Λ-ADIC FORMS AND THE IWASAWA MAIN CONJECTURE

DEBARGHA BANERJEE, V.G. NARASIMHA KUMAR CH, AND EKNATH GHATE

Advanced Instructional School on Arithmetic Geometry
September 22-30, 2008, IIT Guwahati[1]

1. Introduction

The classical Iwasawa main conjecture identifies two seemingly rather different power series in one variable over a p-adic integer ring, up to multiplication by a unit power series. One is the characteristic power series of a Selmer group, the other is a p-adic L-function. The conjecture over $\mathbb{Q}$ was proved by Mazur and Wiles, and over totally real fields by Wiles in [Wil90].

The purpose of these notes is to provide some background on Λ-adic forms to the extent they are used in Wiles' approach in [Wil90] to the proof of the main conjecture, assuming that the totally real base field is $\mathbb{Q}$. We first describe some general results about Λ-adic forms and their Galois representations, and then give an exposition of some specific results about Λ-adic forms in Sections 3 and 4 of [Wil90].

We leave it to the other articles in this volume (especially [CS10]) to explain how the material in these notes is used in the proof of the main conjecture (over $\mathbb{Q}$). However, some brief remarks on how Λ-adic forms enter the proof might be in order. To prove the main conjecture, it suffices to show that the two power series mentioned above have the same zeros, with multiplicity. Iwasawa had already shown that the sum of the multiplicities of the zeros is the same. Thus it suffices to show that the multiplicity of a specific zero of one of the power series (in practice one takes the characteristic power series of the Selmer group) is greater than the corresponding multiplicity of the corresponding zero of the other (the p-adic L-function). This is done by Lambda-fying, so to speak, the classical argument of Ribet [Rib76] (see also [Dal10]), proving the converse of Herbrand's theorem, and goes roughly as follows. The p-adic L-function turns out to be the constant term of a Λ-adic Eisenstein series

[1]This is a compilation of lecture notes given by the three authors at IIT Guwahati.

(cf. Section 4). Thus, if a zero occurs in the p-adic L-function, then, going modulo the corresponding divisor, one expects a congruence between the Λ-adic Eisenstein series and a Λ-adic cuspidal eigenform F. The study of such congruences is made more precise by introducing the Λ-adic Eisenstein ideal (described in Section 8). One now uses the global Galois representation attached to the Λ-adic cusp form F, constructed in considerable detail in Section 6 (see especially Theorem 6.1), along with some important local properties of this representation (Theorem 6.2), to show that one can construct enough classes in the Selmer group so that a zero of greater multiplicity occurs in its characteristic power series. Thus, Λ-adic forms and their Galois representations are used in a rather fundamental way in Wiles' approach [Wil90] to the proof of the main conjecture.

The material in these notes is taken mostly from the papers of Hida and Wiles. For the background on Λ-adic forms and representations (described in Sections 2 through 6), we depend heavily on [Hid93, Chapter 7] and to some extent on [Wil88] and [Hid86]. The material in Sections 7 and 8 is taken almost verbatim from Sections 3 and 4 of [Wil90], though we provide detailed proofs of some of the results.

2. Some notation

We start by recalling some notation from Iwasawa theory. Let p be a prime and let $\mathbb{Z}_p$ denote the ring of integers of $\mathbb{Q}_p$. If $p = 2$, set $q = 4$, and if $p > 2$ set $q = p$. Let $W = 1 + q\mathbb{Z}_p$. Then the units of $\mathbb{Z}_p^\times$ decompose as:

$$\begin{aligned} \mathbb{Z}_p^\times &= (\mathbb{Z}/q)^\times \times W \\ x &= \omega(x) \times \langle x \rangle, \end{aligned}$$

where ω and $\langle\ \rangle$ are defined by the decomposition above.

Let u denote a topological generator of W. Let log be the usual p-adic logarithm from W to $q\mathbb{Z}_p$.

Lemma 2.1. *If $z \in W = 1 + q\mathbb{Z}_p$, then $z = u^{s(z)}$, where $s(z) = \frac{\log(z)}{\log(u)} \in \mathbb{Z}_p$.*

Proof. Let exp be the p-adic exponential map. Then

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

Here we are using the fact that exp induces an isomorphism between $q\mathbb{Z}_p$ and $1+q\mathbb{Z}_p$ with inverse log. □

Let N be an integer prime to p. It will denote tame level. We introduce three Dirichlet characters that occur throughout the exposition.

- χ will denote a fixed Dirichlet character of level Nq.
- ω above may be viewed as a Dirichlet character of conductor q. When p is odd, ω is just the mod p cyclotomic character. If $p = 2$, then ω is the non-trivial character of conductor 4.
- 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 $r \geq 1$ if p is odd, or exact order p^{r-2} with $r \geq 2$ if $p = 2$, define χ_ζ by mapping the image of $u \in W = 1 + q\mathbb{Z}_p$ in $(\mathbb{Z}/p^r)^\times$ to ζ.

Finally let ν_p denote the p-adic cyclotomic character, defined by $\zeta^g = \zeta^{\nu_p(g)}$, for all g in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and all p-power roots of unity ζ.

Let $\Lambda = \mathbb{Z}_p[[X]]$ be the power series ring in one variable X over $\mathbb{Z}_p$. This is the usual Iwasawa algebra. If $s \in \mathbb{Z}_p$, then the coefficients of the power series

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

belongs to $\mathbb{Z}_p$, i.e., $(1+X)^s \in \Lambda$. Indeed if $P(s) \in \mathbb{Q}_p[s]$ is a polynomial in s, then it is easy to check that $P(s)$ is a continuous function from $\mathbb{Z}_p$ to $\mathbb{Q}_p$. In particular, the map $s \mapsto \binom{s}{m}$ is a continuous function from $\mathbb{Z}_p$ to $\mathbb{Q}_p$. This map takes $\mathbb{N}$ to $\mathbb{N}$. But $\mathbb{N}$ is dense in $\mathbb{Z}_p$. So this map induces a continuous function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. In particular, $|\binom{s}{m}|_p \leq 1$ if $s \in \mathbb{Z}_p$.

Let $\kappa : W = 1 + q\mathbb{Z}_p \to \Lambda^\times$ be the character which maps u to $1 + X$, i.e., for each $s \in \mathbb{Z}_p$,

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

The character κ may also be viewed as a Galois character via the natural map $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = W$, where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. The character κ plays a central role in the subject. It is the universal deformation of the trivial mod p character; roughly it plays the role of the Λ-adic analogue of the cyclotomic character ν_p.

3. Λ-adic forms

Let p be an odd prime and let N be an integer prime to p. Let K be a finite field extension of the quotient field of Λ, and let I denote the integral closure of Λ in K. Observe that I is a complete local noetherian ring and is an integrally closed domain of Krull dimension 2. We remark that since I is a normal ring of dimension 2, it is Cohen-Macaulay [Mat86, Exer. 17.3], but unlike Λ, I is not necessarily regular.

Definition 3.1. A Λ-adic form F of level N and character $\chi : (\mathbb{Z}/Np)^\times \to \mathbb{C}^\times$ is a formal q-expansion

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

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

$$\begin{aligned} \nu_{k,\zeta} : \Lambda &\to \bar{\mathbb{Q}}_p \\ X &\mapsto \zeta u^k - 1, \end{aligned}$$

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

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

is the image under a fixed embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ of the q-expansion in $\bar{\mathbb{Q}}[[q]]$ of a classical modular form of

- weight k,
- level Np^r, and,
- character $\chi_\nu = \chi\omega^{-k}\chi_\zeta$.

Note that the character χ_ν has level Np^r with $r \geq 1$.

Thus a Λ-adic form is a family of classical forms of varying weights and level divisible by Np, with identical residual q-expansions. Explicit examples of Λ-adic forms are CM families (see, for instance, [Gha05, Sec. 5]) and Eisenstein families (described in Section 4).

Remark 3.2. Λ-adic forms may be defined for $p = 2$ as well. The definition is similar to the one given above for odd primes p, with some minor changes: one needs to replace p by $q = 4$ in the levels of χ and ω, and now $\zeta \in \mu_{p^{r-2}}$, $r \geq 2$, so that χ_ζ

has level divisible by q. In particular, χ_ν has level Np^r with $r \geq 2$. We will treat the case $p = 2$ in the next section, but will later avoid $p = 2$ in these notes. We also remark that the symbol 'q' has two meanings: it is an odd prime or 4, and also $e^{2\pi iz}$ in various q-expansions. Since both usages are standard, we let this be; in any case which meaning is implied should be clear from the context.

Remark 3.3. Wiles uses a slightly different normalization in his papers [Wil88], [Wil90] when he defines a Λ-adic form. His specialization map $\nu_{k,\zeta}$ maps X to $\zeta u^{k-2}-1$, rather than $\zeta u^k - 1$, and his f_ν is a weight k, level Np^r form, as above, but with character $\chi_\nu = \chi\omega^{2-k}\chi_\zeta$. Further, some authors (cf. Skinner's Hangzhou lectures notes [Ski04]) specialize X to $\zeta u^{k-1} - 1$ (with χ_ν now $\chi\omega^{1-k}\chi_\zeta$). We point out that all the above normalizations are in fact equivalent and one may go between them by a suitable automorphism of Λ. Indeed, we have the useful fact [Hid93, p. 199]:

Lemma 3.4. *The map induced by $X \mapsto aX + b$, where a, $b \in \mathbb{Z}_p$, and $|a|_p = 1$ and $|b|_p < 1$, is an automorphism of* Λ.

The different normalizations explain the occasional appearance of the terms u^2 (in Wiles' papers) or u (in Skinner's notes) in some of the formulas. As an aside, one may ask which normalization is best. It appears that the choice of $k - 2$ is historical and was used originally by Hida and then by Wiles, whereas the choice of k seems easiest for bookkeeping purposes, and is what we shall mainly try and use in these notes. However, we shall eventually switch to $k - 2$ when exposing Wiles' results on Λ-adic forms from [Wil90, Sec. 4] in Section 8, to avoid introducing errors when changing normalizations. We also remark that some formulas, such as those for the Eisenstein family in the next section, or for the determinants of Λ-adic Galois representations, seem to be the most natural when one uses $k-1$, but we will *not* use this normalization in these notes.

Remark 3.5. There is no condition on the weight 1 specializations in the definition of a Λ-adic form, and the study of such specializations is an interesting area of research (cf. [MW86], [GV04]).

A Λ-adic form with q-expansion in $I[[q]]$ is sometimes more precisely referred to as an I-adic form. We shall use both terminologies. Let us write $M(N, \chi, I)$ for the

I-module of I-adic forms of tame level N and character χ. Let

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

be the I-module of all I-adic forms (of some character χ).

Definition 3.6. A Λ-adic form F is cuspidal if all the specializations f_ν above are cusp forms.

We have the corresponding decomposition:

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

of the I-module of I-adic cusp forms.

4. Families of Eisenstein series

The aim of this section is to give an example of a Λ-adic form that is used extensively in Wiles' proof of the Iwasawa main conjecture. This form interpolates a family of Eisenstein series.

4.1. **Classical Eisenstein series.** Recall that if k is an even integer greater than or equal to 4, then the (normalized) Eisenstein series of weight k, level 1 and trivial character has q-expansion given by

$$E_k = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ is the usual arithmetic function, and $\zeta(s)$ is the Riemann zeta function.

Let p be a prime. Since the forms E_k are of level 1 they cannot lie in a p-adic family (as we have seen forms f_ν in a p-adic family have level at least p, not to mention the fact that the character χ_ν depends on k, and cannot be uniformly trivial). Also, the Eisenstein series E_k of weight 2 and level 1 is not even holomorphic. However, for all even $k \geq 2$, the p-stabilized form $E_k^{(p)} = E_k(z) - p^{k-1} E_k(pz)$ is holomorphic and is of level p.

More generally, for any $k \geq 1$ and character ψ mod Np^r, with ψ having the same parity as k, consider the Eisenstein series of weight k, level equal to $\mathrm{cond}(\psi)$, and

character ψ, given by:

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

where $\sigma_{k-1,\psi}(n) = \sum_{d|n} \psi(d) d^{k-1}$ and $L(s,\psi)$ is the Dirichlet L-series attached to ψ. Again, if ψ has level N (i.e., it has trivial p-part), then $E_{k,\psi}$ has level N, which is not divisible by Np. But, its p-stabilization, namely:

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

which has q-expansion:

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

where

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

and

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

is the Dirichlet L-series attached to ψ deprived of the Euler factor at p, has level divisible by Np. NB: $E_{k,\psi}^{(p)} = E_{k,\psi}$, if ψ already has conductor divisible by p. Given these remarks it seems that one should try and interpolate p-stabilized Eisenstein series. Before we do this we recall some classical facts about p-adic L-functions for $\mathrm{GL}_{1/\mathbb{Q}}$, which will be needed to interpolate the constant terms.

4.2. **Kubota-Leopoldt p-adic L-function.** Let χ be an arbitrary even Dirichlet character. The Kubota-Leopoldt p-adic L-function $L_p(s,\chi)$ attached to χ is a continuous function for $s \in \mathbb{Z}_p \setminus \{1\}$ (also continuous at $s = 1$, if χ is non-trivial), which satisfies the interpolation property

$$L_p(1-k,\chi) = (1 - \chi\omega^{-k}(p) p^{k-1}) L(1-k, \chi\omega^{-k}), \tag{4.1}$$

for $k \geq 1$. Say χ is of type W if χ factors through W (that is, as a Galois character, χ factors through the Galois group $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$). NB: the trivial character is of type W. Set

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

Iwasawa showed [Was96, Thm. 7.10] that there exists a unique power series $G_\chi(X) \in I_\chi := \mathbb{Z}_p[\chi][[X]]$ such that

$$L_p(1-s,\chi) = \frac{G_\chi(u^s-1)}{H_\chi(u^s-1)}. \tag{4.2}$$

Moreover, if ρ is a character of type W, then (cf. [Wil90, (1.4)]):

$$G_{\chi\rho}(X) = G(\rho(u)(1+X)-1). \tag{4.3}$$

This can be proved using [Was96, Thm. 7.10]; see also [Ven10, Prop. 2.1].

4.3. **Λ-adic Eisenstein series.** We are now ready to begin interpolating p-stabilized Eisenstein series. Recall that

- $q = p$ if p is odd, and,
- $q = 4$ if $p = 2$.

Fix an even character χ of conductor Nq. This will be the character of the Λ-adic form we construct (in the sense of Definition 3.1). For each $k > 1$ and

- $\zeta \in \mu_{p^{r-1}}$, with $r \geq 1$, if p is odd, and,
- $\zeta \in \mu_{p^{r-2}}$, with $r \geq 2$ if $p = 2$,

let $\psi = \chi_\nu = \chi\omega^{-k}\chi_\zeta$ be the character of level Np^r, which is the character of the form f_ν (see Definition 3.1). NB: Since χ is even, ψ has the same parity as k. Consider the corresponding Eisenstein series $E^{(p)}_{k,\psi}$ attached to $\psi = \chi\omega^{-k}\chi_\zeta$. This is a modular form in $M_k(Np^r, \psi)$.

Proposition 4.4. *Set $I_\chi = \mathcal{O}[[X]]$ with $\mathcal{O} = \mathbb{Z}_p[\chi]$. If $\chi \neq 1$, then there is a Λ-adic form*

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

which specializes to $E_{k,\psi}^{(p)}$*, with* $\psi = \chi\omega^{-k}\chi_\zeta$*, under the homomorphism of* I_χ *to* $\bar{\mathbb{Q}}_p$ *induced by* $\nu_{k,\zeta}$*, for* $k > 1$*,* ζ *as above. If* $\chi = 1$*, then* $\mathcal{E}_\chi$ *still exists, but it is strictly speaking not a* Λ*-adic form, since the constant term of* $\mathcal{E}_\chi$ *has denominator* X*.*

Proof. We first interpolate the non-constant terms. As remarked earlier, if $s \in \mathbb{Z}_p$, then

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

By Lemma 2.1, if d is an integer with $d \equiv 1 \mod q$, then $d = u^{s(d)}$ for $s(d) \in \mathbb{Z}_p$. Hence, if we set

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

then

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

This basic computation hints at what we should do for general d (coprime to p). Recall $\mathbb{Z}_p^\times = (\mathbb{Z}/q)^\times \times W$ with $x = \omega(x) \cdot \langle x \rangle$. Given d with $(d,p) = 1$, we have $\langle d \rangle \in W$. So define

$$A_d(X) = \frac{1}{d}(1+X)^{s(\langle d \rangle)}. \tag{4.5}$$

Then

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

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

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

Then

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

where $\psi = \chi\omega^{-k}\chi_\zeta$. Thus we have successfully interpolated the non-constant terms of $E_{k,\psi}^{(p)}$.

Now we need to interpolate the constant terms, that is, we need to find $A_{0,\chi}(X) \in I_\chi$ such that

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

But such a power series is furnished by the Kubota-Leopoldt p-adic L-function attached to χ. We define:

$$A_{0,\chi}(X) = \frac{1}{2}\frac{G_\chi(X)}{H_\chi(X)}.$$

Recall that in the present setting our χ has conductor Nq. If either the N-part or the p-part of χ is non-trivial, then χ is not of type W, and so if χ is non-trivial then $H_\chi(X) = 1$. If χ is trivial, then it is trivially of type W and $H_\chi(X) = X$. Thus $A_{0,\chi}(X) \in I_\chi$ if $\chi \neq 1$, and $XA_{0,\chi}(X) \in I_\chi$ if $\chi = 1$. Now:

$$\begin{aligned} A_{0,\chi}(\zeta u^k - 1) &= \frac{1}{2}\frac{G_\chi(\zeta u^k - 1)}{H_\chi(\zeta u^k - 1)} \\ &= \frac{1}{2}\frac{G_{\chi\chi_\zeta}(u^k - 1)}{H_{\chi\chi_\zeta}(u^k - 1)} \qquad \text{by (4.3)} \\ &= \frac{L_p(1-k, \chi\chi_\zeta)}{2} \qquad \text{by (4.2)} \\ &= \frac{(1 - (\chi\omega^{-k}\chi_\zeta)(p)p^{k-1}) \cdot L(1-k, \chi\omega^{-k}\chi_\zeta)}{2} \qquad \text{by (4.1)} \\ &= \frac{L^{(p)}(1-k, \psi)}{2}, \end{aligned} \tag{4.6}$$

as desired.

Thus, if we define $\mathcal{E}_\chi = \sum_{n=0}^\infty A_{n,\chi}(X)q^n$, then $\mathcal{E}_\chi \in I_\chi[[q]]$ if $\chi \neq 1$ (and $X\mathcal{E}_\chi \in I_\chi[[q]]$ if $\chi = 1$), and $\mathcal{E}_\chi$ has the desired interpolation property. □

4.4. **Cuspidal families.** In this section we construct a cuspidal Λ-adic form starting with a classical cusp form of weight 1, and the Λ-adic form $\mathcal{E}_\chi$ just constructed. The argument is somewhat artificial so we will be brief.

Let $f_1 \in S_1(Nq, \psi_1)$ be a fixed cusp form of weight 1. Recall

$$\mathcal{E}_\chi(\zeta u^{k-1} - 1) = E^{(p)}_{k-1,\psi} \in M_{k-1}(Np^r, \psi)$$

where $\psi = \chi\omega^{1-k}\chi_\zeta$. Thus the product $f_1 \cdot E^{(p)}_{k-1,\psi}$ is a cusp form:

$$f_1 \cdot E^{(p)}_{k-1,\psi} \in S_k(Np^r, \chi'\omega^{-k}\chi_\zeta),$$

with $\chi' := \psi_1\chi\omega$. We show $f_1 \cdot E^{(p)}_{k-1,\psi}$ are the specializations at $X = \zeta u^k - 1$ of a cuspidal Λ-adic form F of level N and character χ' for $k > 1$ and ζ as above.

Assume that the q-expansions of f_1 and ψ_1 are both $\mathbb{Z}_p[\chi]$-rational (otherwise extend scalars). Then we may formally multiply the q-expansions in $I_\chi = \mathbb{Z}_p[\chi][[X]]$ of f_1 and $\mathcal{E}_\chi$. Say the resulting q-expansion is $f_1 \cdot \mathcal{E}_\chi = \sum_{n=0}^{\infty} a_n(X)q^n$, for some $a_n(X) \in I_\chi$. Now define

$$F := \sum_{n=0}^{\infty} a_n(u^{-1}X + u^{-1} - 1)q^n,$$

noting that the substitution made above is an automorphism of I_χ (cf. Lemma 3.4). Then on substituting $X = \zeta u^k - 1$ we get

$$F(\zeta u^k - 1) = \sum_{n=0}^{\infty} a_n(\zeta u^{k-1} - 1)q^n = f_1 \cdot \mathcal{E}_\chi(\zeta u^{k-1} - 1) = f_1 \cdot E^{(p)}_{k-1,\chi\omega^{1-k}\chi_\zeta}.$$

So F is the desired cuspidal family.

4.5. **Wiles' normalizations.** As mentioned in Remark 3.3, Wiles' normalization involves substituting $X = \zeta u^{k-2} - 1$, rather than $X = \zeta u^k - 1$. This changes the definition of $\mathcal{E}_\chi$ slightly. Since we will also work with Wiles' $\mathcal{E}_\chi$ below let us point out the changes that need to be made in the old definition:

(1) The denominator of d in (4.5) gets shifted to the numerator (i.e., multiply the old $A_d(X)$ by d^2) so that now

$$A_d(X) = d(1 + X)^{s(\langle d \rangle)},$$

and $A_{n,\chi}(X)$ for $n \geq 1$ is now defined with this new $A_d(X)$. We remark here that with 'Skinner's normalization' $X = \zeta u^{k-1} - 1$ one could simply drop the d altogether from $A_d(X)$, and so this normalization gives the neatest formula!.

(2) Let

$$\begin{aligned} \hat{G}_\chi(X) &= G_{\chi\omega^2}(u^2(1 + X) - 1), \\ \hat{H}_\chi(X) &= H_{\chi\omega^2}(u^2(1 + X) - 1). \end{aligned}$$

Then the new constant term is defined as

$$A_{0,\chi}(X) = \frac{1}{2}\frac{\hat{G}_\chi(X)}{\hat{H}_\chi(X)}.$$

It is easily verified that the Wiles' Eisenstein family $\mathcal{E}_\chi = \sum_{n=0}^{\infty} A_{n,\chi}(X)q^n$ interpolates the p-stabilized Eisenstein series $E_{k,\psi}^{(p)}$ with $\psi = \chi\omega^{2-k}\chi_\zeta$ (note the $2-k$ instead of the $-k$) when one specializes at $X = \zeta u^{k-2} - 1$. This is more or less obvious for the non-constant terms; for the constant term we simply note:

$$\begin{aligned} A_{0,\chi}(\zeta u^{k-2} - 1) &= \frac{1}{2}\frac{\hat{G}_\chi(\zeta u^{k-2} - 1)}{\hat{H}_\chi(\zeta u^{k-2} - 1)} \\ &= \frac{1}{2}\frac{G_{\chi\omega^2}(\zeta u^k - 1)}{H_{\chi\omega^2}(\zeta u^k - 1)} \\ &= \frac{1}{2}\frac{G_{\chi\omega^2\chi_\zeta}(u^k - 1)}{H_{\chi\omega^2\chi_\zeta}(u^k - 1)} \qquad \text{by (4.3)} \\ &= \frac{L^{(p)}(1-k, \chi\omega^{2-k}\chi_\zeta)}{2} \qquad \text{as in (4.6).} \end{aligned}$$

5. Hida theory

In this section we mention some facts from Hida theory. From this point on, the prime p will be an odd prime. We start with some definitions.

Definition 5.1. A Λ-adic form is a newform if each f_v is N-new.

Note that we do not require f_v to be p-new; indeed the specializations f_ν may be p-old if $r = 1$.

The spaces $M(N, I)$ and $S(N, I)$ have a natural action of the Hecke operators T_q for $q \nmid Np$ and U_q for $q|Np$, given by the usual formulas. Sometimes we just write T_n for the n-th Hecke operator (including at the primes dividing Np). The Hecke action commutes with specialization.

Definition 5.2. 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 (in particular each f_ν is a U_p-eigenform).

We now define the Λ-adic Hecke algebra $h(N, \Lambda)$ to be the Λ-subalgebra of the Λ-algebra $\mathrm{End}_\Lambda(M(N, \Lambda))$ generated by all the Hecke operators above. We define $h(N, I)$ by $h(N, \Lambda) \otimes_\Lambda I$. There is a bijection between I-algebra homomorphisms of $h(N, I)$ with values in I, and I-adic cuspidal Hecke eigenforms normalized to have first Fourier coefficient 1, induced by the map $(\lambda : h(N, I) \to I) \mapsto (F = \sum_{n=1}^{\infty} \lambda(T_n)q^n)$.

Definition 5.3. A Λ-adic form is primitive if it is an eigenform, a newform, and normalized such that $a_1(F) = 1$.

The spaces $M(N, I)$ and $S(N, I)$ of I-adic forms are not in general finitely generated as I-modules, even if one restricts to the new part. Put another way, the number of primitive I-adic forms of tame level N is not necessarily finite. Hida realized that just as holomorphic forms are more manageable in the class of real-analytic forms, in the p-adic world, ordinary forms are better behaved in the class of algebraic holomorphic forms.

Definition 5.4. A Λ-adic form F is ordinary if f_v is ordinary (that is, $a_p(f_\nu)$ is a p-adic unit), for all ν as above.

Note the Eisenstein family $\mathcal{E}_\chi$ is ordinary, since $A_{p,\chi}(X) = 1$.

The sum of ordinary forms in the above sense (whether classical or Λ-adic) is not again necessarily ordinary in the above sense. To rectify this, Hida introduced a projector $e = \lim_{n\to\infty} U_p^{n!}$, and using e, defined the spaces of ordinary Λ-adic forms as follows:

$$\begin{aligned} M^{\mathrm{ord}}(N, I) &= eM(N, I), \\ S^{\mathrm{ord}}(N, I) &= eS(N, I). \end{aligned}$$

Since $e(F) = F$ if F is ordinary in the sense of the previous definition, the sum of ordinary forms is now ordinary in the more general sense above. One of the key reasons the ordinary part is important is because of the following theorem.

Theorem 5.5. *$M^{\mathrm{ord}}(N, I)$ is finitely generated as an I-module.*

Proof. We prove this when $I = \Lambda$ since the proof is easily modified for general I. Note that after specialization at $\nu = \nu_{k,1}$, Λ-adic forms in $M^{\mathrm{ord}}(N, \Lambda)$ wind up in the classical space $M_k^{\mathrm{ord}}(\Gamma_1(Np), \mathbb{Z}_p) = eM_k(\Gamma_1(Np), \mathbb{Z}_p)$. The proof now involves two parts. One first shows that the spaces $M_k^{\mathrm{ord}}(\Gamma_1(Np), \mathbb{Z}_p)$ have rank independent of k. One then shows that this forces $M^{\mathrm{ord}}(N, \Lambda)$ to be finitely generated as a Λ-module.

Let us deal with the first part first. By duality it suffices to show that the Hecke algebra acting on $M_k^{\mathrm{ord}}(\Gamma_1(Np), \mathbb{Z}_p)$ has rank independent of k. By the Eichler-Shimura isomorphism it further suffices to show that $\mathrm{H}^1(\Gamma_1(Np), L(n, \mathbb{Z}_p))$ has rank independent of n, where $n = k - 2$, and $L(n, A) = \mathrm{Sym}^n(A^2)^*$ is the space of homogeneous

polynomials in two variables with coefficients in A. But now a pretty cohomological argument (see [Hid93, p. 203]) shows that the rank is in fact bounded by dimension $e\mathrm{H}^1(\Gamma_1(Np), \mathbb{F}_p)$. We remark that since $\mathbb{F}_p = L(0, \mathbb{F}_p) = L(2-2, \mathbb{F}_p)$, the number of ordinary forms of all weights and level Np is controlled by the weight 2 ordinary forms.

Now say that M is a finitely generated free submodule of $M^{\mathrm{ord}}(N, \Lambda)$. Choose a basis $F_1,\ F_2, \ldots, F_d$. Choose integers $n_1,\ n_2, \ldots n_d$ such that $\det(a_{n_i}(F_j)) \neq 0$ in Λ. By the Weierstrass preparation theorem, there is a $k > 1$ such that the specialization of $\det(a_{n_i}(F_j))$ at $u^k - 1$ is also not 0. Let $f_1,\ f_2, \ldots, f_d$ be the corresponding specializations at $\nu_{k,1}$; by hypothesis they generate a free rank d submodule of $M_k^{\mathrm{ord}}(\Gamma_1(Np), \mathbb{Z}_p)$. But as we have mentioned above this last module has bounded rank, and so d is bounded from above. In particular the maximal rank free submodule of $M^{\mathrm{ord}}(N, \Lambda)$ has bounded rank, say r.

Now we can show that $M^{\mathrm{ord}}(N, \Lambda)$ is finitely generated as a Λ-module. Suppose $F_1, F_2, \ldots, F_r$ is a maximal linearly independent set of elements in $M^{\mathrm{ord}}(N, \Lambda)$. Then these elements form a basis of $M^{\mathrm{ord}}(N, \Lambda) \otimes_\Lambda Q(\Lambda)$, where $Q(\Lambda)$ is the quotient field of Λ. Thus, every element of $F \in M^{\mathrm{ord}}(N, \Lambda)$ is a linear combination $F = \sum_{i=1}^{r} x_i F_i$ of these F_i's with coefficients $x_i \in Q(\Lambda)$. For any set of r natural numbers $n_1, n_2, \ldots, n_r$, we have the matrix equation

$$AX = B$$

where $A = (a_{n_i}(F_j))$, $X = (x_1, x_2, \ldots, x_r)^t$ and $B = (a_{n_1}(F), \ldots, a_{n_r}(F))^t$. Choose the n_i such that $D = \det(A) \in \Lambda$ is non-zero. Multiplying the above matrix equation by the adjoint matrix of A, we see that $Dx_i \in \Lambda$, for $i = 1, \ldots, r$. Hence $DM^{\mathrm{ord}}(N, \Lambda) \subseteq \Lambda F_1 + \cdots + \Lambda F_r$. It follows that $M^{\mathrm{ord}}(N, \Lambda) \cong DM^{\mathrm{ord}}(N, \Lambda)$ is finitely generated as a Λ-module, since is isomorphic to a submodule of a finitely generated Λ-module, and Λ is noetherian. □

Remark 5.6. Clearly since $M(N, \Lambda)$ is a submodule of $\Lambda[[q]]$ it is torsion-free. With a bit more effort one can show that the finitely generated torsion-free Λ-module is in fact Λ-free (see [Hid93, p. 209]).

We now define the ordinary Λ-adic Hecke algebra $h^{\mathrm{ord}}(N, \Lambda)$ to be the Λ-subalgebra of $\mathrm{End}_\Lambda(M^{\mathrm{ord}}(N, \Lambda))$ generated over Λ by all the Hecke operators above. Similarly we define $h^{\mathrm{ord}}(N, I)$ by $h^{\mathrm{ord}}(N, \Lambda) \otimes_\Lambda I$. The finiteness of the space of ordinary Λ-adic

forms was initially proved by Hida who showed that $h^{\mathrm{ord}}(N,\Lambda)$ is finitely generated as a Λ-module. This statement already implies the first part of the following theorem which summarizes some of the main results of Hida theory.

Theorem 5.7 (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 lives in some primitive, ordinary form F.*
(3) *The form F in part (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.*

Parts (2) and (3) follow from what is usually referred to as Hida's control theorem and are not proved in these notes. The representation ρ_F in part (4) was constructed by Hida. In the next few sections we explain an alternative method of Wiles for constructing ρ_F. We also describe the local behaviour of ρ_F (a result of Wiles). This last result plays a key role in the proof of the Iwasawa main conjecture.

6. Ordinary Λ-adic Galois representations

The goal of this section is to construct Galois representations attached to ordinary Λ-adic eigenforms. All the material here is either taken directly (or modified slightly) from [Hid93] or [Wil88].

In this section p is an odd prime. Recall Λ denotes the power series ring $\mathbb{Z}_p[[X]]$, K is a finite extension of the field of fractions of Λ, and I denotes the integral closure of Λ in K. We shall explain Wiles' method of attaching a Galois representation into $\mathrm{GL}_2(K)$ to a normalized ordinary I-adic cuspidal eigenform F.

6.1. **Results.** We first state the precise result.

Theorem 6.1 (Hida, Wiles)**.** *Let F be a normalized I-adic eigenform of level N in $S^{\mathrm{ord}}(N,\chi,I)$, 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 $\rho_F : \mathrm{G}_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K)$ 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 *and* $\kappa : W = 1 + p\mathbb{Z}_p \to \Lambda^\times$ *is the usual character, and for any* $x \in \mathbb{Z}_p^*$, $\langle x\rangle := \omega(x)^{-1}x \in W$.

As mentioned above, the global representation ρ_F is absolutely irreducible. However the local representation obtained by restricting $\rho = \rho_F$ to a decomposition group D_p at the prime p, is reducible. More precisely, we have:

Theorem 6.2 (Wiles)**.** *Maintaining the same notations as above, the restriction of* ρ_F *to* D_p *is given up to equivalence by*

$$\rho_F\mid_{D_p} \sim \begin{pmatrix} \epsilon_1 & * \\ 0 & \epsilon_2 \end{pmatrix},$$

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

We shall prove Theorem 6.1 over the next several sections. Before we start, let us explain the strategy of the proof. Starting with a family of representations $\rho_i : \mathrm{G}_\mathbb{Q} \to \mathrm{GL}_2(M_i)$, where M_i is a finite extension of $\mathbb{Q}_p$, we wish to construct a Λ-adic representation $\rho : \mathrm{G}_\mathbb{Q} \to \mathrm{GL}_2(K)$ such that the 'reduction' of the representation ρ (see §6.3 below) at certain height 1 prime ideals $\{P_i\}_{i=1}^\infty$ is isomorphic to ρ_i (over some finite extension of $\mathbb{Q}_p$). In our case, the representations $\{\rho_i\}_{i=1}^\infty$ come from the representations associated to the classical specializations $F(P_i)$ (see §6.5 below), where P_i's are height 1 primes that are the kernels of the specialization maps $\nu = \nu_i$ considered earlier; the resulting representation ρ will be ρ_F. In order to patch the representations $\{\rho_i\}_{i=1}^\infty$ into a Λ-adic representation, a new notion was introduced by Wiles in [Wil88], namely that of a pseudo-representation (see §6.6 below). The importance of this notion lies in the fact that it is easier to patch pseudo-representations than it is to patch usual representations.

6.2. **Continuity of the Galois representation.** Before we prove Theorem 6.1, let us comment on what it means for a Λ-adic Galois representation $\rho : \mathrm{G}_\mathbb{Q} \to \mathrm{GL}_2(K)$ to be continuous.

Definition 6.3. 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

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

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

Remark 6.4. [Hid93, §7.5]. Since I is a ring of Krull dimension 2, its field of fractions K is not locally compact in any non-discrete topology on K (cf. Bourbaki, Commutative Algebra, §9.3). This implies that the image of a continuous representation of $\mathrm{G}_{\mathbb{Q}}$ into $\mathrm{GL}_2(K)$, with non-discrete topology on K, is small. This is why one takes the $\mathbf{m}$-adic topology on $\mathrm{End}_I(\mathcal{L})$ to define the continuity of ρ.

Remark 6.5. It is easy to see that an I-module $\mathcal{L}$ as above exists. However, $\mathcal{L}$ may not be free over I, and so one takes the projective limit topology on $\mathrm{Aut}_I(\mathcal{L})$. One thinks of the projective limit topology as a slight generalisation of the 'usual topology' on $\mathrm{GL}_2(I)$, which is induced from the product topology on I^4, since if $\mathcal{L}$ is a free module of rank 2 over I, then the projective limit topology on $\mathrm{Aut}_I(\mathcal{L})$ coincides with the 'usual topology'. Also, the continuity of the representation does not depend on the choice of the lattice $\mathcal{L}$, because of the Artin-Rees lemma, according to [Hid93, p. 228].

6.3. **Reduction of the representation ρ_F modulo a non-zero prime ideal P.** We wish to speak of the reduction of ρ_F modulo a non-zero prime ideal P, even before we have constructed the representation ρ_F. For any prime ideal P of I, let $Q(I/P)$ denote the field of fractions of I/P.

Definition 6.6. 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 $\mathbf{m}$-adic topology of $Q(I/P)$, it is semi-simple, and it satisfies the following properties:

- $\rho_F(P)$ is unramified outside Np,
- For any prime $q \nmid Np$,

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

6.4. **Existence of the residual representation at a non-zero prime P.** A priori it is not clear that the residual representation $\rho_F(P)$ attached to ρ_F exists. However, for any non-zero prime ideal, the residual representation exists.

Theorem 6.7. *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. 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. Let I_P denote the localisation of I at P. It is easy to see that I_P is a DVR. Since I_P is a PID, $\mathcal{L}_P = \mathcal{L} \otimes_I I_P$ becomes a free module of rank 2 over I_P. Identifying $\mathcal{L}_P$ with I_P^2 we 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 $I_P/PI_P = Q(I/P)$, we get

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

Let $\rho_F(P)$ be the semi-simplification of ρ_P. This is a candidate for the residual representation of ρ at P. Clearly, $\rho_F(P)$ satisfies the conditions mentioned in Definition 6.6, since ρ_F does. For example, the continuity of $\rho_F(P)$ follows from that of ρ_F, noting that after localizing $\mathcal{L}_P$ becomes free module over I_P, hence the projective limit topology and the usual topology coincide. The uniqueness of the representation $\rho_F(P)$ follows from the fact that the semi-simplification of a representation over a field of characteristic 0 is completely determined by its traces (see Lemma 6.8 below). The same result shows that $\rho_F(P)$ is independent of the choice of lattice $\mathcal{L}$. □

Lemma 6.8 ([Ser89, Chap. 1, §2])**.** *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* Trace $(\rho_1(g))$ = Trace $(\rho_2(g)), \forall\ g \in G$, *then ρ_1 and ρ_2 are isomorphic over K.*

Remark 6.9. By induction on the height of prime ideals, one can define the residual representation for prime ideals of height 2 as well. For further details, see [Hid93, §7.3].

6.5. **Identifying the residual representations $\rho_F(P)$ for arithmetic prime P.** We will in particular be interested in identifying the reductions of ρ_F at certain special height one prime ideals of I. Let

$$\Xi(I) \ = \ \{P : P = \text{kernel of a specialization map } \nu : I \to \bar{\mathbb{Q}}_p \text{ as in definition 3.1}\}.$$

The elements of $\Xi(I)$ are clearly height one prime ideals of I and are called arithmetic primes. We sometimes identify the homomorphisms ν with their kernels P.

Any element $\alpha \in I$ can be viewed as a function on $\mathrm{Spec}(I)(\bar{\mathbb{Q}}_p) = \mathrm{Hom}(I, \bar{\mathbb{Q}}_p)$ by $\alpha(P) := P(\alpha) = \alpha \pmod P$. In particular $F(P)$ gives a formal q-expansion in $\bar{\mathbb{Q}}_p[[q]]$. If P is an arithmetic prime, then $F(P)$ is by definition a classical cuspidal eigenform of weight at least 2, and so there is a classical Galois representation $\rho_{F(P)}$ attached to $F(P)$ by Deligne. We show that this representation agrees with the residual representation $\rho_F(P)$ attached to ρ_F.

First let us recall the definition of Galois representations attached to classical cusp forms. Let ψ be a character of conductor Np^r. Define

$$S_k(\Gamma_0(Np^r), \psi; A) := S_k(\Gamma_0(Np^r), \psi; \mathbb{Z}[\psi]) \otimes_{\mathbb{Z}[\psi]} A,$$

for any algebra A in $\mathbb{C}$ or $\bar{\mathbb{Q}}_p$, containing $\mathbb{Z}[\psi]$. Let $h_k(\Gamma_0(Np^r), \psi; A)$ denote the corresponding Hecke algebra. We have the following duality between cusp forms and the Hecke algebra:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}[\psi]}(h_k(\Gamma_0(Np^r), \psi; A), A) & \xrightarrow{\sim} & S_k(\Gamma_0(Np^r), \psi; A) \\ \varphi & \mapsto & \displaystyle\sum_{n=1}^{\infty} \varphi(T(n))q^n. \end{array} \tag{6.10}$$

Under this duality normalized eigenforms correspond to $\mathbb{Z}[\psi]$-algebra homomorphisms from $h_k(\Gamma_0(Np^r), \psi; A)$ to A. Let f be a normalised eigenform in $S_k(\Gamma_0(Np^r), \psi; K_f)$ where 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 6.11. *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*

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

The existence of such a representation was proved by Eichler-Shimura when $k = 2$, and by Deligne for $k \geq 2$.

As mentioned above, the representation $\rho_{f,\wp}$ is irreducible. However the local representation obtained by restricting $\rho_{f,\wp}$ to a decomposition subgroup D_p at the prime

p, is reducible. More precisely, we have:

$$\rho_{f,\wp}\,|_{D_p} \sim \begin{pmatrix} \psi\nu_p^{k-1} & \lambda(a_p)^{-1} & * \\ & 0 & \lambda(a_p) \end{pmatrix}, \tag{6.12}$$

where $\lambda(a)$ is the unramified character of D_p taking $\mathrm{Frob}_p \in D_p/I_p$ to a and ν_p is the p-adic cyclotomic character.

Now let P be a prime corresponding to ν extending $\nu_{k,\zeta}$, i.e., an arithmetic prime. Let $f = f_\nu = F(P)$. Let $\wp$ be the prime of K_f induced by the fixed embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$. By the computations in (6.14) below, we see 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 $Q(I/P)$. We can state a refined version of Theorem 6.11, for $f = F(P)$, as follows:

Corollary 6.13. *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 properties mentioned in Theorem* 6.11.

We can now show that the residual representation $\rho_F(P)$ attached to ρ_F is nothing but Deligne's representation $\rho_{F(P)}$, as Galois representations into $\mathrm{GL}_2(Q(I/P))$. To do this it is enough to show that the characteristic polynomials of the Frobenius elements outside Np coincide (by Lemma 6.8, and noting that the Frobenius elements outside Np are dense in $\mathrm{G}_{\mathbb{Q}}$). We compare the polynomials in Definition 6.6 and Theorem 6.11. Recall that for an integer n prime to p, we defined $s(\langle n\rangle) \in \mathbb{Z}_p$ so that $\langle n\rangle = u^{s(\langle n\rangle)}$. Now

$$\kappa(\langle n\rangle)(\zeta u^k - 1) = \kappa(u^{s(\langle n\rangle)})(\zeta u^k - 1) = (\zeta u^k)^{s(\langle n\rangle)} = \chi_\zeta(n)\omega^{-k}n^k,$$

since $\chi_\zeta(n) = \chi_\zeta(\langle n\rangle) = \zeta^{s(\langle n\rangle)}$ and $\langle n\rangle = \omega^{-1}(n)n$. Hence, if $P|_\Lambda = \ker(\nu_{k,\zeta})$, then

$$\begin{aligned} \lambda(T_q)(P) = a_q(F)(P) = a_q(F(P)) = a_q(f_\nu), \text{ and} \\ ((\chi\kappa\nu_p^{-1})(q))(P) = (\chi\omega^{-k}\chi_\zeta)(q)q^{k-1} = \chi_\nu(q)q^{k-1}, \end{aligned} \tag{6.14}$$

as desired.

6.6. **Pseudo-representations.** 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 6.15. Let G be a pro-finite group with an identity e, and a special element c of order 2. A pseudo-representation π from G to B, which shall be denoted by $\pi : G \to B$, is a triple $\pi = (A, D, X)$ of continuous maps

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

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) $X(\sigma, e) = X(e, \sigma) = X(\sigma, c) = X(\sigma, c) = 0$,
(7) $X(\sigma, \tau)X(\gamma, \eta) = X(\sigma, \eta)X(\gamma, \tau)$.

Remark 6.16. We denote A, D, X by A_π, D_π, X_π, when we need to specify π explicitly.

The function X is in fact determined by the function A, since for any $\sigma, \tau \in G$, we have $X(\sigma, \tau) = A(\sigma\tau) - A(\sigma)A(\tau)$. So it is possible to give an alternative description of a pseudo-representation using only the maps A and D. However, the given definition is convenient because it turns out to be important whether or not $X(\sigma, \tau) = 0$.

The name pseudo-representation implies, of course, a relationship with representations. Suppose ρ is an odd, 2-dimensional representation from G to B. By this we mean $\rho : G \to \mathrm{GL}_2(B)$ is a continuous homomorphism with $\rho(c) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Letting $\rho(\sigma) = \left(\begin{smallmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{smallmatrix}\right)$, one verifies immediately that $\pi = (A, D, X)$ given by

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

is a pseudo-representation from G to B.

Definition 6.17. If $\pi : G \to B$ is as above, then we say that π is the pseudo-representation *associated* to ρ, or that π *comes from* ρ.

Given a pseudo-representation π, we can define the Trace and Determinant of π.

Definition 6.18. $\mathrm{Tr}(\pi)(\sigma) := A(\sigma) + D(\sigma),\ \mathrm{Det}(\pi)(\sigma) := A(\sigma)D(\sigma) - X(\sigma, \sigma)$.

Remark 6.19. It is clear that if π comes from a representation, then the definitions of the Trace and Determinant of π coincide with that of the representation.

We have the following easily checked identities for $A(\sigma)$ and $D(\sigma)$, which play an important role in the proofs:

$$\begin{aligned} A(\sigma) &= \frac{\mathrm{Tr}(\pi)(\sigma) + \mathrm{Tr}(\pi)(c\sigma)}{2}, \text{ and,} \\ D(\sigma) &= \frac{\mathrm{Tr}(\pi)(\sigma) - \mathrm{Tr}(\pi)(c\sigma)}{2}. \end{aligned} \tag{6.20}$$

Here is a natural question: When does a pseudo-representation come from a representation? This question has an affirmative answer in some cases, as we see now.

Theorem 6.21. *Let π be a pseudo-representation from G to B such that either X is identically zero or $X(h_1, h_2) \in B^*$ 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. Let us divide the proof into two cases:
Case (i): If $X \equiv 0$, then we can define ρ by letting, for $g \in G$,

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

Since X is identically zero, ρ is a representation from $G \to GL_2(B)$.

Case (ii): Suppose $\exists$ two elements $h_1, h_2 \in G$ such that $X(h_1, h_2) \in B^*$. We define the representation ρ by setting, for $g \in G$,

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

with $a(g) = A(g),\ d(g) = D(g),\ b(g) = \frac{X(g,h_2)}{X(h_1,h_2)},\ c(g) = X(h_1, g)$. It is easy to check that ρ is a representation, by using the axioms for pseudo-representations (for the calculations see [Hid93, §7.5, Prop 1]). □

Corollary 6.22. *If B is a field, then the pseudo-representation π always comes from a 2-dimensional, odd, representation.*

Let us return to our situation where $G = \mathrm{G}_{\mathbb{Q}}$ and I is a finite extension of Λ. As mentioned earlier, the proof of Theorem 6.1 depends on patching results for pseudo-representations, which we describe now.

Lemma 6.23. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of I. Let $\pi(\mathfrak{a})$ and $\pi(\mathfrak{b})$ be pseudo-representations of G into $I/\mathfrak{a}$ and $I/\mathfrak{b}$, which are compatible, i.e., there exist two functions T and D on a dense subset Σ of G, with values in I, such that*

$$\begin{aligned} \mathrm{Tr}(\pi(\mathfrak{a}))(\sigma) \equiv T(\sigma) \pmod{\mathfrak{a}} \quad \text{and} \quad \mathrm{Tr}(\pi(\mathfrak{b}))(\sigma) \equiv T(\sigma) \pmod{\mathfrak{b}}, \\ \mathrm{Det}(\pi(\mathfrak{a}))(\sigma) \equiv D(\sigma) \pmod{\mathfrak{a}} \quad \text{and} \quad \mathrm{Det}(\pi(\mathfrak{b}))(\sigma) \equiv D(\sigma) \pmod{\mathfrak{b}}, \end{aligned} \tag{6.24}$$

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

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

on Σ.

Proof. Let us briefly explain the proof. We have the following short exact sequence

$$\begin{array}{ccccc} 0 \to I/(\mathfrak{a} \cap \mathfrak{b}) & \to & I/\mathfrak{a} \oplus I/\mathfrak{b} & \to & I/(\mathfrak{a} + \mathfrak{b}) \to 0 \\ \bar{a} & \mapsto & (\bar{a}, \bar{a}) & & \\ & & (\bar{a}, \bar{b}) & \mapsto & \overline{a - b}. \end{array}$$

Consider the map $\pi = \pi(\mathfrak{a}) \oplus \pi(\mathfrak{b})$ from G to $I/\mathfrak{a} \oplus I/\mathfrak{b}$. Since, $\pi(\mathfrak{a})$ and $\pi(\mathfrak{b})$ are pseudo-representations, it is easy to see π is also a pseudo-representation into $I/\mathfrak{a} \oplus I/\mathfrak{b}$. By (6.24), $\mathrm{Tr}(\pi) \bmod (\mathfrak{a} + \mathfrak{b})$ vanishes identically on Σ, and hence $\mathrm{Tr}(\pi)(\sigma) \equiv T(\sigma) \bmod (\mathfrak{a} \cap \mathfrak{b})$, for all $\sigma \in \Sigma$. So π is a candidate for $\pi(\mathfrak{a} \cap \mathfrak{b})$. It suffices to show π takes values in $I/\mathfrak{a} \cap \mathfrak{b}$. Since $\mathrm{Tr}(\pi)$ is a continuous map, the zero ideal is closed in $I/(\mathfrak{a} + \mathfrak{b})$ and Σ is dense in G, $\mathrm{Tr}(\pi) \bmod (\mathfrak{a} + \mathfrak{b})$ vanishes on G, and hence $\mathrm{Tr}(\pi)$ indeed takes values in $I/\mathfrak{a} \cap \mathfrak{b}$. Now, by (6.20), it is clear that the functions A_π, D_π, X_π corresponding to π, take values in $I/\mathfrak{a} \cap \mathfrak{b}$, as desired. □

We wish to generalize the lemma to a countable collection of ideals. Before stating this result, let us recall some results from commutative algebra.

Lemma 6.25. *Let A be a complete semi local ring, $\mathbf{m}$ be the intersection of its maximal ideals, and $\{\mathfrak{a}_n\}_{n=1}^{\infty}$ be a decreasing sequence of ideals such that $\cap_{n=1}^{\infty} \mathfrak{a}_n = 0$. Then there exists an integral valued function $s(n)$ which tends to infinity with n, such that $\mathfrak{a}_n \subseteq \mathbf{m}^{s(n)}$.*

Proof. See [ZS60, Chap 8, §5, Thm 13]. □

Lemma 6.26. *Let $\{\mathfrak{a}_n\}_{n=1}^{\infty}$ be a decreasing sequence of ideals in I such that $\cap_{n=1}^{\infty}\mathfrak{a}_n = 0$. Then the natural map $\eta : I \to \varprojlim_n I/\mathfrak{a}_n$ is an isomorphism.*

Proof. It is clear that $\ker(\eta) = \cap_{n=1}^{\infty}\mathfrak{a}_n$, and this is zero by assumption. For the surjectivity, we use Lemma 6.25. Let $(\bar{a}_n)$ be an element of $\varprojlim_n I/\mathfrak{a}_n$. We need to prove that there exists an element $a \in I$, such that $\eta(a) = (\bar{a}_n)$, i.e., $a - a_n \in \mathfrak{a}_n, \forall\ n \in \mathbb{N}$. For every $n \in \mathbb{N}$ and $j \geq n$, we have

$$a_j - a_n \in \mathfrak{a}_n.$$

By the above lemma, $a_j - a_n \in \mathbf{m}^{s(n)}$, i.e., the sequence $(\bar{a}_n)$ is a Cauchy sequence with respect to the $\mathbf{m}$-adic topology on I. Since I is complete with respect to this topology, the sequence $\{a_n\}$ converges to an element, say a, i.e., for every $j \geq 1$, we have

$$a - a_j \in \mathbf{m}^{s(j)}.$$

Now we show that, for every $n \in \mathbb{N}$, $a - a_n \in \mathfrak{a}_n$. Let us fix n. Adding the two displays above for $j \geq n$, we see $a - a_n \in \bigcap_{j\geq n}(\mathfrak{a}_n + \mathbf{m}^{s(j)})$. The ideal $\mathfrak{a}_n$ is closed in the $\mathbf{m}$-adic topology of I [ZS60, Chap 8, §4, Thm. 9] and hence $\mathfrak{a}_n = \bigcap_{j\geq n}(\mathfrak{a}_n + \mathbf{m}^{s(j)})$. Therefore, $a - a_n \in \mathfrak{a}_n$, for every $n \in \mathbb{N}$. □

Lemma 6.27. *Let R be a commutative noetherian integral domain. Let S denote a countable collection of height 1 prime ideals in R. Then*

$$\bigcap_{P\in S} P = 0.$$

Proof. Denote $\bigcap_{P\in S} P$ by J. In order to show $J = 0$, it suffices to show that any non-zero element x of J is contained in only finitely many height 1 prime ideals of R. Since R is noetherian, primary decomposition exists for ideals, and we can write

$$\mathrm{Rad}(x) = \cap_{i=1}^{n} Q_i,$$

where $\mathrm{Rad}(x)$ is the radical of (x) and $\{Q_i\}_{i=1}^{n}$ are prime ideals of R. Observe that the Q_i's are non-zero, because x is non-zero. Then

$$\{P \mid P \text{ is a prime ideal of height 1 containing } x\} \subseteq \{Q_1, Q_2, \cdots, Q_n\}.$$

□

We now have:

Theorem 6.28. *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 $n \geq 1$,*

$$\begin{aligned} \mathrm{Tr}(\pi(P_n))(\sigma) &\equiv T(\sigma) \pmod{P_n}, \\ \mathrm{Det}(\pi(P_n))(\sigma) &\equiv D(\sigma) \pmod{P_n}, \end{aligned} \tag{6.29}$$

for all $\sigma \in \Sigma$. Let $\mathfrak{a}_n = \cap_{i=1}^{n} P_i$. Then there exists a pseudo-representation π of G into I, such that for all $\sigma \in \Sigma$, and $n \geq 1$,

$$\begin{aligned} \mathrm{Tr}(\pi)(\sigma) &\equiv T(\sigma) \pmod{\mathfrak{a}_n}, \\ \mathrm{Det}(\pi)(\sigma) &\equiv D(\sigma) \pmod{\mathfrak{a}_n}, \end{aligned} \tag{6.30}$$

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

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

Proof. First, we shall show that, for every $n \geq 1$, there are pseudo-representations $\pi(\mathfrak{a}_n) : G \to I/\mathfrak{a}_n$ such that

$$\mathrm{Tr}(\pi(\mathfrak{a}_n))(\sigma) \equiv T(\sigma) \pmod{\mathfrak{a}_n}, \tag{6.31}$$

for every $\sigma \in \Sigma$. We do this by induction on n. For $n = 2$, applying Lemma 6.23 for the ideals P_1, P_2, and their associated pseudo-representations $\pi(P_1)$, $\pi(P_2)$, we get that $\pi(\mathfrak{a}_2)$ exists with the property (6.31). Assume that, we can construct pseudo-representations till $n-1$, i.e., that we can construct $\pi(\mathfrak{a}_1), \cdots, \pi(\mathfrak{a}_{n-1})$ satisfying (6.31). Now, applying Lemma 6.23 for the ideals $\mathfrak{a}_{n-1}$, P_n and their associated pseudo-representations $\pi(\mathfrak{a}_{n-1})$, $\pi(P_n)$, we get that $\pi(\mathfrak{a}_n)$ exists satisfying (6.31). Hence, we have constructed $\pi(\mathfrak{a}_n)$ satisfying (6.31), for all n.

In order to define the pseudo-representation π, let us first define its trace $\mathrm{Tr}(\pi)$ as follows:

$$\begin{aligned} \mathrm{Tr}(\pi) : G &\to \prod_{n=1}^{\infty} I/\mathfrak{a}_n \\ g &\mapsto (\mathrm{Tr}(\pi(\mathfrak{a}_n))(g)). \end{aligned} \tag{6.32}$$

By (6.31), all the $\pi(\mathfrak{a}_n)$'s are compatible (in the sense defined in Lemma 6.23), and hence $\mathrm{Tr}(\pi)(\Sigma) \subseteq \varprojlim_n I/\mathfrak{a}_n$. Now, by Lemma 6.26, $\mathrm{Tr}(\pi)(\Sigma) \subseteq I$, and satisfies:

$$\mathrm{Tr}(\pi)(\sigma) \equiv \mathrm{Tr}(\pi(\mathfrak{a}_n))(\sigma) \pmod{\mathfrak{a}_n}, \tag{6.33}$$

for all $\sigma \in \Sigma$. Since $I = \varprojlim_n I/\mathfrak{a}_n$ is closed in $\prod_{n=1}^{\infty} I/\mathfrak{a}_n$, we get $\mathrm{Tr}(\pi)(G) \subseteq I$, by the continuity of trace and the density of Σ in G. Now, we can construct the map π, from $\mathrm{Tr}(\pi)$, by defining $A(g),\ D(g)$ as in (6.20). It is easy to check that π is a pseudo-representation by using the fact that each $\pi(\mathfrak{a}_n)$ is a pseudo-representation. By (6.31) and (6.33), it is easy to see that (6.30) holds. The last statement follows from Lemma 6.27. A similar argument works for the Det function. □

Corollary 6.34. *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.*

Proof. This follows from Corollary 6.22 and Remark 6.19. □

6.7. **Existence of the representation ρ_F.** In this section, given F as in §6.1, we shall show the existence of the representation $\rho = \rho_F$. The strategy is to specialize F at a countable subset of prime ideals P in $\Xi(I)$ for which one has an associated Galois representation by Corollary 6.13, and then to patch these representations to construct ρ.

Theorem 6.35 (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 exist elements a_q and ϵ_q, in I, such that,

$$\mathrm{Trace}\ \rho_n(\mathrm{Frob}_q) = a_q \pmod{P_n}, \text{ and}$$
$$\mathrm{Det}\ \rho_n(\mathrm{Frob}_q) = \epsilon_q \pmod{P_n}.$$

Then there exists a continuous, odd, representation

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

with

$$\begin{aligned} \text{Trace } \rho(\text{Frob}_q) &= a_q, \\ \text{Det } \rho(\text{Frob}_q) &= \epsilon_q, \end{aligned}$$

for $q \nmid Np$. Also, ρ is irreducible and unique, 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 $\rho_n(c) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. We fix a representation ρ_n with this 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 $\sigma \in \mathrm{G}_{\mathbb{Q}}$. Let π_n denote the pseudo-representation associated to ρ_n (see Definition 6.17 in §6.6). A priori π_n is a pseudo-representation from $\mathrm{G}_{\mathbb{Q}}$ to $\widetilde{I/P_n}$. What is important for us is that ρ_n is actually a pseudo-representation into I/P_n. Let us explain this point more clearly.

In general, if $\rho(c) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, then the pseudo-representation ρ only depends on $\text{Trace}(\rho)$. In our case, by assumption, $\text{Trace}(\rho_n)$ belongs to I/P_n. Hence, we have a sequence of pseudo-representations from $\mathrm{G}_{\mathbb{Q}}$ into I/P_n. Take $\Sigma := \{\text{Frob}_q \mid q \nmid Np\}$. We know, by the Chebotarev density theorem, that Σ is dense $\mathrm{G}_{\mathbb{Q}}$. We are now in a position to apply Theorem 6.28 to get a pseudo-representation π from $\mathrm{G}_{\mathbb{Q}}$ into I such that

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

for all $q \nmid Np$. Now think of π as taking values in K. Then, by Corollary 6.34, we can lift this pseudo-representation π to a representation ρ such that both have the same traces and determinants on Σ. It is clear that ρ is irreducible, if ρ_n is irreducible for some n. Also, the representation ρ^{ss} is unique, by Lemma 6.8. Hence the theorem is proved. □

Remark 6.36. The above theorem can be found in a more general form in [Wil88, Lem. 2.2.3], where one works outside an analytic density zero set of primes.

As a consequence of the above theorem, we can finally prove Theorem 6.1:

Proof. We can take a countable collection of prime ideals of I, say $\{P_n\}_{n=1}^{\infty}$, of height 1 from $\Xi(I)$. We can take ρ_n to be the representation associated to $F(P_n)$, which

exists by Corollary 6.13. Maintaining the same notations as above, for every prime $q \nmid Np$, take

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

By the computations in (6.14), for every $q \nmid Np$, a_q and ϵ_q satisfy the conditions mentioned in the above theorem. Hence, we have a representation ρ, such that for each prime $q \nmid Np$

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

We call this ρ as ρ_F. Hence, we have proved Theorem 6.1. □

Remark 6.37. The same proof works for the prime $p = 2$, with a slight modification in the definition of the pseudo-representation. For further details, see [Wil88].

This finishes the proof of Theorem 6.1. Let us now prove Theorem 6.2.

6.8. **Proof of Theorem 6.2.** Define a continuous semi-simple representation ρ_0 from D_p to $\mathrm{GL}_2(I)$ as follows: for $g \in D_p$ set

$$\rho_0(g) = \begin{pmatrix} A(g) & 0 \\ 0 & D(g) \end{pmatrix},$$

where $A = (\chi\kappa\nu_p^{-1}) \cdot \lambda(a_p(F))^{-1}$ and $D = \lambda(a_p(F))$. Note that A and D take values in I since $a_p(F)$ is a unit in I. Indeed, $a_p(F)$ is a unit in I/P_i, for infinitely many height 1 prime ideals $\{P_i\}_{i=1}^{\infty}$ of I, and $I^\times = \varprojlim_n (I/\bigcap_{i=1}^{n} P_i)^\times$.

We shall show that ρ_0 and $(\rho_{F|_{D_p}})^{\mathrm{ss}}$ have the same traces. To prove this, the following observations are useful:

- Let ρ be a representation from $\mathrm{G}_{\mathbb{Q}}$ to $\mathrm{GL}_2(K)$ and let P be any height 1 prime ideal of I. Take a $\mathrm{G}_{\mathbb{Q}}$-stable lattice $\mathcal{L}$ over I. With respect to $\mathcal{L} \otimes_I I_P$, we may view ρ as a representation $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(I_P)$. Let $\rho_P = \rho$ modulo PI_P. (The residual representation $\rho(P)$ of ρ at P is, by definition, the semi-simplification of ρ_P.) Similarly, define $\rho_{|_{D_p,P}}$ to be $\rho_{|_{D_p}}$ modulo PI_P. Clearly

$$\rho_{|_{D_p,P}} = \rho_{P|_{D_p}}. \tag{6.38}$$

- It is known that Deligne's representation $\rho_{F(P)}$ is equivalent to the residual representation $\rho(P)$ attached to $\rho = \rho_F$ at an arithmetic prime P, i.e., $\rho_{F(P)} \sim$

$\rho(P)$. Since Deligne's representation $\rho_{F(P)}$ is irreducible, we further have $\rho_{F(P)} \sim \rho_P$. In particular, we have

$$\rho_{F(P)|_{D_p}} \sim \rho_{P|_{D_p}}. \tag{6.39}$$

Returning to the proof, let $\{P_n\}_{n=1}^{\infty}$ be a sequence of arithmetic height 1 prime ideals of I. Since the traces of ρ_0 and $(\rho_{F|_{D_p}})^{\mathrm{ss}}$ belongs to I, it is enough show that they are equal mod P_n, because $\bigcap\limits_{n\geq 1} P_n = 0$, by Lemma 6.27. But this follows, since mod P_n, we have:

$$\mathrm{trace}(\rho_0) \overset{(6.14)}{\equiv} \mathrm{trace}(\rho_{F(P_n)|_{D_p}}) \overset{(6.39)}{=} \mathrm{trace}(\rho_{P_n|_{D_p}}) \overset{(6.38)}{=} \mathrm{trace}(\rho_{|_{D_p,P_n}}).$$

Thinking of ρ_0 as a representation into $\mathrm{GL}_2(K)$, we conclude that $\rho_0 \sim (\rho_{F|_{D_p}})^{\mathrm{ss}}$, by Lemma 6.8.

By using the above description of the representation $(\rho_{F|_{D_p}})^{\mathrm{ss}}$, there are two possibilities for the representation $\rho_{F|_{D_p}}$, up to isomorphism, namely:

(1) $\rho_{F|_{D_p}} \sim \begin{pmatrix} A & U \\ 0 & D \end{pmatrix}$, or,

(2) $\rho_{F|_{D_p}} \sim \begin{pmatrix} A & 0 \\ U & D \end{pmatrix}$,

where U is a continuous map. These cases are not mutually exclusive. If the first case holds then we immediately obtain Theorem 6.2. In the second case, we shall show that $\rho_{F|_{D_p}}$ is semi-simple (i.e., U can be taken to be 0), proving the theorem in this case as well.

Indeed, suppose that $\rho_{F|_{D_p}}$ is non-split (i.e., not semi-simple). In particular, one knows that F is not of CM type [GV04, Prop. 12]. By an argument on [GV04, §4, p. 2161], we know that $\rho_{F(P_n)|_{D_p}}$ does not split for all but finitely many specializations. We now show that all the $\rho_{F(P_n)|_{D_p}}$ split, an obvious contradiction. Hence, $\rho_{F|_{D_p}}$ must be split, as desired.

Lemma 6.40. *For an arithmetic prime P of I, if the representation $\rho_{F|_{D_p}}$ is an extension of a ramified character by an unramified character, so is $\rho_{F(P)|_{D_p}}$.*

Proof. By (6.39), it is enough to show that $\rho_{P|_{D_p}}$ has an unramified subspace. This can be shown as follows.

By assumption, there exists a basis, say v_1, v_2, of K^2 such that $\rho_{F|_{D_p}}$ acts K-linearly on v_2 by the character D. Take any $\mathrm{G}_{\mathbb{Q}}$-stable lattice $\mathcal{L}$ over I_P. Since I_P is a DVR, there exists an I_P basis w_1, w_2 of $\mathcal{L}$, i.e., $\mathcal{L} = I_P w_1 + I_P w_2$. Now look at $Kv_2 \cap \mathcal{L}$. There exists an integer $r \in \mathbb{Z}$, such that $\pi^r v_2 = aw_1 + bw_2$, where π is a uniformizer of I_P, and a, $b \in I_P$ with $aI_P + bI_P = 1$. Clearly $\pi^r v_2 \in Kv_2 \cap \mathcal{L}$. It is clear that $I_P(\pi^r v_2) \subseteq I_P w_1 + I_P w_2$. Since $aI_P + bI_P = 1$, we can find a vector $\tilde{v}_1 \in I_P w_1 + I_P w_2$, such that $I_P(\pi^r v_2) + I_P \tilde{v}_1 = I_P w_1 + I_P w_2 = \mathcal{L}$.

Let us look at the representation ρ_F with respect to the new lattice $\mathcal{L}_2 = I_P \tilde{v}_1 + I_P(\pi^r v_2)$. It is clear that $\mathcal{L}_2$ is $\mathrm{G}_{\mathbb{Q}}$-stable lattice over I_P. With respect to $\mathcal{L}_2$, the representation $\rho_{F|_{D_p}}$ looks like

$$\begin{pmatrix} A_1 & 0 \\ U_1 & D \end{pmatrix} \in \mathrm{GL}_2(I_P). \tag{6.41}$$

Since trace of $\rho_{F|_{D_p}}$ is $A+D$, it is easy to see that $A_1 = A$. Now we have the following isomorphisms / equalities over $Q(I/P)$,

$$\rho_{F(P)|_{D_p}} \overset{(6.39)}{\sim} \rho_{P|_{D_p}} \overset{(6.38)}{=} \rho_{|_{D_p,P}} \overset{(6.41)}{=} \begin{pmatrix} \bar{A} & 0 \\ \bar{U}_1 & \bar{D} \end{pmatrix},$$

where bar denotes mod P reduction. Since D is unramified, $\bar{D}$ is also unramified. Also since P is an arithmetic prime, $\bar{A}\bar{D}$ is ramified by (6.12), noting $k \geq 2$ there. Hence, $\bar{A}$ is ramified. This shows that the representation $\rho_{F(P)|_{D_p}}$ is an extension of a ramified character by an unramified character. □

By the above lemma, $\rho_{F(P_n)|_{D_p}}$ is an extension of a ramified character by an unramified character. But by (6.12), it is also an extension of an unramified character by a ramified character. Hence the $\rho_{F(P_n)|_{D_p}}$ split, for all n. This completes the proof of Theorem 6.2.

7. Constructing cusp forms out of semi-cusp forms

Definition 7.1. A classical form f (respectively Λ-adic form F) is said to be a semi-cusp form if the constant term $a_0(f) = 0$ (respectively $a_0(F) = 0$).

When there is more than one cusp, a semi-cusp form, whether classical or Λ-adic, is not necessarily a cusp form. At one stage in the proof of the Iwasawa main conjecture

(see [Wil90, sec. 3]), Wiles needs to create a Λ-adic cusp form out of a Λ-adic semi-cusp form F. We describe a criterion in [Wil90, sec. 3] which achieves this. This criterion is used at a key point in the next section.

Let ϕ denote the Euler ϕ-function. Define the following Hecke operator (cf. [Wil90, p. 506]):

$$w \;:=\; e \cdot T_N \cdot \prod_{\ell | N} (T_\ell^{\phi(Np)} - (\kappa(\langle \ell \rangle) l^{-1})^{\phi(Np)}).$$

Remark 7.2. In Wiles' definition of w on [Wil90, p. 506], there is a Λ-adic diamond operator $\langle \ell \rangle$ which is essentially our $\kappa(\langle \ell \rangle)\ell$. The discrepancy of ℓ^2 in our definition of w comes from the fact that in this section we are working with the usual normalization $X \mapsto \zeta u^k - 1$ and not with Wiles' normalization $X = \zeta u^{k-2} - 1$. However, in the next section, we use Wiles' normalization, and so need to use the operators w with $\kappa(\langle \ell \rangle)\ell$, rather than $\kappa(\langle \ell \rangle)\ell^{-1}$. Also, strictly speaking, in our notation we should really be writing U_ℓ instead of T_ℓ.

In any case, we have the following result [Wil90, Lem. 3.2]:

Proposition 7.3. *Suppose p is odd and χ is a primitive character of level Np. If $F \in M(N, \chi, I)$ is a semi-cusp form, i.e., $a_0(F) = 0$, then wF is a cusp form.*

Proof. The proof we give is more explicit that the one given in [Wil90]. We take advantage of the assumption made in these notes that the base field is $\mathbb{Q}$.

Let f_ν be the specialization of F at ν, lying over $\nu_{k,\zeta}$. We must show that wf_ν is a cusp form. Recall that $f_\nu \in M_k(Np^r, \chi_\nu)$, and this last space has a Hecke-stable decomposition:

$$M_k(Np^r, \chi_\nu) \;=\; S_k(Np^r, \chi_\nu) \oplus \mathcal{E}(Np^r, \chi_\nu),$$

where $\mathcal{E}(Np^r, \chi_\nu)$ is the Eisenstein part of $M_k(Np^r, \chi_\nu)$. Thus, we may accordingly write:

$$f_\nu \;=\; g_\nu + E_\nu.$$

Since f_ν is a semi-cusp form by hypothesis, we note E_ν has the important property that the constant term of E_ν vanishes. Applying w to the above decomposition, we get

$$wf_\nu \;=\; wg_\nu + wE_\nu.$$

Since wg_ν is a cusp form, we are reduced to showing that $wE_\nu = 0$. We do this by analyzing the various possibilities for the basis elements that occur when one expands E_ν in a given basis, and by showing that (a part of) w kills each such basis element.

Recall that $\mathcal{E}_k(Np^r, \chi_\nu)$, for $k \geq 2$, has the well-known basis (see, for instance, Section 4.7 of Miyake's book *Modular Forms*):

$$E_k(\chi_1, \chi_2)(mz)$$

where

- χ_1 and χ_2 are characters with $\chi_1\chi_2 = \chi_\nu$, and,
- If $M_1 = \mathrm{cond}(\chi_1)$ and $M_2 = \mathrm{cond}(\chi_2)$, then $mM_1M_2 \,\big|\, Np^r$.

When $k = 2$ and both χ_1 and χ_2 are trivial, the basis element $E_2(\chi_1, \chi_2)$ has to be modified slightly: in this case instead of $M_1 = M_2 = 1$, one takes $M_1 = 1$ and M_2 to be a prime number. Here $E_k(\chi_1, \chi_2)$ is the Eisenstein series defined by the identities:

$$L(E_k(\chi_1, \chi_2), s) \;=\; L(s, \chi_1)L(s - k + 1, \chi_2),$$

that is,

$$a_n(E_k(\chi_1, \chi_2)) \;=\; \sum_{d|n} \chi_1\left(\frac{n}{d}\right)\chi_2(d)d^{k-1}, \text{ for } n \geq 1,$$

and,

$$a_0(E_k(\chi_1, \chi_2)) \;=\; \begin{cases} 0 & \text{if } \chi_1 \neq 1, \\ \frac{-B_{k,\chi}}{2k} & \text{otherwise (except it's} \\ \frac{M_2-1}{24} & \text{when } k = 2, \text{ and } \chi_1,\ \chi_2 \text{ are trivial).} \end{cases}$$

In particular $E_k(\chi_1, \chi_2)(mz)$ has vanishing constant term iff $\chi_1 \neq 1$.

Write E_ν as a linear combination of the above basis elements. Since E_ν has zero constant term, not all the basis elements can occur. If the p-part of $\chi_\nu = \chi\omega^{-k}\chi_\varsigma$ is primitive (e.g., if $r > 1$ or the p-part of χ is not ω^k), then χ_ν is primitive of level Np^r, so $m = 1$, and there is only one basis element with non-zero constant term, namely $E_k(1, \chi_\nu)(z)$. Thus, the only basis elements that can occur in E_ν are the $E_k(\chi_1, \chi_2)(z)$ with $\chi_1 \neq 1$. Now assume that $r = 1$ and the p-part of χ_ν is trivial. Think of χ_ν as a character of level N, and note $E_k(1, \chi_\nu)$ has level N (instead of Np). In this case

there are two basis elements with non-zero constant term, namely $E_k(1,\chi_\nu)(z)$ and $E_k(1,\chi_\nu)(pz)$. Change basis and replace these forms by their p-stabilizations:

$$\begin{aligned} E_k^{(p)}(1,\chi_\nu)(z) &= E_k(1,\chi_\nu)(z) - \chi_\nu(p)p^{k-1}E_k(1,\chi_\nu)(pz) \\ F_k^{(p)}(1,\chi_\nu)(z) &= E_k(1,\chi_\nu)(z) - E_k(1,\chi_\nu)(pz). \end{aligned}$$

These have p-th Fourier coefficients 1, and $\chi_\nu(p)p^{k-1}$, respectively. Clearly $E_k^{(p)}$ has non-zero constant term, whereas $F_k^{(p)}$ has zero constant term. Thus again in this new basis the only basis elements that occur in this linear combination of E_ν are the $E_k(\chi_1,\chi_2)(mz)$ with $\chi_1 \neq 1$ and $m = 1$ or p, and $F_k^{(p)}$.

Thus it suffices to show that w kills the basis elements $E_k(\chi_1,\chi_2)(mz)$ with $\chi_1 \neq 1$, and $F_k^{(p)}$. We do this case by case. First note that Hida's idempotent e, hence w, kills $F_k^{(p)}$, since $a_p(F_k^{(p)})$ is not a p-adic unit. Similarly if $m > 1$, then $a_p(E_k(\chi_1,\chi_2)(mz)) = 0$, so again w kills $E_k(\chi_1,\chi_2)(mz)$. Thus it suffices to show that w kills the basis elements $E_k(\chi_1,\chi_2)(z)$ with $\chi_1 \neq 1$, i.e., with $M_1 \neq 1$. We have the further cases:

(1) Suppose $\ell|M_1$ and $\ell|M_2$, for some $\ell|Np^r$: In this case $a_\ell = \chi_1(\ell)+\chi_2(\ell)\ell^{k-1} = 0$. If $\ell|N$, then $a_\ell|a_N$ and $a_N = 0$, so T_N kills $E_k(\chi_1,\chi_2)$. If $\ell = p$, then $a_p = 0$ in which case e does the trick.

(2) Suppose $\ell|M_1$ but $\ell \nmid M_2$, for some $\ell|Np^r$. Write E_k for $E_k(\chi_1,\chi_2)$, for simplicity. There are two further sub-cases:

(i) Suppose $\ell \neq p$. In this case $a_\ell = \chi_1(\ell) + \chi_2(\ell)\ell^{k-1} = \chi_2(\ell)\ell^{k-1}$. Thus

$$T_\ell E_k = a_\ell E_k = \epsilon_1 l^{k-1} E_k,$$

where ϵ_1 is a $\phi(N)$-th root of unity. Now as we have checked many times before $\kappa(\langle\ell\rangle)l^{-1}$ specializes under ν to $\omega^{-k}\chi_\zeta(\ell)l^{k-1}$, so

$$(\kappa(\langle\ell\rangle)l^{-1})E_k = \epsilon_2\zeta^{s(\langle\ell\rangle)}l^{k-1}E_k,$$

for some $\phi(p)$-th root of unity ϵ_2. Thus:

$$(T_\ell^{\phi(Np)} - (\kappa(\langle\ell\rangle)l^{-1})^{\phi(Np)})E_k = (1-\zeta')(l^{k-1})^{\phi(Np)}E_k,$$

for some p-power root of unity ζ'. But note that $1-\zeta'$ is not a p-adic unit (though the power of ℓ is), so further composing with e kills E_k. (NB: The last part of the argument just given corrects the somewhat incorrect hint on [Wil90, p. 506, line 19], which claims that the previous line is already identically 0; this seems to us to hold only in the special case when ζ and hence ζ' are 1).

(ii) Finally suppose $\ell = p$. Then $a_\ell = a_p = \chi_2(p)p^{k-1}$ is not a p-adic unit, so again $eE_k = 0$.

Since, in all cases w kills the basis elements in E_ν, we are done. □

8. Eisenstein ideals and p-adic L-functions

In Mazur's famous paper [Maz77], key use is made of the so called Eisenstein ideal. This ideal measures congruences between cusp forms of weight 2 for $\Gamma_0(p)$ and the (unique, normalized) Eisenstein series of weight 2 for $\Gamma_0(p)$. As with many things in [Wil90], Wiles defines a Λ-adic analogue of this ideal (cf. [Wil90, Sec. 4]), and proves a result which shows that it measure congruences between Λ-adic cusp forms (of some tame level N and character χ), and the Λ-adic Eisenstein series $\mathcal{E}_\chi$ introduced in Section 4. We describe Wiles' result in this section.

8.1. **Classical Eisenstein ideal.** As motivation, we first recall some facts about the classical Eisenstein ideal.

We have the standard decomposition of forms of level p and trivial nebentypus:

$$M_2(p,1) = S_2(p,1) \oplus \mathcal{E}_2(p,1),$$

where the space of cusp forms $S_2(p,1)$ has dimension equal to the genus of $X_0(p)$, and $\mathcal{E}_2(p,1)$ is one-dimensional spanned by the Eisenstein series that was earlier called $E_2^{(p)}$ (this is also $E_2(\chi_1,\chi_2)$ of the last section, with χ_1 trivial of conductor 1, and χ_2 trivial of conductor p). As mentioned in the last section, $E_2^{(p)}$ has q-expansion:

$$E_2^{(p)} \;=\; \frac{p-1}{24} + \sum_{n=1}^{\infty} \sigma_1^{(p)}(n)\, q^n.$$

One is interested in studying congruences between cuspidal eigenforms f_2 and $E_2^{(p)}$, i.e., congruences of the form

$$f_2 \equiv E_2^{(p)} \mod \ell,$$

where ℓ is a prime (call such primes ℓ Eisenstein congruence primes). Heuristically, one can write down such congruences by noting that if ℓ divides the constant term of $E_2^{(p)}$, then $E_2^{(p)}$ mod ℓ looks like a mod ℓ cuspidal eigenform, and so should lift to a characteristic zero cuspidal eigenform. This is in fact what happens. To make this precise, we need the notion of a congruence module. Let $\mathbb{T}_{M_2}$, respectively, $\mathbb{T}_{S_2}$, $\mathbb{T}_{\mathcal{E}_2}$, be the Hecke algebras acting on the three spaces in the decomposition above.

There are natural projection maps $\mathbb{T}_{M_2} \twoheadrightarrow \mathbb{T}_{S_2}$ and $\mathbb{T}_{M_2} \twoheadrightarrow \mathbb{T}_{\mathcal{E}_2}$, and these induce the natural map $\mathbb{T}_{M_2} \hookrightarrow \mathbb{T}_{S_2} \oplus \mathbb{T}_{\mathcal{E}_2}$.

Definition 8.1. Let

$$C(\mathbb{T}) = \frac{\mathbb{T}_{S_2} \oplus \mathbb{T}_{\mathcal{E}_2}}{\mathbb{T}_{M_2}}$$

be the congruence module with respect to the decomposition above.

It is easy to see that $|C(\mathbb{T})| < \infty$ and $\ell \,\big|\, |C(\mathbb{T})|$ iff there is a congruence of the form we are interested in. Thus the Eisenstein congruence primes are exactly the primes in the support of $|C(\mathbb{T})|$.

There is another way to write down $C(\mathbb{T})$, that is completely intrinsic to $\mathbb{T}_{S_2}$. This uses the Eisenstein ideal I, an ideal of $\mathbb{T}_{S_2}$. Noting that $a_q(E_2^{(p)}) = q + 1$ for primes $q \neq p$ and $a_p(E_2^{(p)}) = 1$, one defines:

Definition 8.2. The Eisenstein ideal I is the ideal of T_{S_2} spanned by $T_q - (q+1)$ for all $q \neq p$, and by $U_p - 1$.

Lemma 8.3. *The natural map $\mathbb{T}_{S_2} \hookrightarrow \mathbb{T}_{S_2} \oplus \mathbb{T}_{\mathcal{E}_2}$ induces an isomorphism*

$$\frac{\mathbb{T}_{S_2}}{I} \xrightarrow{\sim} C(\mathbb{T}).$$

In view of the lemma we deduce that the Eisenstein congruence primes are those in the support of T_{S_2}/I. But now, we have (cf. [Maz77, Prop. 9.7]):

Theorem 8.4. *Let n be the numerator of $\left(\frac{p-1}{12}\right)$. Then*

$$\frac{\mathbb{T}_{S_2}}{I} \xrightarrow{\sim} \frac{\mathbb{Z}}{n}.$$

In particular we see that $n \in I$ (compare with the definition of I below).

One concludes that the Eisenstein congruence primes are exactly the prime divisors of the numerator of (twice) the constant term of $E_2^{(p)}$.

8.2. **Λ-adic Eisenstein ideal.** Following Wiles, we wish to 'Λ-fy' the previous discussion. Let p be an odd prime and let χ be a fixed non-trivial, even, primitive Dirichlet character of level Np. In Section 4, we had introduced the Λ-adic Eisenstein series $\mathcal{E}_\chi$ attached to χ. This has q-expansion in $I_\chi[[q]]$ where $I_\chi = \mathbb{Z}_p[\chi][[X]]$ (not to be confused with I, which in this section is reserved for the Eisenstein ideal).

To avoid errors in what follows we work with Wiles' normalization, so in particular, we take $\mathcal{E}_\chi$ as modified in Section 4.5. Consider the direct sum

$$S^{\mathrm{ord}}(N,\chi,I_\chi)\oplus I_\chi\cdot\mathcal{E}_\chi$$

inside the space $M^{\mathrm{ord}}(N,\chi,I_\chi)$. As before, we wish to understand congruences between ordinary Λ-adic cuspidal eigenforms, and $\mathcal{E}_\chi$. Let $\mathbb{T}_{S^{\mathrm{ord}}}$ denote the Λ-adic Hecke algebra acting on $S^{\mathrm{ord}}(N,\chi,I_\chi)$. Noting that $a_n(\mathcal{E}_\chi)=A_{n,\chi}(X)\in I_\chi$, for all integers $n\geq 1$ (where $A_{n,\chi}(X)$ is modified as in Section 4.5), we define (cf. [Wil90, eq. (4.2)]):

Definition 8.5. The Λ-adic Eisenstein ideal is the ideal in $\mathbb{T}_{S^{\mathrm{ord}}}$ generated by

- $T_q - A_{q,\chi}(X)$ for prime $q\nmid Np$,
- $U_q - A_{q,\chi}(X)$, for prime $q|Np$, and,
- $\hat{G}^0_\chi(X)$.

Recall that $\hat{G}_\chi(X)$ is the numerator of (twice) the constant term of Wiles' $\mathcal{E}_\chi$. Here $\hat{G}^0_\chi(X)$ is the power series constructed from $\hat{G}_\chi(X)$ by dividing out any possible factors of the form $(1+X-\zeta u^{-1})$ occurring in $\hat{G}_\chi(X)$. As Wiles remarks, one takes the modified p-adic L-function $\hat{G}^0_\chi(X)$ in I in order to avoid certain zeros which cause later complications in his proof of the Iwasawa main conjecture.

The main result of this section is the following theorem (cf. [Wil90, Thm. 4.1]):

Theorem 8.6. *Let χ_0 denote the trivial character of conductor p. Suppose that either $\chi\neq\omega^{-2}$ or $L_p(1,\chi_0)=\infty$. Then*

$$\frac{\mathbb{T}_{S^{\mathrm{ord}}}}{I}\xrightarrow{\sim}\frac{I_\chi}{(\hat{G}^0_\chi(X))}.$$

Before we begin the proof, we need the following abstract lemma.

Lemma 8.7. *Let $\mathfrak{b}=(G^0)$ be a principal ideal of I_χ, and say that $F\in S^{\mathrm{ord}}(N,\chi,I_\chi)$ is a mod $\mathfrak{b}$ eigenform. Assume that $(G^0,a_1(F))=1$ so that $a_1(F)$ is invertible in $I_\chi/\mathfrak{b}$. Then the map*

$$\begin{aligned}\lambda:\mathbb{T}_{S^{\mathrm{ord}}} &\to I_\chi/\mathfrak{b}\\ T_m &\mapsto \frac{a_m(F)}{a_1(F)}\end{aligned}$$

is a surjective I_χ-algebra homomorphism.

Proof. When F is normalized, i.e., $a_1(F) = 1$, this is immediate by the correspondence between normalized eigenforms, and homomorphisms of the Hecke algebra. When F is not normalized, we leave the proof that the given map is still a homomorphism as an exercise. □

Proof. Returning to the proof of the theorem, we wish to apply the above lemma with $G^0 = \hat{G}^0_\chi$ and $F = F'$, a certain non-normalized mod $\mathfrak{b}$ cuspidal eigenform of Eisenstein type. We construct F' explicitly now.

Let ψ be an auxiliary even character of conductor Np^r. Let $E_1(1, \psi\omega^{-1})$ be the Eisenstein series defined in the previous section, but for $k = 1$. Write the constant term in lowest terms as $g_{1,\psi\omega^{-1}}/h_{1,\psi\omega^{-1}}$. Set

$$J_{\chi,\psi} := E_1(1, \psi\omega^{-1}) \cdot \mathcal{E}_{\chi\psi^{-1}}(u^{-1}(1+X) - 1).$$

Here are some remarks.

- $J_{\chi,\psi} \in M(N, \chi, I_\chi)$ is a Λ-adic form in the sense of Wiles. Indeed the first term lies in $M_1(Np^r, \psi\omega^{-1})$ and the second term, after specialization at $X = \zeta u^{k-2} - 1$, lies in $\mathcal{E}_{k-1}(Np^r, \chi\psi^{-1}\omega^{2-(k-1)}\chi_\zeta)$, so the product (after specialization) lies in $M_k(Np^r, \chi\omega^{2-k}\chi_\zeta)$, as desired.
- The constant term of $J_{\chi,\psi}$ is

$$\frac{1}{2} \cdot \frac{g_{1,\psi\omega^{-1}}}{h_{1,\psi\omega^{-1}}} \cdot \frac{\hat{G}_{\chi\psi^{-1}}(u^{-1}(1+X) - 1)}{\hat{H}_{\chi\psi^{-1}}(u^{-1}(1+X) - 1)}.$$

Following Wiles, define the following two expressions in I_χ:

$$\begin{aligned} h_{1,\psi} &= \hat{H}_\chi(X) \cdot g_{1,\psi\omega^{-1}} \cdot \hat{G}_{\chi\psi^{-1}}(u^{-1}(1+X) - 1), \\ h_{2,\psi} &= \hat{G}_\chi(X) \cdot h_{1,\psi\omega^{-1}} \cdot \hat{H}_{\chi\psi^{-1}}(u^{-1}(1+X) - 1), \end{aligned}$$

and set

$$F = 2\left(h_{1,\psi}\mathcal{E}_\chi - h_{2,\psi}J_{\chi,\psi}\right).$$

Then by construction F is a Λ-adic semi-cusp form in $M(N, \chi, I_\chi)$, i.e., $a_0(F) = 0$.

By Proposition 7.3, the form $F' = wF$ is a cusp form. We use the operator w as described in Remark 7.2, since in this section we are using Wiles' normalization.

Noting that $h_{2,\psi}$ is divisible by $\hat{G}^0_\chi(X)$, we compute:

$$\begin{aligned} F' &= 2h_{1,\psi}\cdot w\mathcal{E}_\chi - 2h_{2,\psi}\cdot wJ_{\chi,\psi} \\ &\equiv 2h_{1,\psi}\cdot\left(e\cdot T_N\cdot\prod_{\ell|N}(T_\ell^{\phi(Np)}-(\kappa(\langle\ell\rangle)l)^{\phi(Np)})\right)\mathcal{E}_\chi \mod (\hat{G}^0_\chi) \\ &\equiv 2h_{1,\psi}\cdot\left(\prod_{\ell|N}(1-(\kappa(\langle\ell\rangle)l)^{\phi(Np)})\right)\mathcal{E}_\chi \mod (\hat{G}^0_\chi), \end{aligned}$$

since

$$\begin{aligned} e\mathcal{E}_\chi &= \mathcal{E}_\chi, \\ T_N\mathcal{E}_\chi &= \mathcal{E}_\chi, \text{ and,} \\ T_\ell\mathcal{E}_\chi &= \mathcal{E}_\chi, \end{aligned}$$

for all $\ell|N$.

Thus if $\mathfrak{b}=(\hat{G}^0_\chi)$, then $F'\equiv c\mathcal{E}_\chi \mod \mathfrak{b}$, with

$$c = 2h_{1,\psi}\cdot\left(\prod_{\ell|N}(1-(\kappa(\langle\ell\rangle)l)^{\phi(Np)})\right).$$

In particular F' is a (non-normalized) mod $\mathfrak{b}$ cuspidal eigenform. To apply Lemma 8.7 we need to further note:

Lemma 8.8. *The following hold:*

1. *There is a ψ such that $h_{1,\psi}$ has no zero in common with $\hat{G}_\chi(X)$, except possibly those of $\hat{H}_\chi(X)$.*
2. *If $\chi\neq\omega^{-2}$ or $L_p(1,\chi_0)=\infty$, then $\hat{G}_\chi(X)$ has no zero in common with $\hat{H}_\chi(X)$.*
3. *For $\ell|N$, the power series $1-(\kappa(\langle\ell\rangle)l)^{\phi(Np)}$ has no zero in common with $\hat{G}^0_\chi(X)$.*

In particular, for appropriate ψ, which we fix once and for all, and under the hypotheses of the theorem, c has no zero in common with $\hat{G}^0_\chi(X)$.

Proof. We prove the statements one by one.

(1) Let $\psi^{-1}=\chi_\zeta$. Then, a short computation using (4.3) shows that

$$\hat{G}_{\chi\psi^{-1}}(u^{-1}(1+X)-1)=G_\chi(\zeta u^{-1}(1+X)-1).$$

By choosing ζ of sufficiently large order we see that we may assume this power series has no zeros in common with $\hat{G}_\chi(X)$, from which (1) follows.

(2) If $\chi\omega^2 \neq 1$, then $\chi\omega^2$ is not of type W, so $\hat{H}_\chi(X) = H_{\chi\omega^2}(u^2(1+X)-1) = 1$ and the claim follows trivially. If $\chi\omega^2 = 1$ then $\hat{H}_\chi(X) = u^2(1+X)-1$, and the only root is $X = u^{-2}-1$. But on substituting $X = u^{-2}-1$, we have:

$$\frac{\hat{G}_\chi(X)}{\hat{H}_\chi(X)} = \frac{G_{\chi_0}(u^2(1+X)-1)}{H_{\chi_0}(u^2(1+X)-1)} = \frac{G_{\chi_0}(u^0-1)}{H_{\chi_0}(u^0-1)} = L_p(1-0,\chi_0) = \infty,$$

by hypothesis, so the numerator of the LHS does not have a zero at $X = u^{-2}-1$.

(3) Since $\omega(\ell)^{\phi(p)} = 1$ and $\langle\ell\rangle = u^{s(\langle\ell\rangle)}$ we have

$$(\kappa(\langle\ell\rangle)l)^{\phi(Np)} = ((1+X)^{s(\langle\ell\rangle)}\langle l\rangle)^{\phi(Np)} = ((1+X)u)^{s(\langle\ell\rangle)\phi(Np)} = 1$$

iff $X = \zeta u^{-1}-1$. But these were precisely the zeros that were removed from $\hat{G}_\chi(X)$ to get $\hat{G}^0_\chi(X)$.

□

Applying Lemma 8.7 to to $\mathfrak{b} = (\hat{G}^0_\chi)$, and F' with $a_1(F') = c$, which as we have just noted is coprime to $\hat{G}^0_\chi$, we get the last isomorphism of the following sequence of surjective I_χ-algebra homomorphisms:

$$\frac{I_\chi}{(\hat{G}^0_\chi(X))} \twoheadrightarrow \frac{\mathbb{T}_{S^{\mathrm{ord}}}}{I} \twoheadrightarrow \frac{\mathbb{T}_{S^{\mathrm{ord}}}}{\ker(\lambda)} \xrightarrow{\sim} \frac{I_\chi}{(\hat{G}^0_\chi(X))}.$$

The second surjection arises by noting that $I \subset \ker(\lambda)$, since by Lemma 8.7, the homomorphism λ takes T_n to $a_n(F')/c \equiv A_{n,\chi} \bmod \mathfrak{b}$. Finally, the first surjection arises from the structure map $I_\chi \to \mathbb{T}_{S^{\mathrm{ord}}}$ by noting that $\hat{G}^0_\chi(X) \in I$.

But a surjective endomorphism of a noetherian ring is an isomorphism, proving the theorem.

□

References

[CS10] J. Coates and R. Sujatha. The main conjecture. This volume.

[Dal10] C. Dalawat. Ribet's modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. This volume.

[Gha05] E. Ghate. Ordinary forms and their local Galois representations. In *Algebra and number theory*, pages 226–242. Hindustan Book Agency, Delhi, 2005.

[GV04] E. Ghate and V. Vatsal. On the local behaviour of ordinary Λ-adic representations. *Ann. Inst. Fourier, Grenoble*, 54(7):2143–2162, 2004.

[Hid86] H. Hida. Galois representations into $\mathrm{GL}_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms. *Invent. Math.*, 85:545–613, 1986.

[Hid93] H. Hida. *Elementary Theory of L-functions and Eisenstein series*. Cambridge University Press, 1993.

[Mat86] H. Matsumura. Commutative ring theory. *Cambridge studies in advanced mathematics*, 8, 1986.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47:33–186, 1977.

[MW86] B. Mazur and A. Wiles. On p-adic analytic families of Galois representations. *Compositio Math.*, 59:231–264, 1986.

[Rib76] K. Ribet. A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. *Invent. Math.*, 34(3):151–162, 1976.

[Ski04] C. Skinner. CMS lecture notes. Zhejiang University, Hangzhou, 2004.

[Ser89] J-P. Serre. *Abelian l-adic representations and elliptic curves. Second edition*. Advanced Book Classics. Addison-Wesley Publishing Company, Redwood City, CA, 1989.

[Ven10] O. Venjakob. Deligne-Ribet's work on L-values. This volume.

[Was96] L. Washington. *Introduction to cyclotomic fields, Second edition*. Springer-Verlag, Berlin-New York, 1996.

[Wil88] A. Wiles. On ordinary λ-adic representations associated to modular forms. *Inv. Math.*, 94(3):529–573, 1988.

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

[ZS60] O. Zariski and A. Samuel. *Commutative Algebra*. The University Series, 1960.

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400005, India.

E-mail address: debargha@math.tifr.res.in

E-mail address: ganesh@math.tifr.res.in

E-mail address: eghate@math.tifr.res.in