A PROOF OF THE IWASAWA MAIN CONJECTURE FOR $\mathbb{Q}$

GYUJIN OH

Contents

We will sketch a proof of the Iwasawa Main Conjecture for $\mathbb{Q}$, following Wiles' approach [Wil2]. This note is largely based on [Ski].

1. Recap of the setting

We use the following notations.

- p is an odd prime, and $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.
- $\mathbb{Q}_n$ is the unique $\mathbb{Z}/p^n\mathbb{Z}$-extension of $\mathbb{Q}$ in $\mathbb{Q}_\infty$.
- $\chi : G_\mathbb{Q} \to \mathbb{Z}_p^\times$ is the cyclotomic character, and $\omega : G_\mathbb{Q} \to \mathbb{Z}_p^\times$ is the Teichmuller character (i.e. they are the same mod p).
- Frob will mean arithmetic Frobenius.
- $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, $\gamma \in \Gamma$ a topological generator, $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$.
- $\Lambda = \mathbb{Z}_p[[\Gamma]] \xrightarrow{\sim} \mathbb{Z}_p[[T]]$ via identification $\gamma \mapsto 1+T$. Let $\mathcal{W} = (\mathrm{Spf}\,\Lambda)^{\mathrm{rig}}$, which is the rigid analytic unit disk, in a sense that $\mathcal{W}(L) = \{x \in L \mid |x-1|_p < 1\}$ for any algebraic extension $L/\mathbb{Q}_p$. This gives a universal family of characters $\Psi : G_\mathbb{Q} \twoheadrightarrow \Gamma \hookrightarrow \Lambda^\times$.
- For an integer k and a p-power root of unity ζ, we can associate an arithmetic point $\phi_{k,\zeta} \in \mathcal{W}(\mathbb{Q}_p[\zeta])$, which as a continuous homomorphism $\Lambda \to \mathbb{Q}_p[\zeta]$ sends γ to $\zeta\chi^k(\gamma)$. Applying this to Ψ, we get $\Psi_{k,\zeta} := \phi_{k,\zeta} \circ \Psi = \psi_\zeta \omega^{-k}\chi^k$ where $\psi_\zeta : G_\mathbb{Q} \to \Gamma \to \mathbb{Z}_p[\zeta]^\times$ sends $\gamma \mapsto \zeta$.
- For a topological $\mathbb{Z}_p$-module M, let M^* be the Pontryagin dual $M^* = \mathrm{Hom}_{\mathrm{cont}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$. This swaps compactness and discreteness.

The Iwasawa Main Conjecture for $\mathbb{Q}$ is about two objects built out of a Dirichlet character ψ, seen as a character of $G_\mathbb{Q}$. Throughout the note we will assume that ψ is odd.

- Let the conductor of ψ be denoted as N_ψ.
- Let $\mathcal{O}_\psi = \mathbb{Z}_p[\psi]$, $F_\psi = \mathbb{Q}_p[\psi]$, $\Lambda_\psi = \Lambda \otimes_{\mathbb{Z}_p} \mathcal{O}_\psi$. Then $\psi\Psi$ can be thought as a character $\psi\Psi : G_\mathbb{Q} \to \Lambda_\psi^\times$.

Date: Nov 9, 2018.

- (Analytic side) We have seen that there is a ***p-adic L-function*** $\mathcal{L}_\psi \in \mathrm{Frac}(\Lambda_\psi)$, i.e. for any nonnegative integer k and p-power root of unity ζ,
$$\phi_{k,\zeta}(\mathcal{L}_\psi) = L^{\{p\}}(0, \psi\Psi_{k,\zeta}) = L^{\{p\}}(-k, \psi\psi_\zeta\omega^{-k}),$$
where $L^{\{p\}}$ is the L-function with the p-Euler factor removed. There exist $g_\psi, h_\psi \in \Lambda_\psi$ such that
$$\mathcal{L}_\psi = \frac{g_\psi}{h_\psi}, h_\psi = \begin{cases} \xi\chi(\gamma)\gamma - 1 & \text{if } \psi = \omega^{-1}\psi_\xi \text{ for some } p\text{-power root of 1 } \xi \\ 1 & \text{otherwise} \end{cases}.$$
- (Algebraic side) Let
$$\mathrm{Sel}_\infty(\psi) = H^1_{\mathrm{nr}}(\mathbb{Q}, \Lambda^*_\psi(\psi\Psi^{-1})), X_\infty(\psi) = \mathrm{Sel}_\infty(\psi)^*,$$
$$\mathrm{Sel}(\psi\chi^{-k}) = H^1_{\mathrm{nr}}(\mathbb{Q}, F_\psi/\mathcal{O}_\psi(\psi\chi^{-k})), X(\psi\chi^{-k}) = \mathrm{Sel}(\psi\chi^{-k})^*.$$
Then, if $p \nmid \varphi(N_\psi)$, for any nonnegative integer $k \geq 0$,
$$\mathrm{Sel}(\psi\psi_\zeta^{-1}\omega^k\chi^{-k}) \xrightarrow{\sim} (\mathrm{Sel}_\infty(\psi) \otimes_{\mathcal{O}_\psi} \mathcal{O}_\psi[\zeta])[\gamma - \zeta\chi^k(\gamma)],$$
$$\frac{(X_\infty(\psi) \otimes_{\mathcal{O}_\psi} \mathcal{O}_\psi[\zeta])}{(\gamma - \zeta\chi^k(\gamma))(X_\infty(\psi) \otimes_{\mathcal{O}_\psi} \mathcal{O}_\psi[\zeta])} \xrightarrow{\sim} X(\psi\psi_\zeta^{-1}\omega^k\chi^{-k}),$$
unless $k = 0$ and $\psi|_{G_{\mathbb{Q}_p}} = \psi_\zeta|_{G_{\mathbb{Q}_p}}$; the maps are just natural maps all induced from $\mathcal{O}_\psi \hookrightarrow \Lambda_\psi$. If $k = 0, \psi\psi_\zeta^{-1}|_{G_{\mathbb{Q}_p}} = 1$, then there are dual exact sequences
$$0 \to \mathrm{Sel}(\psi\psi_\zeta^{-1}) \to \mathrm{Sel}_\infty(\psi)[\gamma - \zeta] \to F_\psi/\mathcal{O}_\psi \to 0,$$
$$0 \to \mathcal{O}_\psi \to \frac{X_\infty(\psi)}{(\gamma - \zeta)X_\infty(\psi)} \to X(\psi\psi_\zeta^{-1}) \to 0.$$
- Furthermore, we have seen that $X_\infty(\psi)$ is a finitely generated torsion Λ_ψ-module, which has no finite order nontrivial Λ_ψ-submodule if $p \nmid \varphi(N_\psi)$. Thus we can use structure theory of finitely generated Λ_ψ-modules.
- The Iwasawa Main Conjecture in this setting is then $(g_{\psi^{-1}}) = \mathrm{Ch}(X_\infty(\psi))$.

2. Reduction: one divisibility is enough

Although the IMC is about an equality of ideals, in this special case of GL_1, one only needs to prove that $(g_{\psi^{-1}})$ divides $\mathrm{Ch}(X_\infty(\psi))$ thanks to the following proposition.

Proposition 2.1. *Let $K = \mathbb{Q}(\mu_{N_\psi})$. Then, two $\Lambda_\mathcal{O} = \Lambda \otimes_{\mathbb{Z}_p} \mathcal{O}$-modules*
$$I^-_{\mathrm{alg}}(K) := \prod_{\psi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})}, \psi \text{ odd}} \mathrm{Ch}(X_\infty(\psi)), I^-_{\mathrm{an}}(K) := \left(\prod_{\psi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})}, \psi \text{ odd}} g_\psi \right),$$
have the same μ and λ-invariants, where $\mathcal{O}$ is the ring of integers of big enough finite extension of $\mathbb{Q}_p$ (e.g. containing all $\mathbb{Z}_p[\psi]$'s for ψ's appearing in the product).

Remark 2.1. Beyond GL_1, one really needs to show both sides of divisibilities.

Proof that this implies that one divisibility is enough. This is basically because λ, μ-invariants are additive. We want to prove that for every height 1 prime $\mathfrak{p} \subset \Lambda_\psi$, $\mathrm{ord}_\mathfrak{p}(g_{\psi^{-1}}) = \mathrm{ord}_\mathfrak{p}\,\mathrm{Ch}(X_\infty(\psi))$ ($\because$ associated primes of normal domains are height 1 primes, and primary decomposition). Note that $\mathfrak{p}$ is principal $\mathfrak{p} = (f_\mathfrak{p})$, and for any $f \in \Lambda_\mathcal{O}$, $\sum_\mathfrak{p} \lambda(f_\mathfrak{p})\,\mathrm{ord}_\mathfrak{p}(f) = \lambda(f)$ and similarly for μ. As each $X_\infty(\psi)$ is not pseudo-null (e.g. interpolation property) it has at least one nonvanishing μ

or λ-invariant. So any $\mathrm{ord}_{\mathfrak{p}}(g_{\psi^{-1}}) < \mathrm{ord}_{\mathfrak{p}}\,\mathrm{Ch}(X_\infty(\psi))$ will be seen in one of strict inequalities of λ, μ. □

Proof of Proposition 2.1. What are μ and λ-invariants? Recall we had

$$\#M/\frac{\omega_n}{\omega_{n_0}}M = p^{\mu(M)fp^n+\lambda(M)ef(n-n_0)+O(1)},$$

for e, f ramification degree/residue class degree of $\mathcal{O}/\mathbb{Z}_p$. Eventually everything will follow from analytic class formula and interpolation properties.

Step 1. Analytic side: analytic class number formula.

Let $\mathcal{O}_n = \mathcal{O}[\mu_{p^n}]$. Then the polynomials $X^{p^n}-1$ split completely in $\mathcal{O}_n$, so that, for any $n \geq n_0$,

$$\begin{aligned}\Lambda_{\mathcal{O}_n}/(\frac{\omega_n}{\omega_{n_0}}, I^-_{\mathrm{an}}(K)) &= \prod_{\zeta^{p^n}=1,\zeta^{p^{n_0}}\neq 1} \Lambda_{\mathcal{O}_n}/(\gamma-\zeta, I^-_{\mathrm{an}}(K)) \\ &= \prod_{\zeta^{p^n}=1,\zeta^{p^{n_0}}\neq 1} \prod_{\psi\in\widehat{\mathrm{Gal}(K/\mathbb{Q})},\psi \text{ odd}} \mathcal{O}_n/\phi_{0,\zeta}(g_\psi),\end{aligned}$$

where $\omega_n = \gamma^{p^n}-1$ as before. Recall that the analytic class number formula says that, for any cyclotomic field K', $(h^-_{K'}) = (w_{K'}\prod_{\psi\in\widehat{\mathrm{Gal}(K'/\mathbb{Q})},\psi \text{ odd}} L(0,\psi))$ as fractional $\mathbb{Z}_p$-ideals (i.e. ord_p of both sides are the same), where h^- means the order of the minus part of the (p-part of, b/c we are just interested in ord_p) class group, and $w_{K'}$ is the order of the unit group.

Also $\phi_{0,\zeta}(g_\psi)$ interpolates $L(0,\psi\psi_\zeta)$ (up to an Euler factor). Let $K_n = K\mathbb{Q}_n = \mathbb{Q}(\mu_{p^n N_\psi^{(p)}})$, where $N_\psi = p^r N$ where N is the prime-to-p factor (we pick n and n_0 large enough). Then $\{\psi\psi_\zeta \mid \psi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})}, \psi \text{ odd}, \zeta^{p^n}=1, \zeta^{p^{n_0}}\neq 1\}$ counted with multiplicity is consisted of p^r copies of $\{\psi \mid \psi \in \widehat{\mathrm{Gal}(K_n/\mathbb{Q})}$ which does not factor through $\mathrm{Gal}(K_{n_0}/\mathbb{Q})\}$. The effects of Euler factors and w_K also cancel out so that we eventually get

$$\Lambda_{\mathcal{O}_n}/(\frac{\omega_n}{\omega_{n_0}}, I^-_{\mathrm{an}}(K)) = \mathcal{O}_n/((h^-_n/h^-_{n_0})^{p^r}),$$

where $h^-_n = h^-_{K_n}$, so that

$$\#\Lambda_{\mathcal{O}_n}/(\frac{\omega_n}{\omega_{n_0}}, I^-_{\mathrm{an}}(K)) = (h^-_n/h^-_{n_0})^{p^r[\mathcal{O}_n:\mathbb{Z}_p]},$$

or going back to $\mathcal{O}$,

$$\#\Lambda_{\mathcal{O}}/(\frac{\omega_n}{\omega_{n_0}}, I^-_{\mathrm{an}}(K)) = (h^-_n/h^-_{n_0})^{p^r[\mathcal{O}:\mathbb{Z}_p]}.$$

Step 2. Algebraic side: p-adic Selmer group and class group.

For the algebraic side, one could imagine $I^-_{\mathrm{alg}}(K)$ being the characteristic ideal of some $\Lambda_{\mathcal{O}}$-module, most likely the Pontryagin dual of minus part of unramified Galois cohomology of $\Lambda^*_{\mathcal{O}}(\Psi^{-1})$, and this is really the case ($I^-_{\mathrm{alg}}(K) = \mathrm{Ch}((H^1_{\mathrm{nr}}(K, \Lambda^*_{\mathcal{O}}(\Psi^{-1}))^-)^*)$). To be more precise,

$$\prod_{\psi\in\widehat{\mathrm{Gal}(K/\mathbb{Q})}} \mathcal{O}(\psi) \to \mathrm{Hom}_{\mathcal{O}}(\mathcal{O}[\mathrm{Gal}(K/\mathbb{Q})], \mathcal{O}),$$

sending $(a_\psi) \mapsto (g \mapsto \sum a_\psi \psi^{-1}(g))$, is an injection with finite order cokernel, so

$$\prod_{\psi\in\widehat{\mathrm{Gal}(K/\mathbb{Q})}} H^1_{\mathrm{nr}}(\mathbb{Q}, \Lambda^*_{\mathcal{O}}(\psi^{-1}\Psi^{-1})) \to H^1_{\mathrm{nr}}(\mathbb{Q}, \mathrm{Hom}_{\mathcal{O}}(\mathcal{O}[\mathrm{Gal}(K/\mathbb{Q})], \Lambda^*_{\mathcal{O}}(\Psi^{-1}))) \cong H^1_{\mathrm{nr}}(K, \Lambda^*_{\mathcal{O}}(\Psi^{-1})),$$

has finite order kernel/cokernel, where the last identification is Shapiro's lemma. This is $\mathrm{Gal}(K/\mathbb{Q})$-equivariant, so restricting to the minus part and taking Pontryagin duals,

$$X_\infty(K)^- := (H^1_{\mathrm{nr}}(K, \Lambda^*_{\mathcal{O}}(\Psi^{-1}))^-)^*$$

is pseudo isomorphic to $\prod_{\psi \in \widehat{\mathrm{Gal}(K/\mathbb{Q})}, \psi \text{ odd}} X_\infty(\psi)$.

On the other hand, restricting cocycle in $H^1_{\mathrm{nr}}(K, \Lambda^*_{\mathcal{O}}(\Psi^{-1}))$ to G_{K_∞} gives a $\Gamma_K = \mathrm{Gal}(K_\infty/K)$-homomorphism ($\Gamma_K$ acts by $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_r)$) $\mathrm{Gal}(E_\infty/K_\infty) \to \Lambda^*_{\mathcal{O}}(\Psi^{-1})$, where E_∞/K_∞ is the maximal pro-p abelian unramified extension. This is in fact an isomorphism by inflation-restriction

$$H^1_{\mathrm{nr}}(K, \Lambda^*_{\mathcal{O}}(\Psi^{-1})) \xrightarrow{\sim} \mathrm{Hom}_{\Gamma_K}(\mathrm{Gal}(E_\infty/K_\infty), \Lambda^*_{\mathcal{O}}(\Psi^{-1})),$$

and one can obviously take minus parts and take dual to get

$$\mathrm{Gal}(E_\infty/K_\infty)^{-,\iota} \otimes_{\mathbb{Z}_p[[\Gamma_K]]} \Lambda_{\mathcal{O}} \xrightarrow{\sim} X_\infty(K)^-,$$

where ι means Γ_K acts by inversion (i.e. g acts by g^{-1}). Now one could "imagine"

- $\mathrm{Gal}(E_\infty/K_\infty)/\omega_n \mathrm{Gal}(E_\infty/K_\infty) = \mathrm{Gal}(E_n/K_n) = p$-class group of K_n (because modding out by ω_n is something like picking up n-th level of the cyclotomic tower).
- So

  $$\#\Lambda_{\mathcal{O}}/(\frac{\omega_n}{\omega_{n_0}}, I^-_{\mathrm{alg}}(K)) = \#(X_\infty(K)^-/\frac{\omega_n}{\omega_{n_0}} X_\infty(K)^-) = (h^-_n/h^-_{n_0})^{p^r[\mathcal{O}:\mathbb{Z}_p]}$$

  ($p^r = \mathrm{Gal}(\mathbb{Q}_r/\mathbb{Q})$), so we have the same asymptotics for the both algebraic and analytic side.

This is almost true. What you need to know is that there is a finite index (thus pseudo-isomorphic) $\mathbb{Z}_p[[\Gamma_K]]$-submodule of $\mathrm{Gal}(E_\infty/K_\infty)$ that really picks up p-class group of K_n for n large enough. (By Iwasawa. Reference: [Was, Lemma 13.10]) □

3. Something that should become a proof of the Iwasawa Main Conjecture for $\mathbb{Q}$ (i.e. review of the proof of Converse to Herbrand)

Now one divisibility is enough, so we want to use the strategy of using Ribet's lemma to produce extensions. This will more or less go in the same way that we proved Converse to Herbrand. I will sketch what is a morally correct proof. **We change ψ^{-1} to ψ.**

(1) We want to relate g_ψ, p-adic L-function, to something likeEisenstein series (or more generally modular forms) with Λ_ψ coefficients. This is the case (Hida families).
(2) There is somehow the notion of Galois representation over Λ_ψ associated to such modular forms, and we have similar control on the shape of ordinary such. This is also true.
(3) Order of vanishing r of g_ψ, after localizing at $\mathfrak{p}$, means there is a $\mathfrak{p}^r$-congruence of Eisenstein series and cusp forms. This is not exactly true in this case though. This will be made more precise by introducing the Eisenstein ideal, which roughly measures the maximal possible congruence between cusp form and Eisenstein series.
(4) Now by following the exactly same argument we produce an indecomposable, reducible yet residually split extension

    $$0 \to M_2 \to M \to M_1 \to 0.$$

    M_2 is "$\mathbb{1}$" whereas M_1 is "$\psi\Psi$". So M defines a class in $H^1(\mathbb{Q}, M_2(\psi^{-1}\Psi^{-1}))$.
(5) Any Λ_ψ-homomorphism $\phi : M_2 \to \Lambda^*_\psi$ will give an unramified class in $H^1_{\mathrm{nr}}(\mathbb{Q}, \Lambda^*_\psi(\psi^{-1}\Psi^{-1}))$. This association $\mathrm{Hom}_{\Lambda_\psi}(M_2, \Lambda^*_\psi) \to H^1_{\mathrm{nr}}(\mathbb{Q}, \Lambda^*_\psi(\psi^{-1}\Psi^{-1}))$ is injective.

(6) Taking Pontryagin dual, we get a surjection $\mathrm{Sel}_\infty(\psi^{-1}) \to M_2$. Now fitting ideal argument gives

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}}(\mathrm{Ch}_\infty(\psi^{-1})) &= \mathrm{ord}_{\mathfrak{p}}(\mathrm{Sel}_\infty(\psi^{-1})) \\ &\geq \mathrm{ord}_{\mathfrak{p}}(\mathrm{Fitt}\, M_2)\end{aligned}$$

and $\mathrm{Fitt}\, M_2 \bmod \mathfrak{p}^r$ is zero because M_2 comes from faithful Galois module by reduction mod Eisenstein ideal.

4. Hida families

Now we explain ***Hida theory***, which will explain up to (2). No proofs will be given, one could consult [Hid1] or [Hid2].

The definition of modular forms with Λ_ψ-coefficients will be just formal q-expansion with coefficients in Λ_ψ such that its specialization at all arithmetic points $\phi_{k,\zeta}$, with sufficiently high weight k and ζ sufficiently close to 1, give q-expansions of a modular form of appropriate weight, level and Nebentype.

Definition 4.1 ($\mathbb{I}$-adic modular form)**.** *Let $\mathbb{I}$ be a finite complete local integral Λ_ψ-algebra. Then an $\mathbb{I}$-adic modular form is a formal q-expansion $\mathbb{f} = \sum a(n)q^n$ with $a(n) \in \mathbb{I}$ such that, for each $\phi : \mathbb{I} \to \overline{\mathbb{Q}}_p$ with $\phi|_{\Lambda_\psi} = \phi_{k,\zeta}$, with $k \gg 0$, and ζ primitive p^t-th root of unity with $t \gg 0$, the specialization*

$$\mathbb{f}_\phi := \sum \phi(a(n))q^n,$$

is the q-expansion of a modular form in $M_{k+1}(Np^{t+1}, \psi\psi_\zeta\omega^{-k}, \phi(\mathbb{I}))$ (where the last term is coefficient ring).

There are too many $\mathbb{I}$-adic modular forms. However, one maintains a good finiteness property one restricts attention to ***ordinary $\mathbb{I}$-adic forms*** (=Hida families), which just means $\mathbb{f}_\phi$ are ordinary (recall ordinary means $U_p = [\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}]$ has eigenvalue a p-unit (p-valuation zero)). Some relevant properties are following.

- For classical modular forms $M_k(\Gamma_1(Np^r), \mathcal{O})$, there is an idempotent in the Hecke algebra $\mathbb{T} \subset \mathrm{End}(M_k(\Gamma_1(Np^r), \mathcal{O}))$ called ***ordinary projector*** e_{ord} that picks exactly $M_k^{\mathrm{ord}}(\Gamma_1(Np^r), \mathcal{O})$. It can be defined as $\lim_{n\to\infty} U_p^{n!}$ (This is because U_p preserves p-integrality.). The same applies to cusp forms.
- The Hecke operators and U_p-operators on the level of q-expansions define an operator on $\mathbb{I}$-adic modular forms, and the same is true that $e = \lim_{n\to\infty} U_p^{n!}$ exists as an idempotent inside $\mathrm{End}_{\mathbb{I}}(\mathbb{M}(\psi, \mathbb{I}))$ which picks up exactly $\mathbb{M}^{\mathrm{ord}}(\psi, \mathbb{I})$. We can then define $\mathbb{T}^{\mathrm{ord}}(\psi, \mathbb{I}) \subset \mathrm{End}_{\mathbb{I}}(\mathbb{S}^{\mathrm{ord}}(\psi, \mathbb{I}))$ as $\mathbb{I}$-algebra generated by T_ℓ's, $\ell \nmid Np$, and U_ℓ's, $\ell | Np$. It is commutative, so one could naturally define the notion of eigenform.
- Now $\mathbb{T}^{\mathrm{ord}}(\psi, \mathbb{I}), \mathbb{M}^{\mathrm{ord}}(\psi, \mathbb{I}), \mathbb{S}^{\mathrm{ord}}(\psi, \mathbb{I})$ have important finiteness properties.
  (1) $\mathbb{M}^{\mathrm{ord}}(\psi, \mathbb{I})$ and $\mathbb{S}^{\mathrm{ord}}(\psi, \mathbb{I})$ are **finite** $\mathbb{I}$-algebras. This can be translated into that for classical modular forms, $\mathrm{rank}_{\mathrm{coeff}} M_k^{\mathrm{ord}}(\mathrm{lvl}, \mathrm{char} \cdot \omega^{-k}, \mathrm{coeff})$ is **independent of k** for k large enough (boundedness by Eichler-Shimura (relating to cohomology of modular curves) + cohomological argument to get upper bdd $eH^1(X(\mathrm{lvl}), \mathbb{F}_p)$, so that if $\mathbb{M}^{\mathrm{ord}}$ is not finite, then it will give blow-up of rank in classical modular forms).
  (2) (Irrelevant) Every classical p-stabilized ordinary eigenform lives in a unique Hida family up to Galois conjugacy and change of coefficient fields. Conversely, $\mathbb{M}^{\mathrm{ord}}(\psi, \mathbb{I})$ specialized at $\phi : \mathbb{I} \to \overline{\mathbb{Q}}_p$ whose restriction to Λ_ψ is arithmetic is really isomorphic to M_{k+1} with appropriate level, Nebentype...

(3) $\mathbb{T}^{\mathrm{ord}}(\psi,\mathbb{I})$ is a **finite torsion-free reduced $\mathbb{I}$-algebra**. Torsion-free b/c of how it is constructed, finite b/c $\mathbb{S}^{\mathrm{ord}}$ is finite, and reduced b/c our definition of $\mathbb{I}$-adic modular form $\mathbb{f}$ forces to be N-new (b/c ψ has primitive tame level N). In general the new quotient will be the one that's reduced.

- Obviously for the quotient $\mathbb{J}$ of $\mathbb{T}^{\mathrm{ord}}(\psi,\mathbb{I})$ by a minimal prime, the quotient map $\mathbb{T}^{\mathrm{ord}}(\psi,\mathbb{I})\to\mathbb{J}$ will give an eigenvalue of ordinary $\mathbb{J}$-adic eigenform $\mathbb{f}_{\mathbb{J}}$ of character ψ.
- Now another important feature is that there should be an associated Galois representation. This is summarized in the following theorem.

Theorem 4.1 (Hida, Wiles). *Let $\mathbb{f}$ be a normalized cuspidal $\mathbb{I}$-adic eigenform with character ψ. Then, there is a Galois representation $\rho_{\mathbb{f}}: G_{\mathbb{Q}}\to \mathrm{GL}_2(V)$ for a 2-dimensional $\mathrm{Frac}(\mathbb{I})$-vector space V such that*

(1) $\rho_{\mathbb{f}}$ is continuous with respect to the $\mathfrak{m}_{\mathbb{I}}$-adic topology.
(2) $\rho_{\mathbb{f}}$ is irreducible.
(3) $\det\rho_{\mathbb{f}}=\psi\Psi$.
(4) $\rho_{\mathbb{f}}$ is unramified away from Np, and $\operatorname{tr}\rho_{\mathbb{f}}(\mathrm{Frob}_\ell)=a(\ell)$ for $\ell\not| Np$.
(5) For $\ell\mid N$, if $a(\ell)\neq 0$, then

$$\rho_{\mathbb{f}}|_{G_{\mathbb{Q}_\ell}}\cong\begin{pmatrix}\alpha_\ell^{-1}\psi\Psi & 0\\ 0 & \alpha_\ell\end{pmatrix},\alpha_\ell|_{I_\ell}=1,\alpha_\ell(\mathrm{Frob}_\ell)=a(\ell),$$

(6) If $\mathbb{f}$ is ordinary, then

$$\rho_{\mathbb{f}}|_{G_{\mathbb{Q}_p}}\cong\begin{pmatrix}\alpha_p^{-1}\psi\Psi & *\\ 0 & \alpha_p\end{pmatrix},\alpha_p|_{I_p}=1,\alpha_p(\mathrm{Frob}_p)=a(p).$$

This really uses pseudo-representations. References: [Hid1], [Wil1].

One could imagine that, by mimicking the construction of Eisenstein series for Converse to Herbrand case,

$$\mathbb{E}_\psi=\frac{1}{2}g_\psi+h_\psi\sum_{n=1}^{\infty}\left(\sum_{d|n,(d,Np)=1}\prod_{\ell^e\| d}\psi\Psi(\mathrm{Frob}_\ell^e)\right)q^n,$$

is an ordinary Λ_ψ-adic modular form which specializes to (denominator of p-adic L-function times) ordinary Eisenstein series. Indeed, at arithmetic point $\phi_{k,\zeta}$,

$$\phi_{k,\zeta}(\mathbb{E}_\psi)=\phi_{k,\zeta}(h_\psi)E^{\mathrm{ord}}_{k+1,\psi\psi_\zeta\omega^{-k}}(z),$$

where

$$E^{\mathrm{ord}}_{k+1,\psi\psi_\zeta\omega^{-k}}(z)=\frac{1}{2}L(-k,\psi\psi_\zeta\omega^{-k})+\sum_{n=1}^{\infty}\sum_{d|n,(d,Np)=1}\psi\psi_\zeta\omega^{-k}(d)d^kq^n.$$

5. Constructing Eisenstein congruence

Now we start proving the Iwasawa Main Conjecture for $\mathbb{Q}$. Pick a height 1 prime $\mathfrak{p}\subset\Lambda_\psi$. Following the blueprint, step (3) requires us to make an Eisenstein congruence. We make this in a mathematical statement. For notational convenience, let $\mathbb{T}_\psi=\mathbb{T}^{\mathrm{ord}}(\psi,\Lambda_\psi)$.

Definition 5.1 (Eisenstein ideal). *The ideal $I_\psi=\langle\{T_\ell-1-\psi\Psi(\mathrm{Frob}_\ell)\}_{\ell\not| Np},\{U_\ell-1\}_{\ell|Np}\rangle\subset\mathbb{T}_\psi$ is called the Eisenstein ideal.*

As $\mathbb{T}_\psi$ is generated by Hecke and U_p-operators, the structure map $\Lambda_\psi\to\mathbb{T}_\psi/I_\psi$ is surjective. Let the kernel be denoted as J_ψ. Then what we want to prove is that

$$\mathrm{ord}_{\mathfrak{p}}(J_\psi)\geq\mathrm{ord}_{\mathfrak{p}}(g_\psi). \tag{5.1}$$

Naively, if there is an ordinary cusp form congruent mod $\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(g_\psi)}$ to $\mathbb{E}_\psi$, then

$$\mathbb{T}_{\psi,\mathfrak{p}} \to \Lambda_{\psi,\mathfrak{p}}/\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(g_\psi)}\Lambda_{\psi,\mathfrak{p}},$$
$$T_\ell \mapsto 1 + \psi\Psi(\mathrm{Frob}_\ell), U_\ell \mapsto 1,$$

will be a surjective $\Lambda_{\psi,\mathfrak{p}}$-homomorphism whose kernel contains $I_\psi\mathbb{T}_{\psi,\mathfrak{p}}$, proving (5.1). But the Converse to Herbrand case used that there is only 1 cusp in level 1, and this cannot be used here. So we need something more.

- **Step 0. Trivial cases and exceptional primes.** Indeed if $\psi = \omega^{-1}\psi_\xi$ so that p-adic L-function has a pole, then we know it is a simple pole, so g_ψ is a unit, so there is nothing to prove. We can exclude this case. More generally we can assume that $f_{\mathfrak{p}} \mid g_\psi$, where $\mathfrak{p} = (f_{\mathfrak{p}})$. Even after this we have to exclude certain primes, ***exceptional primes***, namely those $\mathfrak{p}$ such that either p is in $\mathfrak{p}$ or $\psi\Psi|_{G_{\mathbb{Q}_p}} \equiv 1 (\mathrm{mod}\,\mathfrak{p})$. We will not say anything further about exceptional primes; it is less relevant to the theme of the seminar. (For those containing p one could use the vanishing of μ-invariant of Ferraro-Washington to deduce that $\mathrm{ord}_{\mathfrak{p}}(g_\psi) = 0$. For other exceptional primes Grenberg and Ferraro proved that both sides are 1. For IMC for general totally real fields, Wiles uses a different argument.)
- **Step 1. Making $a_0 = 0$.** Note that by Weierstrass preparation theorem, every $f \in \Lambda_\psi$ has a unique power series expansion in $T := \gamma - 1$ with coefficients in $\mathcal{O}_\psi$. In particular, for $\mathbb{f}$ a Λ_ψ-adic modular form, and $g(T) = \zeta(1+T)^m - 1$ for some p-power root of 1 ζ and $m \geq 0$ integer, the formal q-expansion $\mathbb{f}(g(T))$ is also an $\mathbb{I}$-adic modular form for some appropriate $\mathbb{I}$ (containing Λ_ψ and ζ).

  Now $\zeta = \chi^{-(p-1)}(\gamma)$ is some p-power root of unity. Then there certainly exists $N \gg 0$ such that $f_{\mathfrak{p}} \not| g_\psi(\zeta^N(1+T) - 1)$. Then

  $$\mathscr{G}_\psi := G_{N(p-1)}\mathbb{E}_\psi(\zeta^N(1+T) - 1),$$

  is a Λ_ψ-adic modular form with $a_0(\mathscr{G}_\psi) = g_\psi(\zeta^N(1+T) - 1)$, and

  $$\mathscr{G}'_\psi := e_{\mathrm{ord}}\mathscr{G}_\psi,$$

  is an ordinary Λ_ψ-adic modular form, with $a_0(\mathscr{G}'_\psi) = g_\psi(\zeta^N(1+T) - 1)$, a $\mathfrak{p}$-unit. Here G_k is the usual constant term 1 classical modular form formed as a product of Eisenstein series, i.e. $G_k(z) = (240E_4(z))^a(-504E_6(z))^b$ for $4a + 6b = k$. Now one can use this to produce

  $$\mathscr{F}_\psi := g_\psi(\zeta^N(\gamma)(1+T) - 1)\mathbb{E}_\psi - g_\psi\mathscr{G}'_\psi,$$

  an ordinary Λ_ψ-adic modular form with $a_0(\mathscr{F}) = 0$! This is up to $\mathfrak{p}$-unit congruent to $\mathbb{E}_\psi$ mod $\mathfrak{p}^r$. (Some explanation on the construction: you multiply with G_{k_0} because our definition of Hida family asserts that specialization at weight k point gives weight $k+1$ modular form, so you have to recover weight; you require multiples of $(p-1)$ so that there is no effect mod p to make sure that the ordinary projector does not eliminate everything but constant term and/or $\mathscr{F}$ is not a constant.)
- **Step 2. Producing an ordinary cusp form.** Now how about vanishing at other cusps? There is the following cute trick.

  Lemma 5.1. *Let $\mathrm{g} \in \mathbb{M}^{\mathrm{ord}}(\psi, \Lambda_\psi)$ with $a_0(\mathrm{g}) = 0$. Then,*

  $$w\mathrm{g} := \prod_{\ell|N} U_\ell(U_\ell^{\varphi(N_\psi)} - \Psi(\mathrm{Frob}_\ell)^{\varphi(N_\psi)})\mathrm{g},$$

  is a cusp form!

  Proof. One checks this by specializing at each arithmetic point and see that all ordinary Eisenstein series showing up in the space of ordinary modular forms vanish by this Hecke

operator. More specifically, if $E_{\chi_1,\chi_2} = 1 + \sum_{n\geq 1}\sum_{d|n}\chi_1(n/d)\chi_2(d)d^k q^n$, with $\chi_1\chi_2 = \psi\psi_\zeta\omega^{-k}$, then

- p does not divide conductor of χ_1 as E_{χ_1,χ_2} has to be ordinary.
- $\ell \neq p$ does not divide both conductors of χ_1, χ_2, because you have U_ℓ in the operator to make sure $a_\ell \neq 0$.
- If $\ell \neq p$ divides the conductor of χ_1 but not that of χ_2, then $U_\ell E_{\chi_1,\chi_2} = \ell^k\chi_2(\ell)E_{\chi_1,\chi_2}$, whereas $\Psi_{k,\zeta} = \psi_\zeta\omega^{-k}\chi^k$. Note $\chi(\mathrm{Frob}_\ell) = \ell$, $\psi_\zeta(\mathrm{Frob}_\ell) = \chi_2(\ell)$ and raising power to $\varphi(N_\psi)$ eliminates ambiguity coming from both ω and ψ.
- If $\ell = 1$, then this does not show up because we had $a_0 = 0$ to start with.

□

- **Step 3. Going back.** Note that $w\mathscr{F}_\psi$ is not literally congruent to $\mathbb{E}_\psi \bmod \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(g_\psi)}$. Modulo J_ψ, it is congruent to $\prod_{\ell|N}(1-\Psi(\mathrm{Frob}_\ell)^{\varphi(N_\psi)})g_\psi(\zeta^N(\gamma)(1+T)-1)\mathbb{E}_\psi$. We know $g_\psi(\zeta^N(\gamma)(1+T)-1)$ is a $\mathfrak{p}$-unit so this not a problem. To make sure that we can invert $\prod_{\ell|N}(1-\Psi(\mathrm{Frob}_\ell)^{\varphi(N_\psi)})$, assume $1-\Psi(\mathrm{Frob}_\ell)^{\varphi(N_\psi)} \in \mathfrak{p}$. Then, $\Psi(\gamma) \bmod \mathfrak{p}$ is a root of unity ξ. Thus $\mathfrak{p} \mid g_\psi$ implies, by interpolation, $L^{\{p\}}(0, \psi\psi_\xi^{-1}) = 0$, which means $\psi\psi_\xi^{-1} = 1$, or $\psi\Psi|_{G_{\mathbb{Q}_p}} \equiv 1 (\mathrm{mod}\,\mathfrak{p})$, which is a contradiction as we have already excluded exceptional primes. So we can safely invert extra factors to get a desired congruence.

6. Use of Ribet's lemma, finishing up the proof

Now we want to prove that for non-exceptional primes $\mathfrak{p}$,

$$\mathrm{ord}_\mathfrak{p}(\mathrm{CH}_\infty(\psi)) \geq \mathrm{ord}_\mathfrak{p}(J_\psi).$$

This will be established by Ribet's lemma argument as before. We can suppose $t := \mathrm{ord}_\mathfrak{p}(J_\psi) > 0$.

- **Step 1. Start with ordinary Galois representation.** We start exactly as in the proof of Converse to Herbrand. Let $\mathfrak{p}' \subset \mathbb{T}_\psi$ be the unique height one prime containing $(I_\psi, \mathfrak{p})$ by Going-Down ($\mathbb{T}_\psi/\Lambda_\psi$ is flat). Let $\mathfrak{q}_1, \cdots, \mathfrak{q}_m$ be the minimal prime ideals contained in $\mathfrak{p}'$. Let $\mathbb{J}_i = \mathbb{T}_\psi/\mathfrak{q}_i$, and $A = \mathbb{T}_\psi/\cap_{i=1}^m \mathfrak{q}_i$. Let $K = \mathrm{Frac}(A) = A \otimes_{\Lambda_\psi} \mathrm{Frac}(\Lambda_\psi) = \prod \mathrm{Frac}(\mathbb{J}_i)$, $\rho_i = \rho_{\mathbb{J}_i}$. As these specialize to newforms at primes away from p, these are all pairwise non-isomorphic. Let $V = \oplus V_{\mathbb{J}_i}$, $\rho = \oplus\rho_{\mathbb{J}_i}$. This is then a continuous free two-dimensional K-representation of $G_\mathbb{Q}$ on V. This is the ordinary Galois representation we will start with. In particular, we have following properties.
  (1) $\mathrm{tr}\,\rho$ is A-valued, because all $\mathrm{tr}\,\rho(\mathrm{Frob}_\ell)$ for $\ell \not| Np$ is just $T_\ell \in A$, so by continuity everything is A-valued. In particular, $\mathrm{tr}\,\rho = 1 + \psi\Psi (\mathrm{mod}\, I_\psi A)$ (this is also because $T_\ell = 1 + \psi\Psi(\mathrm{Frob}_\ell)$ for Frob_ℓ's).
  (2) As $\mathfrak{p}$ is nonexceptional, we can pick $\sigma_0 \in G_{\mathbb{Q}_p}$ such that $\psi\Psi(\sigma_0) - 1 \notin \mathfrak{p}$.
  (3) By ordinarity we start with a basis such that $\rho|_{G_{\mathbb{Q}_p}} = \begin{pmatrix}\alpha^{-1}\psi\Psi & * \\ 0 & \alpha\end{pmatrix}$, where $\alpha|_{I_p} = 1$, $\alpha(\mathrm{Frob}_p) = U_p$. We do one further elementary row operation to diagonalize $\rho(\sigma_0) = \begin{pmatrix}\alpha^{-1}\psi\Psi(\sigma_0) & 0 \\ 0 & \alpha(\sigma_0)\end{pmatrix}$.
- **Step 2. Construct a nonsplit extension over $A_\mathfrak{p}$ first.** Note that as $\alpha(\sigma_0) \equiv 1 (\mathrm{mod}\,\mathfrak{p})$ and not literally a unit, we cannot simply invert as in the case of proof of Converse to Herbrand. Rather we have to allow inverting something not in $\mathfrak{p}$, namely work over $A_\mathfrak{p}$, as

$$r := \alpha^{-1}\psi\Psi(\sigma_0) - \alpha(\sigma_0) \notin \mathfrak{p} (\because \alpha \equiv 1 (\mathrm{mod}\,\mathfrak{p})).$$

Writing $\rho(\sigma) = \begin{pmatrix}a_\sigma & b_\sigma \\ c_\sigma & d_\sigma\end{pmatrix} \in M_2(K), \sigma \in K[G_\mathbb{Q}]$, we can argue similarly as before so that

(1) $ra_\sigma, rd_\sigma, r^2 b_\sigma c_\tau \in A$ for all $\sigma, \tau \in A[G_{\mathbb{Q}}]$, and

$$ra_\sigma \equiv \psi\Psi(\sigma_0\sigma), -rd_\sigma \equiv 1(\sigma_0\sigma), r^2 b_\sigma c_\tau \equiv 0 (\mathrm{mod}\, I_\psi A).$$

This is because if we let

$$\delta_1 = \sigma_0 - \alpha(\sigma_0), \delta_2 = \sigma_0 - \alpha^{-1}\psi\Psi(\sigma_0) \in A[G_{\mathbb{Q}}],$$

then

$$ra_\sigma = \mathrm{Tr}\,\rho(\delta_1\sigma) \equiv \psi\Psi(\sigma_0\sigma), -rd_\sigma = \mathrm{Tr}\,\rho(\delta_2\sigma) \equiv 1(\sigma_0\sigma) (\mathrm{mod}\, I_\psi A).$$

(2) $\mathcal{C} := \{c_\sigma \mid \sigma \in A[G_{\mathbb{Q}}]\}$ is a finite faithful A-module. This is (a) finite because ρ is continuous and $G_{\mathbb{Q}}$ is compact, and (b) faithful because $\rho_{\mathbb{J}_i}$'s are all irreducible and distinct. Namely, let $\mathcal{M} := A_{\mathfrak{p}} v_1 \oplus \mathcal{C}_P v_2 \subset V$ be a $G_{\mathbb{Q}}$-stable lattice. Then, $\mathcal{M} \otimes_{\Lambda_{\psi,\mathfrak{p}}} F_\psi$ is a nonzero $K[G_{\mathbb{Q}}]$-stable submodule of V, projecting onto each $V_{\mathbb{J}_i}$, so $\mathcal{M} \otimes_{\Lambda_{\psi,\mathfrak{p}}} F_\psi = V$, implying $\mathcal{C}_{\mathfrak{p}} \otimes_{\Lambda_{\psi,\mathfrak{p}}} F_\psi = K$.

(3) $c_\sigma = 0$ for $\sigma \in I_p$. This is because $\mathcal{M}_1 := A_{\mathfrak{p}} v_1$ is I_p-stable.

Before manipulating we note

$$\begin{aligned} A_{\mathfrak{p}}/I_\psi A_{\mathfrak{p}} &= A_{\mathfrak{p}'}/I_\psi A_{\mathfrak{p}'} \\ &= \mathbb{T}_{\psi,\mathfrak{p}'}/I_\psi \mathbb{T}_{\psi,\mathfrak{p}'} (\because A_{\mathfrak{p}'} = \mathbb{T}_{\psi,\mathfrak{p}'}) \\ &= \Lambda_{\psi,\mathfrak{p}}/J_\psi \Lambda_{\psi,\mathfrak{p}}. \end{aligned}$$

Now letting $\mathcal{M}_2 := \mathcal{C}_{\mathfrak{p}} v_2$, then

$$0 \to \overline{\mathcal{M}_2} \to \overline{\mathcal{M}} \to \overline{\mathcal{M}_1} \to 0,$$

is a nonsplit extension of $A_{\mathfrak{p}}/I_\psi A_{\mathfrak{p}}[G_{\mathbb{Q}}] = \Lambda_{\psi,\mathfrak{p}}/J_\psi\Lambda_{\psi,\mathfrak{p}}[G_{\mathbb{Q}}]$-modules. This makes sense because

- for $c \in \mathcal{C}_{\mathfrak{p}}$, $\rho(\sigma)cv_2 = b_\sigma c v_1 \oplus d_\sigma c v_2 \in cv_2 + I_\psi \mathcal{M}$, making $\overline{\mathcal{M}_2} = \mathcal{M}_2/I_\psi\mathcal{M}_2$ an $A_{\mathfrak{p}}[G_{\mathbb{Q}}]$-direct summand of $\overline{\mathcal{M}} = \mathcal{M}/I_\psi\mathcal{M}$ on which $G_{\mathbb{Q}}$ acts trivially,
- and the quotient $\overline{\mathcal{M}_1}$, which $\mathcal{M}_1$ surjects onto, is a rank 1 $A_{\mathfrak{p}}/I_\psi A_{\mathfrak{p}}$-module acted by $G_{\mathbb{Q}}$ via $\psi\Psi$.

Thus what we get is nonsplit (as $\overline{\mathcal{M}}$ is generated by v_1)

$$0 \to \overline{\mathcal{M}_2} \to \overline{\mathcal{M}} \to \Lambda_{\psi,\mathfrak{p}}/J_\psi\Lambda_{\psi,\mathfrak{p}}(\psi\Psi) \to 0.$$

This is split

- Over p because $\mathcal{M}_1$ is I_p-stable.
- Over $\ell \mid N$ because of property (5) of associated Galois representation, so that I_ℓ-action factors through its image in $\mathrm{Gal}(\mathbb{Q}(\mu_{N_\psi})/\mathbb{Q})$.
- Over all other primes as for those primes ρ_i's are unramified.

- **Step 3. Make it over A.** Now just take $A[G_{\mathbb{Q}}]$-submodule $\mathfrak{M}$ generated by v_1 of $\overline{\mathcal{M}}$ and transfer things. This is a finite Λ_ψ-module, and restricting the whole picture to $\mathfrak{M}$, we get $0 \neq [\mathfrak{M}] \in H^1(\mathbb{Q}, \mathfrak{M}_2(\psi^{-1}\Psi^{-1}))$; it is nonzero because it is nonsplit when localized to $\mathfrak{p}$. Note here $\mathfrak{M}_2 = \mathfrak{M} \cap \overline{\mathcal{M}_2}$, and here again $G_{\mathbb{Q}}$ acts trivially. We are not quite sure if $[\mathfrak{M}]$ is an unramified class, but we know it is unramified almost everywhere, and $r_1[\mathfrak{M}]$ becomes unramified everywhere for some $r_1 \in \Lambda_\psi - \mathfrak{p}$. Now we apply the same idea; for $\phi \in \mathrm{Hom}_{\Lambda_\psi}(\mathfrak{M}_2, \Lambda_\psi^*)$, we send this class via $H^1(\mathbb{Q}, \mathfrak{M}(\psi^{-1}\Psi^{-1})) \to H^1(\mathbb{Q}, \Lambda_\psi^*(\psi^{-1}\Psi^{-1}))$. This gives a map

$$\theta : \mathrm{Hom}_{\Lambda_\psi}(\mathfrak{M}_2, \Lambda_\psi^*) \to H^1(\mathbb{Q}, \Lambda_\psi^*(\psi^{-1}\Psi^{-1})).$$

What we have realized above is that θ localized at $\mathfrak{p}$ is sent to the Selmer group. Thus to apply the Fitting ideal argument, we would only need to show that $\theta_{\mathfrak{p}}$ is injective (or equivalently $\theta_{\mathfrak{p}}^*$ is surjective).

Let $\mathfrak{K} = \ker\theta$, $\mathfrak{M}_2' = \cap_{\phi\in\mathfrak{K}}\ker\phi$. For a finite set $S \subset \mathfrak{K}$, we define $\mathfrak{M}_S = \cap_{\phi\in S}\ker\phi$, which is of finite index in $\mathfrak{M}_2$. Let $H_S = H^1(\mathbb{Q}, \mathfrak{M}_2/\mathfrak{M}_S(\psi^{-1}\Psi^{-1}))$. Note that there is a natural inclusion $\mathfrak{M}_2/\mathfrak{M}_S \hookrightarrow \prod_{\phi\in S}\Lambda_\psi^*$ given by $m \mapsto (\phi(m))_{m\in S}$. As $\phi \in \ker\theta$, the class $[\mathfrak{M}]$, sent to H_S, is in the kernel of $H_S \to \prod_{\phi\in S} H^1(\mathbb{Q}, \Lambda_\psi^*(\psi^{-1}\Psi^{-1}))$. Now the long exact sequence

$$0 \to H^0(\mathbb{Q}, \mathfrak{M}_2/\mathfrak{M}_S(\psi^{-1}\Psi^{-1})) \to H^0(\mathbb{Q}, \prod_{\phi\in S}\Lambda_\psi^*(\psi^{-1}\Psi^{-1})) \to H^0(\mathbb{Q}, \prod_{\phi\in S}\Lambda_\psi^*/(\mathfrak{M}_2/\mathfrak{M}_S)(\psi^{-1}\Psi^{-1}))$$
$$\to H^1(\mathbb{Q}, \mathfrak{M}_2/\mathfrak{M}_S(\psi^{-1}\Psi^{-1})) \to H^1(\mathbb{Q}, \prod_{\phi\in S}\Lambda_\psi^*(\psi^{-1}\Psi^{-1})),$$

shows that $[\mathfrak{M}] \in H_S$ is in the quotient of $\prod_{\phi\in S}\Lambda_\psi^*(\psi^{-1}\Psi^{-1}))^{G_\mathbb{Q}}$. On the other hand, each $\Lambda^*(\psi^{-1}\Psi^{-1})^{G_\mathbb{Q}}$ is annihilated by $r_2 := \psi\Psi(\sigma_0) - 1 \notin \mathfrak{p}$. Thus, $r_2[\mathfrak{M}] = 0$ in H_S. Taking inverse limit, we get $r_2[\mathfrak{M}] = 0$ as elements in $H^1(\mathbb{Q}, \mathfrak{M}_2/\mathfrak{M}_2'(\psi^{-1}\Psi^{-1}))$. This implies that $\mathfrak{M}_{2,\mathfrak{p}} = \mathfrak{M}_{2,\mathfrak{p}}'$, so $\theta_\mathfrak{p}$ is injective.

- **Step 4. Fitting ideal time.** Now we have the same argument left. Namely,

$$\begin{aligned}\mathrm{ord}_\mathfrak{p}(\mathrm{Ch}_\infty(\psi^{-1})) &= \mathrm{ord}_\mathfrak{p}(\mathrm{Ch}_\infty(\psi^{-1})_\mathfrak{p}) \\ &= \mathrm{ord}_\mathfrak{p}(\mathrm{Fitt}_{\Lambda_{\psi,\mathfrak{p}}}\Lambda_{\psi,\mathfrak{p}}/\mathrm{Ch}_\infty(\psi^{-1})_\mathfrak{p}) \\ &\geq \mathrm{ord}_\mathfrak{p}(\mathrm{Fitt}_{\Lambda_{\psi,\mathfrak{p}}}\mathfrak{M}_{2,\mathfrak{p}}) \\ &= \mathrm{ord}_\mathfrak{p}(\mathrm{Fitt}_{\Lambda_{\psi,\mathfrak{p}}}\overline{\mathcal{M}_2}),\end{aligned}$$

and

$$\begin{aligned}\mathrm{Fitt}_{\Lambda_{\psi,\mathfrak{p}}}\overline{\mathcal{M}_2}(\mathrm{mod}\, J_\psi\Lambda_{\psi,\mathfrak{p}}) &= \mathrm{Fitt}_{\Lambda_{\psi,\mathfrak{p}}/J_\psi\Lambda_{\psi,\mathfrak{p}}}\overline{\mathcal{M}_2} \\ &= \mathrm{Fitt}_{A_\mathfrak{p}/I_\psi A_\mathfrak{p}}\overline{\mathcal{M}_2} \\ &= \mathrm{Fitt}_{A_\mathfrak{p}}\overline{\mathcal{M}_2}(\mathrm{mod}\, I_\psi A_\mathfrak{p}) \\ &= \mathrm{Fitt}_{A_\mathfrak{p}}\mathcal{M}_2(\mathrm{mod}\, I_\psi A_\mathfrak{p}) = 0,\end{aligned}$$

which is because $\mathcal{M}_2$ is a faithful $A_\mathfrak{p}$-module. This finishes the proof.

Remark 6.1. Unlike $\overline{\mathcal{M}_1}$, we do not know if $\overline{\mathcal{M}_2}$ is free of rank 1 over $\Lambda_{\psi,\mathfrak{p}}/J_\psi\Lambda_{\psi,\mathfrak{p}}$ (or similarly $\mathfrak{M}_2$), because we do not know if $\mathcal{C}_\mathfrak{p}$ is free. This is closely related to determining structure of the Selmer group. Note that the only actual source of attaching Galois representation to automorphic forms is the cohomology of Shimura varieties, so in some sense we can find a natural lattice inside the given Galois representation, namely the cohomology with integral coefficients. On the other hand, one may get different lattices when one tries to look into Shimura varieties of different levels.

In the setting of Converse to Herbrand with $\psi = \omega^i$ where the corresponding Selmer group is some part of class group, what Sharifi's conjectures basically say is that the group structure of the Selmer group is more or less $\mathcal{C}/I_\psi\mathcal{C}$, with respect to the lattice given by the cohomology of $\Gamma_1(M)$-modular curves. The cyclicity of it is Vandiver's conjecture.

References

[Hid1] H. Hida, *Galois representations into* $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ *attached to ordinary cusp forms.* Invent. Math. **85** (1986), 545-614.

[Hid2] H. Hida, *Elementary theory of L-functions and Eisenstein series.* LMS Student Texts **26**. Cambridge University Press, 1993.

[Ski] C. Skinner, *Galois representations, Iwasawa Theory, and Special Values of L-functions.* Lecture notes for the CMI Summer School on Galois Representations (Honolulu, 2009).

[Was] L. Washington, *Introduction to Cyclotomic Fields.* GTM **83**. Springer, 1997.

[Wil1] A. Wiles, *On ordinary* λ*-adic representations associated to modular forms*, Invent. Math. **94** (1988), 529-574.

[Wil2] A. Wiles, *The Iwasawa Conjecture for totally real fields*, Ann. of Math. **131** (1990), 493-540.