Theorem 7.1.6. *Suppose $\{P_n\}_{n=1}^{\infty}$ is a sequence of height 1 prime ideals of I. For each $n \geq 1$, suppose $\pi(P_n)$ is a pseudo-representation of G into I/P_n. Suppose that the $\pi(P_n)$ are compatible on a dense subset Σ of G., i.e., there exist two functions T and D on Σ, with values in I, such that for any $n \geq 1$*

$$\mathrm{Tr}(\pi)(\sigma) \equiv T(\sigma) \ (mod\ \mathfrak{a}_n),$$
$$\mathrm{Det}(\pi)(\sigma) \equiv D(\sigma) \ (mod\ \mathfrak{a}_n),$$

and hence for every $\sigma \in \Sigma$,

$$\mathrm{Tr}(\pi)(\sigma) = T(\sigma), \ \mathrm{Det}(\pi)(\sigma) = D(\sigma).$$

Corollary 7.1.7. *Under the same assumptions as above, the pseudo-representation $\pi : G \to I$, thought of as taking values in K, can be lifted to a representation ρ, such that the trace of ρ is equal to the trace of π.*

Finally, given an F we can show the existence of the representation $\rho = \rho_F$. The strategy here is to specialize F at a countable subset of prime ideals P in $\Xi(I)$ for which there is an associated Galois representation by Corollary 7.0.9, and then to patch these representations using Theorem 7.1.6 and Corollary 7.1.7 to construct ρ.

Theorem 7.1.8 (Wiles)**.** *Suppose that $\{P_n\}_{n=1}^{\infty}$ is an infinite set of distinct prime ideals of I of height one. Let $\widetilde{I/P_n}$ denote the integral closure of I/P_n in $Q(I/P_n)$. Suppose that, for each n, we are given a continuous, odd representation*

$$\rho_n : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\widetilde{I/P_n}),$$

which is unramified outside Np. Suppose that for each prime $q \nmid Np$, there exists elements a_q and ϵ_q, in I, such that

$$\begin{aligned} \mathrm{Trace}\, \rho_n(\mathrm{Frob}_q) &= a_q \ (mod\ P_n), \quad and \\ \mathrm{Det}\ \rho_n(\mathrm{Frob}_q) &= \epsilon_q \ (mod\ P_n). \end{aligned}$$

Then there exists a continuous, odd, representation

$$\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(K),$$

with

$$\mathrm{Trace}\, \rho(\mathrm{Frob}_q) = a_q,$$
$$\mathrm{Det}\, \rho(\mathrm{Frob}_q) = \epsilon_q,$$

for $q \nmid Np$. Also, ρ is irreducible if ρ_n is irreducible for some n.

Proof. Let c denote complex conjugation with determinant -1 in all ρ_n's. Since $\widetilde{I/P_n}$ is a discrete valuation ring we can pick a basis of $\widetilde{I/P_n}^2$ such that $\rho_n(c) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Fix a representation ρ_n with the above property for each n.

Now, let

$$\rho_n(\sigma) = \begin{pmatrix} a_\sigma^{(n)} & b_\sigma^{(n)} \\ c_\sigma^{(n)} & d_\sigma^{(n)} \end{pmatrix}$$

for each $\sigma \in \mathrm{G}_{\mathbb{Q}}$ and let π_n be the pseudo-representation associated to ρ_n. We have now that ρ_n is a pseudo-representation from $G_{\mathbb{Q}}$ to $\widetilde{I/P_n}$; however, it can be checked that it is actually a pseudo-representation into I/P_n.

In general, if $\rho(c) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ then the pseudo-representation ρ depends only on Trace(ρ). Now, in our case, by assumption, $\mathrm{Trace}(\rho_n) \in I/P_n$, and thus we have a sequence of pseudo-representations from $\mathrm{G}_{\mathbb{Q}}$ into I/P_n. Take $\Sigma = \{\mathrm{Frob}_q : q \nmid Np\}$, then by the Chebotarev Density Theorem, Σ is dense in $\mathrm{G}_{\mathbb{Q}}$, so applying Theorem 7.1.6 we obtain a pseudo-representation π from $\mathrm{G}_{\mathbb{Q}}$ into I such that

$$\mathrm{Tr}(\pi)(\mathrm{Frob}_q) = a_q \quad \text{and} \quad \mathrm{Det}(\pi)(\mathrm{Frob}_q) = \epsilon_q$$

for all $q \nmid Np$. Thinking now of π as taking values in K, by Corollary 7.1.7 we can lift the pseudo-representation π to a representation ρ such that ρ and π have the same traces and determinants for each $q \nmid Np$, thus proving the theorem.

□

With the help of Theorem 7.1.8 we can now prove Theorem 7.0.1.

Proof of Theorem 7.0.1. Consider the set of prime ideals $\{P_n\}_{n=1}^{\infty}$ with each $P_i \in \Xi(I)$, and let ρ_n denote the representation associated to $F(P_n)$ as in Corollary 7.0.9. For every prime $q \nmid Np$ we take

$$a_q = \lambda(T_q) \in I \text{ and } \epsilon_q = \left(\chi\kappa\nu_p^{-1}\right)(q) \in I.$$

By the computations in (7.1) and (7.2), for every $q \nmid Np$, a_q and ϵ_q satisfy the conditions of Theorem 7.1.8. Hence, there exists a representation ρ, such that for each prime $q \nmid Np$

$$\det(1 - \rho(\mathrm{Frob}_q)T) = 1 - \lambda(T_q)T + \left(\chi\kappa\nu_p^{-1}\right)(q)T^2.$$

This ρ is our desired ρ_F.

□

References

[BCG08] D. Banerjee, V.G. Ch, and E. Ghate, Λ-*Adic Forms and the Iwasawa Main Conjecture.* Lecture Notes from: Advanced Instructional School on Arithmetic Geometry, September 22-30, 2008, IIT Guwahati.

[Coh07] H. Cohen, *Number Theory - Volume I: Tools and Diophantine Equations.* Graduate Texts in Mathematics **239**. Springer, first edition, 2007.

[Del68] P. Deligne, *Formes modulaires et représentations ℓ-adiques.* Sém. Bourbaki, 1968/69, no. 355.

[DeSe74] P. Deligne and J. -P. Serre, *Formes modulaires de poids 1.* Ann. Sci. Éc. Norm. Sup. **7**, 507-530, 1974.

[DiSh07] F. Diamond and J. Shurman, *A First Course in Modular Forms.* Graduate Texts in Mathematics **228**. Springer, first edition, 2007.

[Eic54] M. Eichler, *Quaternäre quadratische Formen und die Riemannsche Vermutung fü r die Knogruenzzetafunktion.* Archiv. der Math., **5**, 355-366, 1954.

[Eme99] M. Emerton, A New Proof of a Theorem of Hida. *Int. Math. Res. Not.*, 1999, No. 9, 453-472.

[Hid81] H. Hida, On Congruence Divisors of Cusp Forms as Factors of the Special Values of Their Zeta Functions. *Invent. Math.*, **64**, 1981, 221-262.

[Hid93] Haruzo Hida, *Elementary theory of L-functions and Eisenstein series.* London Mathematical Society Student Texts **26**. Cambridge University Press, second edition, 1993.

[Iwa72] K. Iwasawa. *Lectures on p-adic L-functions.* Annals of Mathematics Studies, **74**. Princeton University Press, 1972.

[Kat83] N.M. Katz, *p-adic Properties of Modular Schemes and Modular Forms.* In “Modular functions of one variable, III”, Lecture Notes in Mathematics 350, Springer-Verlag, 1983, pp. 69190, MR0447119.

[KL64] T. Kubota and H-W. Leopoldt, Eine p-adische Theorie der Zetawerte - Teil I: Einführung der p-adischen Dirichletschen L- Funktionen. *Reine Angew. Math.*, 214/215, 328-339, 1964.

[Lan02] S. Lang, *Algebra.* Graduate Texts in Mathematics **211**. Springer, third edition, 2002.

[Miy89] T. Miyake, *Modular Forms.* Springer, first edition, 1989.

[RS11] K. Ribet and W. Stein, *Lectures on Modular Forms and Hecke Operators.* `http://wstein.org/books/ribet-stein/main.pdf`, 2011.

[Ser73] J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques.* In “Modular functions of one variable, III”, Lecture Notes in Mathematics 350, Springer-Verlag, 1973, pp. 191268, MR0404145.

[Shi71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.* Princeton University Press, 1971.

[Was80] L. Washington, *Introduction to Cyclotomic Fields.* Graduate Texts in Mathematics **83**. Springer, 1980.

[Wil88] A. Wiles, On ordinary Λ-adic representations associated to modular forms. *Invent. Math.*, **94**, Issue 3, 1988, 529-573.

[Wil90] A. Wiles, The Iwasawa conjecture for totally real fields. *Ann. of Math.*, **131**, 1990, 493-540.

Department of Mathematics, The University of Arizona, Tucson, AZ 85743
E-mail address: `rwilliams@math.arizona.edu`