ARITHMETIC INVARIANT AND SHIMURA VARIETIES

HARUZO HIDA

Contents

Date: March 15, 2010.

Six lectures from 1/22/2010 to 2/5/2010 at Emile Borel Center in their Galois trimester. The author is partially supported by the NSF grant: DMS 0753991 and DMS 0854949.

1. Lecture 1: Abelian components of the 'big' Hecke algebra

Fix a prime $p \geq 5$, field embeddings $\mathbb{C} \overset{i_\infty}{\hookleftarrow} \overline{\mathbb{Q}} \overset{i_p}{\hookrightarrow} \overline{\mathbb{Q}}_p$ and a positive integer N prime to p. Consider the space of modular forms $M_{k+1}(\Gamma_0(Np^{r+1}), \psi)$ with $(p \nmid N, r \geq 0)$ (including Eisenstein series) and cusp forms $S_{k+1}(\Gamma_0(Np^{r+1}), \psi)$. Let the ring $\mathbb{Z}[\psi] \subset \mathbb{C}$ and $\mathbb{Z}_p[\psi] \subset \overline{\mathbb{Q}}_p$ be generated by the values ψ over $\mathbb{Z}$ and $\mathbb{Z}_p$, respectively. The Hecke algebra over $\mathbb{Z}[\psi]$ is $H = \mathbb{Z}[\psi][T(n)|n = 1, 2, \cdots] \subset \mathrm{End}(M_{k+1}(\Gamma_0(Np^{r+1}), \psi))$. We put $H_{k+1,\psi} = H_{k+1,\psi/W} = H \otimes_{\mathbb{Z}[\psi]} W$ for a p-adic discrete valuation ring $W \subset \overline{\mathbb{Q}}_p$ containing $\mathbb{Z}_p[\psi]$. Sometimes our $T(p)$ is written as $U(p)$ as the level is divisible by p. The ordinary part $\mathbf{H}_{k+1,\psi/W} \subset H_{k+1,\psi/W}$ is the maximal ring direct summand on which $U(p)$ is invertible. Let $\psi_1 = \psi_N \times$ the tame p-part of ψ. Then, we have a unique 'big' Hecke algebra $\mathbf{H} = \mathbf{H}_{\psi_1/W}$ such that

(1) $\mathbf{H}$ is free of finite rank over $\Lambda := W[[T]]$ equipped with $T(n) \in \mathbf{H}$ for all n,
(2) if $k \geq 1$ and $\varepsilon : \mathbb{Z}_p^\times \to \mu_{p^\infty}$ is a character,
$$\mathbf{H}/(1 + T - \psi(\gamma)\varepsilon(\gamma)\gamma^k)\mathbf{H} \cong \mathbf{H}_{k+1,\varepsilon\psi_k}\ (\gamma = 1 + p) \text{ for } \psi_k := \psi_1\omega^{1-k},$$
sending $T(n)$ to $T(n)$, where ω is the Teichmüller character.

A (normaized) Hecke eigenform in $M_{k+1}(\Gamma_0(Np^{r+1}), \psi)$ has slope 0 if $f|U(p) = a \cdot f$ with $|a|_p = 1$. An important consequence of the above two facts is

(B) *The number of slope* 0 *Hecke eigenform of level* Np^{r+1}, *of weight* $k+1$ *and of given character* ψ *modulo* Np^{r+1} *is bounded independent of* k, r *and* ψ.

If f has slope 0, $\lambda : H \to \overline{\mathbb{Q}}_p$ given by $f|h = \lambda(h)f$ for $h \in H$ factors through $H_{k+1,\psi}$ and $f = \sum_{n=0}^\infty a(n, f)q^n = \text{constant} + \sum_{n=1}^\infty \lambda(T(n))q^n$. Thus the number of slope 0 forms with Neben character ψ is less than or equal to $\mathrm{rank}_W H_{k+1,\psi} = \mathrm{rank}_\Lambda \mathbf{H}_{\psi_1}$ independent of r and ε. The Hecke field of f is $\mathbb{Q}(f) = \mathbb{Q}(\lambda(n)|n = 1, 2, \dots)$.

The corresponding objects for cusp form is denoted by the corresponding lower case characters; so, for example, $h = \mathbb{Z}[\psi][T(n)|n = 1, 2, \cdots] \subset \mathrm{End}(S_{k+1}(\Gamma_0(Np^{r+1}), \psi))$, $h_{k+1,\psi/W} = h \otimes_{\mathbb{Z}[\psi]} W$, the ordinary part $\mathbf{h}_{k+1,\psi} \subset h_{k+1,\psi}$ and the big cuspidal Hecke algebra $\mathbf{h}_{/W}$. Replacing modular forms by cusp forms (and upper case symbols by lower case symbols), we can construct the "big" cupspidal Hecke algebra $\mathbf{h}_{\psi_1}$ and for the algebra, the same assertions as (1) and (2) holds. We have a surjective Λ-algebra homomorphism $\mathbf{H} \twoheadrightarrow \mathbf{h}$ sending $T(n)$ to $T(n)$.

Each point $P \in \mathrm{Spec}(\mathbf{H})$ has a 2-dimensional (semi-simple) Galois representation ρ_P (of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) with coefficients in the residue field $\kappa(P)$ of P such that $\mathrm{Tr}(\rho_{\mathbb{I}}(Frob_l)) = (T(l) \mod P)$ for almost all primes ℓ. In particular, $\mathbb{I}$ carries a Galois representation $\rho_{\mathbb{I}}$ with
$$\mathrm{Tr}(\rho_{\mathbb{I}}(Frob_l)) = a(l) \text{ (for the image } a(l) \text{ in } \mathbb{I} \text{ of } T(l)).$$
If a prime divisor P of $\mathrm{Spec}(\mathbb{I})$ contains $(1 + T - \varepsilon\psi_k(\gamma)\gamma^k)$ with $k \geq 1$, regarding it as an algebra homomorphism $(P : \mathbb{I} \to \overline{\mathbb{Q}}_p) \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$, we therefore have a Hecke eigenform $f_P \in M_{k+1}(\Gamma_0(Np^{r(P)+1}), \varepsilon\psi_k)$ with $f_P|T(n) = a_P(n)f_P$ for $a_P(n) = P(a(n)) \in \overline{\mathbb{Q}}_p$ for all n. Such a P is called *arithmetic* if $k \geq 1$, and we write $\varepsilon_P = \varepsilon$, $r(P) = r$ and $k(P) = k$ for such a P. Thus $\mathbb{I}$ gives rise to a slope 0 analytic family of modular forms $\mathcal{F}_{\mathbb{I}} = \{f_P|\text{arithemtic } P \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)\}$ and Galois representations $\{\rho_P\}_{P \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)}$. For $a \in \mathbb{I}$, we write $a_P \in \overline{\mathbb{Q}}_p$ for $P(a)$.

We call a Galois representation ρ *abelian* if there exists an open subgroup $G \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that the semi-simplification $(\rho|_G)^{ss}$ has abelian image over G. We call $\mathbb{I}$ an *abelian component* if $\rho_{\mathbb{I}}$ is abelian. A component $\mathbb{I}$ is called *cuspidal* if $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbf{h})$, and if not, we call it *Eisenstein* component.

Hereafter assume $\mathbb{I}$ to be cuspidal. We have a p-adic L-function

$$L_p = L_p(Ad(\rho_{\mathbb{I}})) := L_p(1, Ad(\rho_{\mathbb{I}})) = L_p(1, \rho_{\mathbb{I}}^{sym\otimes 2} \otimes \det(\rho_{\mathbb{I}})^{-1}) \in \mathbb{I}$$

interpolating

$$L_p(P) := P(L_p) = (L_p \mod P) = \frac{L(1, Ad(\rho_P))}{\text{period}} \text{ for all arithemtic } P.$$

Writing $\mathrm{Spec}(\mathbf{h}) = \mathrm{Spec}(\mathbb{I}) \cup \mathrm{Spec}(\mathbb{X})$ for the complement $\mathbb{X}$, we have (under a mild assumption)

$$\mathrm{Spec}(\mathbb{I}) \cap \mathrm{Spec}(\mathbb{X}) = \mathrm{Spec}(\mathbb{I} \otimes_{\mathbf{h}} \mathbb{X}) \cong \mathrm{Spec}(\mathbb{I}/(L_p)) \text{ (a congruence criterion)}.$$

If we interpolate L-values including the cyclotomic variable, i.e, adding a variable s interpolating $L(s, Ad(\rho_P))$ moving s, we need to multiply the L-value by the modifying Euler p-factor. For this enlarged two variable adjoint L-function, the modifying factor vanishes at $s = 1$; so, $L_p(s, Ad(\rho_{\mathbb{I}}))$ has an exceptional zero at $s = 1$, and for an $\mathcal{L}$-invariant $0 \neq \mathcal{L}^{an}(Ad(\rho_{\mathbb{I}})) \in \mathbb{I}[\frac{1}{p}]$, we expect to have $L_p'(1, Ad(\rho_{\mathbb{I}})) \stackrel{?}{=} \mathcal{L}^{an}(Ad(\rho_{\mathbb{I}}))L_p$ (in the style of Mazur–Tate-Teitelbaum). Greenberg proposed a definition of a number $\mathcal{L}(Ad(\rho_P))$ conjectured to be equal to $\mathcal{L}^{an}(Ad(\rho_P))$ for arithmetic P. We can interpolate Greenberg's $\mathcal{L}$-invariant $\mathcal{L}(Ad(\rho_P))$ over arithemtic P to get a function $\mathcal{L}(Ad(\rho_{\mathbb{I}})) \neq 0$ in $\mathbb{I}[\frac{1}{p}]$ so that $\mathcal{L}(Ad(\rho_{\mathbb{I}}))(P) = \mathcal{L}(Ad(\rho_P))$ for all arithmetic P.

1.1. **Is characterizing abelian components important?** Here is a list of such characterizations (possibly conjectural)

- (Well known) A cuspidal $\mathbb{I}$ is abelian $\Leftrightarrow$ there exist an imaginary quadratic field $M = \mathbb{Q}[\sqrt{-D}]$ in which p splits into $\mathfrak{p}\overline{\mathfrak{p}}$ and a character $\Psi = \Psi_{\mathbb{I}} : G_M = \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \mathbb{I}^{\times}$ of conductor $\mathfrak{c}\mathfrak{p}^{\infty}$ for an ideal $\mathfrak{c}$ with $\mathfrak{c}\overline{\mathfrak{c}}D_M|N$ such that $\rho_{\mathbb{I}} = \mathrm{Ind}_M^{\mathbb{Q}} \Psi$, where D_M is the discriminant of M. Thus we call cuspidal abelian component a *CM component*. This implies $L_p = L_p(\Psi^-)L(0, \left(\frac{M/\mathbb{Q}}{}\right))$, where $\Psi^-(\sigma) = \Psi(c\sigma c^{-1}\sigma^{-1})$ for complex conjugation c, and $L_p(\Psi^-)$ is the *anticyclotomic* Katz p-adic L-function associated to Ψ^-. This is a base of the proof by Mazur/Tilouine of the anticyclotomic main conjecture.
- (Known) $\mathbb{I}$ is abelian $\Leftrightarrow$ ρ_P is abelian for a single arithmetic prime P.
- (Almost true, 4th lecture) $\mathbb{I}$ abelian $\Leftrightarrow$ $\rho_{\mathbb{I}} \mod p$ is abelian. This is almost equivalent to the vanishing of the Iwasawa μ-invariant for $L_p(\Psi^-)$ (which is known if $\mathfrak{c}$ is made up of primes split over $\mathbb{Q}$). We discuss about μ in the last two lectures.
- (Known under a mild condition, 2nd lecture) Consider the composite of Hecke fields $\mathcal{V}_r(\mathbb{I}) \subset \overline{\mathbb{Q}}$ generated by $a_P(n)$ for all n and all arithmetic P with level $\leq Np^{r+1}$ for a fixed $r \geq 0$. Then $\mathbb{I}$ is abelian $\Leftrightarrow$ $[\mathcal{V}_r(\mathbb{I}) : \mathbb{Q}] < \infty$. This was a question of L. Clozel asked to me in the early 1990s.
- (Horizontal theorem in the 1st lecture) Fix $k \geq 1$ and consider the composite of Hecke fields $\mathcal{H}_k(\mathbb{I})$ generated by $a_P(n)$ for all n and all arithmetic P with weight k. Then $\mathbb{I}$ is abelian $\Leftrightarrow$ $[\mathcal{H}_k(\mathbb{I}) : \mathbb{Q}(\mu_{p^{\infty}})] < \infty$.
- (Known, 3rd lecture) $\mathcal{L}(Ad(\rho_{\mathbb{I}}))$ is a constant function if and only if $\mathbb{I}$ is a CM component. This is a corollary of Horizontal theorem.

- (?) $L_p(s, Ad(f_P))$ (for an arithmetic P) has exceptional zero at $s = 1$ and its $\mathcal{L}$-invariant $\mathcal{L}(Ad(f_P))$. Is $\mathbb{I}$ abelian if and only if $\mathcal{L}(Ad(f_P)) = \log_p(\mathfrak{p}/\overline{\mathfrak{p}})$ for one arithmetic P up to algebraic numbers? Here taking a high power $(\mathfrak{p}/\overline{\mathfrak{p}})^h = (\alpha)$, $\log_p(\mathfrak{p}/\overline{\mathfrak{p}}) = \frac{1}{h}\log_p(\alpha)$ for the Iwasawa logarithm $\log_p$.

All statements seem to have good arithmetic consequences, and I am convinced the importance of giving as many characterizations of abelian components as possible.

1.2. **Horizontal theorem.** Here is what we prove in this first lecture:

Theorem 1.1. *Pick an infinite set $\mathcal{A}$ of arithmetic points P with fixed weight $k(P) = k \geq 1$. Write $\mathcal{H}_{\mathcal{A}}(\mathbb{I}) \subset \mathcal{H}_k(\mathbb{I})$ for the field generated over $\mathbb{Q}(\mu_{p^\infty})$ by $\{a_P(p)\}_{P\in\mathcal{A}}$. Then the field $\mathcal{H}_{\mathcal{A}}(\mathbb{I})$ is a finite extension of $\mathbb{Q}(\mu_{p^\infty})$ if and only if $\mathbb{I}$ is abelian.*

We prepare a lemma:

Lemma 1.2. *Let $\mathcal{F}$ be a slope 0 p-adic analytic family of Hecke eigenforms with coefficients in $\mathbb{I}$. Then we have*

1. *Fix $0 \leq r < \infty$. Let $K = \mathbb{Q}$. Then the degree $[K(f_P) : K(a_P(p))]$ for arithmetic P with $r(P) \leq r$ is bounded independently of P,*
2. *Let $K = \mathbb{Q}(\mu_{p^\infty})$ and fix $k \geq 1$. Then the degree $[K(f_P) : K(a_P(p))]$ for arithmetic P with $k(P) = k$ is bounded independently of P.*

Proof. If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K[\psi_1, \omega])$ fix $a_P(p)$, f_P^σ is still ordinary Hecke eigenforms of the same level and the same Neben character. The number of such forms is bounded by $\mathrm{rank}_{\mathbb{Z}_p[[T]]}\mathbf{h}$. Thus $[K(f_P) : K(a_P(p))] \leq [K[\psi_1, \omega] : K]\,\mathrm{rank}_{\mathbb{Z}_p[[T]]}\mathbf{h}$. □

Hereafter we fix $\mathcal{A}$ and assume that $[\mathcal{H}_{\mathcal{A}}(\mathbb{I}) : K] < \infty$ for $K := \mathbb{Q}(\mu_{p^\infty})$. We try to prove that $\mathbb{I}$ is abelian. Put $K(f_P) = K[a_P(n); n = 1, 2, \ldots] \subset \overline{\mathbb{Q}}$. For a prime l outside Np, let $A(l)$ be a root of $\det(X - \rho_{\mathbb{I}}(Frob_l)) = 0$. Then $\alpha_{l,P} := A_P(l)$ is a root of $X^2 - a_P(l)X + \psi_k(l)l^{k(P)} = 0$. If $l = p$, we put $A(l) = a(l)$. Fix l. Extending $\mathbb{I}$, we assume that $A(l) \in \mathbb{I}$. By the lemma, $L_P = K[\alpha_{l,P}]$ has bounded degree over K independent of l and P for all $P \in \mathcal{A}$; so, l is tamely ramified in L_P/K for $l \gg 0$.

1.3. **Weil numbers.** We start preparing for a proof of the theorem. For a prime l, a Weil l-number $\alpha \in \mathbb{C}$ of integer weight $k \geq 0$ satisfies

$$(1)\ \alpha \text{ is an algebraic integer; } (2)\ |\alpha^\sigma| = l^{k/2} \text{ for all } \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

If α is a Weil number, $\mathbb{Q}(\alpha)$ is contained in a CM field. We call two nonzero algebraic numbers a and b equivalent (written as $a \sim b$) if a/b is a root of unity.

Lemma 1.3. *Let K be a finite field extension of $\mathbb{Q}(\mu_{p^\infty})$. Then for a given prime l and weight $k \geq 0$, there are only finitely many Weil l-numbers of weight k in K up to equivalence. If $l = p$ and $K = \mathbb{Q}[\mu_{p^\infty}]$, any Weil p-number of weight k is equivalent to $(p^*)^{k/2}$, where $p^* = (-1)^{(p-1)/2}p$ if p is odd, and $p^* = 2$ if $p = 2$.*

Proof. If $l \neq p$, the prime l remains prime in $\mathbb{Q}[\mu_{p^\infty}]$ over a finite subextension of $\mathbb{Q}[\mu_{p^\infty}]$. Thus there are only finitely many primes $\mathfrak{L}$ of $\mathbb{Z}[\mu_{p^\infty}]$ above (l) Thus for a Weil l-number α of weight k, for the normalized valuation $v_{\mathfrak{L}}$ of $\mathfrak{L}$ with $v_{\mathfrak{L}}(l) = 1$, $0 \leq v_{\mathfrak{L}}(\alpha) \leq k$ is bounded, and there are only finitely many possibilities of prime factorization of (α). If $(\alpha) = (\beta)$ for two Weil l-numbers α, β, then α/β is a Weil number of weight 0; so, $\alpha \sim \beta$ by Kronecker's theorem. If $l = p$, there is only one prime in $\mathbb{Q}[\mu_{p^\infty}]$ above p; so, any Weil p-number of weight k is equivalent to $(p^*)^{k/2}$, since $\sqrt{p^*} \in \mathbb{Q}[\mu_{p^\infty}]$. Thus the result follows from this if $K = \mathbb{Q}(\mu_{p^\infty})$.

For general finite extension $K/\mathbb{Q}[\mu_{p^\infty}]$, still there are finitely many primes over l in the integer ring of K; so, the same argument works. □

Here is a slight improvement of the above fact:

Proposition 1.4. *Let $\mathcal{K}_d$ be the set of all finite extensions of $\mathbb{Q}[\mu_{p^\infty}]$ of fixed degree d inside $\overline{\mathbb{Q}}$ whose ramification at l is tame. Then there are only finitely many Weil l-numbers up to equivalence of a given weight in the set-theoretic union $\bigcup_{L\in\mathcal{K}_d} L$ in $\overline{\mathbb{Q}}$.*

The point of the proof is as follows. Writing $K = \mathbb{Q}[\mu_{p^\infty}]$ and $K_l = K \otimes_{\mathbb{A}} \mathbb{Q}_l$, by tameness, there are only finitely many isomorphism class of $K \otimes_{\mathbb{A}} \mathbb{Q}_l$-algebras $L_l = L \otimes_{\mathbb{Q}} \mathbb{Q}_l$ for $L \in \mathcal{K}_d$. Thus we only need to prove finiteness for Weil numbers of given weight contained in a fixed isomorphism class of L_l. We look at the universal composite $L_l \otimes_{K_l} L_l$ which is a product of fields indexed by l-adic nonequivalent normalized valuations $v_1, \dots, v_n$. Consider a tuple

$$V(\alpha) = (v_1(\alpha\otimes 1), \dots, v_n(\alpha\otimes 1), v_1(1\otimes\alpha), \dots, v_n(1\otimes\alpha)).$$

If $\alpha \sim \beta$, we have $V(\alpha) = V(\beta)$. The tuple $V(\alpha)$ determines the prime factorization of (α) in any possible composite $K(\alpha,\beta)$; so, if $V(\alpha) = V(\beta)$, $(\alpha) = (\beta)$ in $K(\alpha,\beta)$; so, by Kronecker's theorem, $\alpha \sim \beta$. Since there are only finitely many possibilities of $V(\alpha)$, there are only finitely many classes.

It is not very difficult to prove

Lemma 1.5. *The group of roots of unity in the composite $\mathbf{L}$ of L for $L \in \mathcal{K}_d$ in $\overline{\mathbb{Q}}$ contains $\mu_{p^\infty}(K)$ as a subgroup of finite index.*

By this, we can replace the equivalent $\alpha \sim \beta$ by finer one $\alpha \approx \beta$ requiring $\alpha/\beta \in \mu_{p^\infty}$, and still the finer equivalence classes in the union $\bigcup_{L\in\mathcal{K}_d} L$ of Weil l-numbers of given weight is finite.

1.4. **A key lemma in the entire lectures.** We start with a rigidity lemma:

Lemma 1.6. *Let $\Phi(T) \in W[[T]]$. If there is an infinite subset $\Omega \subset \mu_{p^\infty}(\overline{K})$ such that $\Phi(\zeta - 1) \in \mu_{p^\infty}(\overline{\mathbb{Q}}_p)$ for all $\zeta \in \Omega$, then there exists $\zeta_0 \in \mu_{p^\infty}(W)$ and $s \in \mathbb{Z}_p$ such that $\zeta_0^{-1}\Phi(T) = (1+T)^s = \sum_{n=0}^{\infty} \binom{s}{n} T^n$.*

By the assumption, for $s \in \mathbb{Z}_p^\times$ sufficiently close to 1, $\zeta \mapsto \zeta^s$ is an automorphism of $W[[\mu_{p^\infty}]]$ over W; so, $\Phi(\zeta^s - 1) = \Phi(\zeta)^s \Leftrightarrow \Phi(t^s) = \Phi(t)^s$ $(t = 1+T)$, and the power series is the desired form by a lemma of Chai [C] Theorem 4.3 and [C1] Remark 6.6.1 (iv). Here is a sketch of an elementary proof supplied to me by Kiran Kedlaya.

Proof. Making variable change $T \mapsto \zeta_1^{-1}(T+1) - 1$ for a $\zeta_1 \in \Omega$ (replacing W by its finite extension if necessary), we may replace Ω by $\zeta_1^{-1}\Omega \ni 1$; so, rewriting $\zeta_1^{-1}\Omega$ as Ω, we may assume that $1 \in \Omega$. Note $t = 1 \Leftrightarrow T = 0$.

Write the valuation of W as v (and use the same symbol v for an extension of v to $W[\mu_{p^\infty}]$). Normalize v so that $v(p) = 1$. We are trying to show that $\Phi(T) = (1+T)^s\zeta'$ for some $s \in \mathbb{Z}_p$ and some p-power root of unity ζ'. Anyway, we write $\Phi(0) = \zeta' \in \mu_{p^\infty}(\overline{\mathbb{Q}}_p)$. Replacing Φ by $\zeta'^{-1}\Phi$ (and extending the scalar to a finite extension of W if necessary), we may assume that $\Phi(0) = 1$.

Suppose that $\Phi(T) \notin W$ (non-constant). Write $\Phi(T) - 1 = \sum_{i=1}^{\infty} a_i T^i$. Since W is a DVR, there is a least index $j > 0$ for which $v(a_j)$ is minimized. For ϵ sufficiently small, if $v(\tau) = \epsilon$, then $v(\Phi(\tau) - 1) = v(a_j) + j\epsilon$. In particular, for ζ a p-power root of unity, taking $\tau = \zeta - 1$, we have $v(\zeta - 1) = p^{-m}/(p-1)$ for some non-negative integer m, so we have infinitely many relations of the form $jp^{-m}/(p-1) + v(a_j) = p^{-n}/(p-1)$. Then, we have $m \to \infty \Rightarrow n \to \infty$ (by continuity and non-constancy of $\tau \mapsto \Phi(\tau)$); so, taking limits under $m \to \infty$ yields $v(a_j) = 0$. Also, j must be a power of p, say $j = p^h$, and for m large we have $n = m - h$.

Since $v(a_j) = 0$, $a_j \mod \mathfrak{m}_W$ is in $\mathbb{F}^\times$. For the moment, assume $\mathbb{F} = \mathbb{F}_p$. That is, a_j reduces to an integer b_0 coprime to p in the residue field of W. We can thus replace $\Phi(T)$ by $\Phi_1(T)$ defined by $\Phi(T) = \Phi_1(T) \times (1+T)^s$ for some s (namely $s = b_0 j = b_0 p^{h_0}$ for $h_0 := h$) so as to increase the least index j for which $v(a_j) = 0$. Indeed, writing $\Phi(T) = \sum_{n=0}^{j} a_n T^n + T^{j+1} f(T)$ with $f(T) \in W[[T]]$, we have

$$\sum_{n=0}^{j} a_n T^n \equiv 1 + b_0 T^{p^{h_0}} \equiv (1 + T^{p^{h_0}})^{b_0} \equiv (1+T)^s \mod (\mathfrak{m}_W + (T^{j+1})).$$

we have $\Phi_1(T) \equiv 1 + T^{j+1} f(T)(1+T)^{-s} \equiv 1 \mod (\mathfrak{m}_W + (T^{j+1}))$. Thus if we write j_1 for the j for this new Φ_1, $j_1 > j$, and $j_1 = p^{h_1}$ with $h_1 > h_0$ and $a_{j_1} \equiv b_1 \mod \mathfrak{m}_W$ for $b_1 \in \mathbb{Z}$. Repeating this, for $s = \sum_{k=0}^{\infty} b_k p^{h_k} \in \mathbb{Z}_p$, $\Phi(T)/(1+T)^s - 1 = \sum_{n=1} a_n T^n$ no longer has a least j with minimal $v(a_j)$; so, $\Phi(T)/(1+T)^s = 1$, and we get $\Phi(T) = (1+T)^s$.

Suppose now that $\mathbb{F} \neq \mathbb{F}_p$. We have the Frobenius automorphism ϕ fixing $\mathbb{Z}_p[\mu_{p^\infty}] \subset W[\mu_{p^\infty}]$. Letting ϕ acts on power series by $(\sum_n a_n T^n)^\phi = \sum_n a_n^\phi T^n$, we find $\Phi^\phi(t^\phi) = \Phi(t)^\phi$. Since $\Phi(\zeta - 1)$ is a p-power root of unity for ζ in a infinite set $\Omega \subset \mu_{p^\infty}$, we have $\Phi^\phi(\zeta - 1) = \Phi^\phi(\zeta^\phi - 1) = \Phi(\zeta - 1)^\phi = \Phi(\zeta - 1)$. Since $\Omega \subset \widehat{\mathbb{G}}_m$ is Zariski dense, we find that $\Phi^\phi = \Phi$, which shows $\Phi \in W^\phi[[T]]$ for the subring W^ϕ fixed by ϕ. Note that the residue field of W^ϕ is $\mathbb{F}_p$, and the earlier argument applies to $\Phi \in W^\phi[[T]]$. □

Extending $\mathbb{I}$ to its integral closure, we assume that $\mathbb{I}$ is integrally closed. For a prime l, we write $\mathcal{H}_{\mathcal{A}}^{(l)}(\mathbb{I})$ for the subfield generated by $\alpha_{l,P} \in \overline{\mathbb{Q}}$ for all $P \in \mathcal{A}$. We simply write $\mathcal{H}_{\mathcal{A}}(\mathbb{I}) = \mathcal{H}_{\mathcal{A}}^{(p)}(\mathbb{I})$. Recall $L_P = \mathbb{Q}[\mu_{p^\infty}][\alpha_{l,P}]$.

Proposition 1.7. *Fix a rational prime $l \nmid N$ either $l = p$ or tamely ramified in $L_P/\mathbb{Q}[\mu_{p^\infty}]$ for all $P \in \mathcal{A}$. Suppose $[\mathcal{H}_{\mathcal{A}}^{(l)}(\mathbb{I}) : \mathbb{Q}(\mu_{p^\infty})] < \infty$. Then, for $W = \mathbb{I} \cap \overline{\mathbb{Q}}_p$, we have $A(l)$ in $W[[T]][t^{1/p^n}] \cap \mathbb{I}$ ($t = 1+T$) for some $0 \le n \in \mathbb{Z}$, and there exists a Weil l-number α_1 of weight 1 and a root of unity ζ_0 such that $A_P(l) = \alpha_{l,P} = \zeta_0 \langle \alpha_1 \rangle^{k(P)-1}$ for all arithmetic P; in other words, $A(l)(T) = \zeta_0 (1+T)^s$ for $s = \frac{\log_p(\alpha_1)}{\log_p(\gamma)}$.*

Proof. We give a sketch of a proof assuming $\mathbb{I} = \Lambda = W[[T]]$. Let $A = A(l)$. By Lemma 1.4, we have only a finite number of Weil l-numbers of weight k in $\bigcup_{P \in \mathcal{A}} L_P$ up to roots of unity, and hence A_P for $P \in \mathcal{A}$ hits one of such Weil l-number α of weight k infinitely many times, up to roots of unity.

After a variable change $T \mapsto Y = \gamma^{-k}(1+T) - 1$, we have $A(Y)|_{Y=0} = A(T)|_{T=\gamma^k - 1}$. Note that $|\alpha|_p = 1$. Let $\Omega_1 = \{\varepsilon_P(\gamma) | P \in \mathcal{A}\}$ which is an infinite set in $\mu_{p^\infty}(K)$. Let $\Phi_1(Y) := \alpha^{-1} A(Y) = A(\gamma^{-k}(1+T) - 1) \in W[[Y]]$. The subset Ω_2 of Ω_1 made up of $\zeta \in \Omega_1$ such that $\Phi_1(\zeta - 1)$ is a root of unity is an infinite set. We thus find an infinite subset $\Omega \subset \Omega_2$ and a root of unity ζ_1 such that $\{\Phi_1(\zeta - 1) | \zeta \in \Omega\} \subset \zeta_1 \mu_{p^\infty}(K)$. Then

$\Phi = \zeta_1^{-1}\Phi_1$ satisfies the assumption of Lemma 1.6, and for a root of unity ζ, we have $A(Y) = \zeta\alpha(1+Y)^{s_1}$ for $s_1 \in \mathbb{Z}_p$, and $A(T) = \zeta\alpha(\gamma^{-k}(1+T))^{s_1}$. From this, it is not difficult to determine s_1 as stated in the proposition. □

1.5. **Proof of the theorem.** We start with a couple of preliminary results. Consider the W-algebra endomorphism $\sigma_s : (1+T) \mapsto (1+T)^s = \sum_{n=0}^{\infty} \binom{s}{n} T^n$ of a power series ring Λ for $s \in \mathbb{Z}_p$.

Lemma 1.8. *Let A be an integral domain over Λ. Assume that $\sigma_2 \in \mathrm{Aut}(\Lambda_{/W})$ extends to an endomorphism σ of A. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to GL_2(A)$ be a continuous representation for a field $F \subset \overline{\mathbb{Q}}$, and put $\rho^\sigma := \sigma \circ \rho$. If $\mathrm{Tr}(\rho^\sigma) = \mathrm{Tr}(\rho^2)$. Then ρ is absolutely reducible over the quotient field Q of A.*

Proof. Suppose that ρ is absolutely irreducible over Q, and try to get absurdity. We have the identity $\mathrm{Tr}(\rho^\sigma) = \mathrm{Tr}(\rho^2) = \mathrm{Tr}(\rho^{sym\otimes 2}) - \det(\rho)$ for the symmetric second tensor representation $\rho^{sym\otimes 2}$ of ρ. Over Q, by absolute irreducibility, we have the identity of semi-simplification: $(\rho^{sym\otimes 2})^{ss} \cong \rho^\sigma \oplus \det(\rho)$. Tensoring $\det(\rho)^{-1}$, we get $Ad(\rho)^{ss} \cong (\rho^\sigma \otimes \det(\rho)^{-1}) \oplus \mathbf{1}$. Since $Ad(\rho)$ is self-dual, we have $\mathbf{1} \hookrightarrow Ad(\rho)$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$-modules. In other words, we have a non-trivial element $0 \neq \phi \in \mathrm{End}_{A[H]}(\rho)$ for $H = \mathrm{Gal}(\overline{\mathbb{Q}}/F(\rho^I))$ such that $\mathrm{Tr}(\phi) = 0$. Since ρ is absolutely irreducible, ϕ has to be a scalar multiplication by $z \in A^\times$ by Schur's lemma; so, $\mathrm{Tr}(\phi) = 2z \neq 0$, a contradiction (unless A has characteristic 2). □

Proof of Theorem 1.1. Let $K := \mathbb{Q}(\mu_{p^\infty})$ and $L_P = K(\alpha_{l,P})$ for a prime l. We need to prove that $[\mathcal{H}_{\mathcal{A}}(\mathbb{I}) : K] < \infty \Rightarrow \mathcal{F}$ has complex multiplication. Thus suppose $[\mathcal{H}_{\mathcal{A}}(\mathbb{I}) : K] < \infty$. For each arithmetic P with $k(P) = k$, by Lemma 1.2, $[K(f_P) : K(a_P(p))] < d$ for a positive integer d independent of P. Thus $[L_P : K] < 2d[\mathcal{H}_{\mathcal{A}}(\mathbb{I}) : K]$ for each prime l. Therefore, any odd prime $l > 2d[\mathcal{H}_{\mathcal{A}}(\mathbb{I}) : K]$ is at most tamely ramified in L_P/K. Take such an odd prime $l > 2d[\mathcal{H}_{\mathcal{A}}(\mathbb{I}) : K]$ prime to Np. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{I})$ be the Galois representation associated to $\mathcal{F}$. Thus by Proposition 1.7, we have $\mathrm{Tr}(\rho(Frob_l)) = \zeta(1+T)^a + \zeta'(1+T)^{a'}$ for two roots of unity ζ, ζ' and $a, a' \in \mathbb{Q}_p$. Take an arithmetic $Q \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$. Note that $\zeta(1+T)^a, \zeta'(1+T)^{a'}$ is at most in a quadratic extension of $\mathbb{Q}(f_Q)$; so, it is easy to see that the order of ζ, ζ' is bounded independently of l. Let $\mathfrak{m}_N = \mathfrak{m}_{\mathbb{I}}^N + (T)$ and $\overline{\rho} = \rho \mod \mathfrak{m}_N$ for a sufficiently large N and F be the splitting field of $\overline{\rho}$. We have $\mathrm{Tr}(\rho(Frob_{\mathfrak{l}})) = \zeta^f(1+T)^{fa} + \zeta'^f(1+T)^{fa'}$ and $\rho(Frob_{\mathfrak{l}}) \equiv 1 \mod \mathfrak{m}_N$ (so $\zeta^f \equiv 1 \mod \mathfrak{m}_N$) for a prime $\mathfrak{l}|l$ of F of residual degree f. Since $\zeta^f \equiv 1 \mod \mathfrak{m}_N$, by taking N large, we may assume that $\zeta^f = \zeta'^f = 1$. This shows $\mathrm{Tr}(\sigma_s(\rho(Frob_{\mathfrak{l}}))) = \mathrm{Tr}(\rho(Frob_{\mathfrak{l}})^s)$ for all $0 \neq s \in \mathbb{Z}_p$. Thus by Chebotarev density theorem, we get $\mathrm{Tr}(\sigma_s \circ \rho) = \mathrm{Tr}(\rho^s)$ over $G = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$. Then by the above lemma, $\rho^{ss}|_G$ is abelian, and hence $\mathbb{I}$ is abelian.

On the other hand, if $\mathcal{F} = \mathcal{F}_{\mathbb{I}}$ has complex multiplication by an imaginary quadratic extension $M/\mathbb{Q}$ in $\overline{\mathbb{Q}}$, we have a character $\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \mathbb{I}$ unramified outside $N\mathfrak{p}$ such that α_ℓ is the value of $\lambda_P(Frob_{\mathfrak{l}}) = \lambda(Frob_{\mathfrak{l}}) \mod P$ for a prime $\mathfrak{l}$ in M over ℓ. Here $\mathfrak{p}$ is a prime factor of p in M. Let $\mathbb{F}$ be the residue field of $\mathbb{I}$ (note that $\mathbb{I}$ is a local ring with maximal ideal $\mathfrak{m}$, because it is finite flat over Λ). Write W for the ring of Witt vectors of $\mathbb{F}$. Let $(R, \widetilde{\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to R^\times)$ be the universal couple with the universal character unramified outside $N\mathfrak{p}$ deforming $(\lambda \mod \mathfrak{m})$

over W. Writing C_p for the p-primary part of the ray class group $Cl_M(N\mathfrak{p}^\infty)$ modulo $N\mathfrak{p}^\infty$ of M, by class field theory, $R \cong W[[C_p]]$. By universality, we have a W-algebra homomorphism $\varphi : R \to \mathbb{I}$ such that $\varphi \circ \widetilde{\lambda} = \lambda$. Thus $\mathbb{I} \hookrightarrow W[[\Gamma_M]]$ for the maximal torsion-free quotient Γ_M, and Γ_M contains Γ naturally. The Λ-algebra structure of $\mathbb{I}$ is equal to that coming from the original inclusion $\Lambda \hookrightarrow \mathbb{I}$ (after twist by the k-th power of the p-adic cyclotomic character). Then for an arithmetic point P with $r(P) \leq r$, $\lambda_P = \lambda \mod P$ has infinity type $k-1$; that is, $\lambda_P(\alpha) = \alpha^{k-1}$ for $\alpha \in M$ congruent to 1 modulo Np^{r+1}. For the class number h of M, taking a generator α of $\mathfrak{l}^h$, we have $\lambda_P(\mathfrak{l}) = \alpha^{1/h}\zeta$ for $\zeta \in \mu_{p^r h}$. Thus choosing a complete representative set $\{\mathfrak{a}_j\}_{j=1,\dots,h}$ of ideal classes of M, taking a generator α_j of $\mathfrak{a}_j^h$, we find that $\mathbb{Q}(\alpha_{\ell,P})_{k(P)=k,\ell} \subset \mathbb{Q}(\mu_{p^\infty h})[\alpha_j^{1/h}|j = 1,\dots,h]$ which is a finite extension of $\mathbb{Q}[\mu_{p^\infty}]$ containing $\mathcal{H}_k(\mathbb{I})$, which has finite degree over $\mathbb{Q}[\mu_{p^\infty}]$. This finishes the proof. □

Here is an obvious corollary of the above proof.

Corollary 1.9. *Let $K := \mathbb{Q}[\mu_{p^\infty}]$ and $\mathcal{A} \subset \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ be an infinite set of arithmetic points P with fixed weight $k(P) = k \geq 1$. Unless $\mathcal{F}$ has complex multiplication*

$$\limsup_{P\in\mathcal{A}}[K(a(p, f_P)) : K] = \infty.$$

Indeed, if $\limsup_P[K(a(p, f_P)) : K] < \infty$, the index $[L_P : K]$ $(P \in \mathcal{A})$ is bounded for $A \in \mathbb{I}$ as in Proposition 1.7. Thus we can still apply the above proof and conclude that $\mathcal{F}$ has complex multiplication.

2. Lecture 2: Vertical version

Let $\mathcal{F} = \mathcal{F}_\mathbb{I} = \{f_P\}_{P\in\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)}$ be a cuspidal p-adic analytic family of p-ordinary Hecke eigen cusp forms of slope 0. We have the following "vertical" conjecture:

Conjecture 2.1. *Let $\mathcal{A}$ be an infinite set of arithmetic points with bounded level $r(P) \leq r$ for a fixed $r \geq 0$. Let $\mathcal{V}_\mathcal{A}(\mathbb{I})$ be the field generated over $\mathbb{Q}$ by $\{\alpha_{p,P}\}_{P\in\mathcal{A}}$, where P runs over all arithmetic points with $\mathrm{Im}(\varepsilon_P) \subset \mu_{p^r}$ for a fixed r. Then the field $\mathcal{V}_\mathcal{A}(\mathbb{I})$ is a finite extension of $\mathbb{Q}$ for a fixed $r < \infty$ if and only if f_P is a CM theta series for an arithmetic P with $k(P) \geq 1$.*

Pick a prime l different from p and write $\mathcal{V}^{(l)}_\mathcal{A}(\mathbb{I})$ for the field generated by $\{\alpha_{l,P}, \beta_{l,P}\}$ for all $P \in \mathcal{A}$, where P runs over all points in $\mathcal{A}$. Then we might speculate that

(Vertical l-version): *The field $\mathcal{V}^{(l)}_\mathcal{A}(\mathbb{I})$ is a finite extension of $\mathbb{Q}$ for a fixed $r < \infty$ if and only if for an arithmetic P with $k(P) \geq 1$, either f_P is a CM theta series or the automorphic representation generated by f_P is square-integrable at l.*

We prove

Theorem 2.2 (Vertical theorem)**.** *Let r be a non-negative integer. For an infinite set $\mathcal{A}$ of arithmetic points P with bounded level $r(P) \leq r$ for an $r \geq 0$, assume that $\mathcal{V}_\mathcal{A}(\mathbb{I})$ is a finite extension of $\mathbb{Q}$. If there exists an arithmetic point $P_0 \in \mathcal{A}$ with $k(P_0) \geq 1$ such that*

(1) *$\alpha_0 = a_{P_0}(p)$ is a Weil number,*
(2) *$\Sigma_{\alpha_0} = \{\sigma : \mathbb{Q}(\alpha_0) \hookrightarrow \overline{\mathbb{Q}} \,|\, |i_p(\alpha_0^\sigma)| = 1\}$ is a CM type of $\mathbb{Q}(\alpha_0)$,*
(3) *$\mathcal{V}_\mathcal{A}(\mathbb{I})$ is generated by α_0 over $\mathbb{Q}$.*

Then $\mathbb{I}$ has complex multiplication.

2.1. **Results towards the vertical conjecture.** Let $\mathcal{A}_r$ be the set of all arithmetic points of $\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ with $r(P) \leq r$.

Proposition 2.3. *Let $\mathcal{F} = \{f_P\}_{P \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)}$ be a p-adic analytic family of classical p-ordinary Hecke eigenforms and $\mathcal{A} \subset \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ be an infinite set of arithmetic points P with $r(P) \leq r$ for a fixed $r \geq 0$. Assume that for $P_0 \in \mathcal{A}$*

(1) *$\alpha_0 = a_{P_0}(p)$ is a Weil number,*
(2) *$\Sigma_{\alpha_0} = \{\sigma : \mathbb{Q}(\alpha_0) \hookrightarrow \overline{\mathbb{Q}} \,|\, |i_p(\alpha_0^\sigma)| = 1\}$ is a CM type of $\mathbb{Q}(\alpha_0)$,*
(3) *$\mathcal{V}_{\mathcal{A}}(\mathbb{I}) = \mathbb{Q}(\alpha_0)$ is generated by α_0 over $\mathbb{Q}$.*

Then there exist a Weil p-number α of weight 1 with $|i_p(\alpha)|_p = 1$ such that $a(p, f_P) = \zeta\langle\alpha\rangle^{k(P)}$ for a root of unity ζ for all arithmetic P with $k(P) \geq 1$, where $\langle\alpha\rangle = \exp_p(\log_p(i_p(\alpha)))$ for the Iwasawa logarithm $\log_p$.

Proof. First, in order to give a simple sketch of the proof, suppose first that $M := \mathcal{V}_{\mathcal{A}}(\mathbb{I})$ is an imaginary quadratic field. Take $P \in \mathcal{A}$ with $k(P) > 1$. Then $\alpha_{p,P}$ is a Weil number of weight $k(P) > 1$ with $|\alpha_{p,P}|_p = 1$. Thus (p) has to split in M; so, $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in M. Thus $\Sigma_{\alpha_{p,P}}$ is made of single element $\iota = i_p|_M$, and for each k, there exists at most one Weil number $\alpha_k \in M$ of weight k (up to roots of unity in M) such that $|\alpha_k|_p = 1$. In M, $(\alpha_k) = \overline{\mathfrak{p}}^k$ for the prime ideal $\mathfrak{p}$ of M corresponding to $i_p|_M$. Fix such a k. Taking a k-th root $\alpha = \sqrt[k]{\alpha_k}$, we have $\alpha_l = \alpha^l$ up to roots of unity for all l as $(\alpha_l) = \overline{\mathfrak{p}}^l$.

Since $\mathcal{A}$ is an infinite set, there exists an infinite sequence in $\mathcal{A}$

$$P_1, P_2, \cdots, P_n, \ldots$$

with increasing weight $k(P_1) < k(P_2) < \cdots$ such that

$$(a_{P_j}(p)) = \overline{\mathfrak{p}}^{k(P_j)}$$

for all $j > 0$. Put

$$\langle\alpha\rangle = \exp(\frac{1}{k(P_0)} \log_p(a(p, f_{P_0})) = \exp(\log_p(\alpha)).$$

Since $(a_{P_j}(p)) = \overline{\mathfrak{p}}^{(k(P_j))}$, $a_{P_j}(p)/\langle\alpha\rangle^{k(P_j)}$ is a Weil number of weight 0, that is, it is an algebraic integer with all its conjugates having absolute value 1. Then by Kronecker's theorem, we find $a_{P_j}(p) = \zeta_{P_j}\langle\alpha\rangle^{k(P_j)}$ for a root of unity ζ_{P_j}. Note that $\langle\alpha\rangle$ is contained in a finite extension M'/M. Since there are finitely many roots of unity in M', we have only finitely many possibilities of ζ_{P_j}. Therefore, replacing $\{P_j\}_j$ by its subsequence, we find an infinite sequence $P_1, P_2, \cdots, P_n, \cdots$ of increasing weights such that $a_{P_j}(p) = \zeta\langle\alpha\rangle^{k(P_j)}$ for all $j = 1, 2, \ldots$ for a fixed root of unity ζ. We have a power series $\Phi_\alpha(X) \in W[[X]]$ with coefficients in a discrete valuation ring W finite flat over $\mathbb{Z}_p$ such that $\Phi_\alpha(\gamma^k - 1) = \zeta\langle\alpha\rangle^k$ for all integers k. Since $\mathcal{F}$ is an ordinary family, there exists an element $A \in \mathbb{I}$ such that $a(p, f_P) = (A \mod P)$ for all height 1 prime P of $\mathbb{I}$ containing $(1 + X - \gamma^{k(P)})$. Thus we find $A \equiv \Phi_\alpha \mod P_j$ for infinitely many distinct primes P_j; so, $A = \Phi_\alpha$, as desired.

We now treat the general case where M may not be an imaginary quadratic field. Let $K \subset \overline{\mathbb{Q}}$ be a number field with integer ring O. Consider $O \otimes_{\mathbb{Z}} K$. Then $O \otimes_{\mathbb{Z}} K$ is a product of fields $\sigma(O)K \subset \overline{\mathbb{Q}}$ indexed by (some) embeddings $\sigma : O \hookrightarrow \overline{\mathbb{Q}}$. Take the base ring W containing O. Then $\mathbb{I} \otimes_{\mathbb{Z}} K$ contains $O \otimes_{\mathbb{Z}} K$, and $\mathbb{I} \otimes_{\mathbb{Z}} K$ decomposes accordingly: $\mathbb{I} \otimes_{\mathbb{Z}} K = \prod_\sigma \mathbb{I}_\sigma$. Regard $\mathbb{I} \otimes_{\mathbb{Z}} K$ as a K-algebra from the right factor (and

K is embedded in $\overline{\mathbb{Q}}_p$ by i_p). Note $\mathbb{I}\otimes_{\mathbb{Z}}K = \mathbb{I}\otimes_{\mathbb{Z}_p}\mathbb{Z}_p\otimes_{\mathbb{Z}}K = \mathbb{I}\otimes_{\mathbb{Z}_p}K_p$ for $K_p = \mathbb{Z}_p\otimes_{\mathbb{Z}}K$. For an arithmetic prime P, we have $\mathbb{Z}[f_P] := \mathbb{Z}[a_P(n)|n = 1, 2, \dots] \subset \mathbb{I}/P$. Then $\mathbb{Z}[f_P]\otimes_{\mathbb{Z}}K \subset \mathbb{I}/P\otimes_{\mathbb{Z}}K$ as K is $\mathbb{Z}$-flat. On the other hand, $\mathbb{Z}[f_P]\otimes_{\mathbb{Z}}K = \mathbb{Q}(f_P)\otimes_{\mathbb{Z}}K \cong \prod_{\tau:\mathbb{Q}(f_P)\hookrightarrow\overline{\mathbb{Q}}_p} i_p(\tau(\mathbb{Q}(f_P))K)$. The composite $\sigma(\mathbb{Q}(f_P))K$ is taken in $\overline{\mathbb{Q}}_p$ by sending it by i_p inside $\overline{\mathbb{Q}}_p$. For some τ (for example, complex conjugation $\tau = c$), we may have $|i_p(\tau(a_P(p)))|_p < 1$.

Let us give more details why this strange phenomenon: $|i_p(\tau(a_P(p)))|_p < 1$ could occur. Suppose $K/\mathbb{Q}$ is a Galois extension with $O \subset W$. Then writing $V = K \cap W$ (the valutaion ring corresponding to $i_p : K \hookrightarrow \overline{\mathbb{Q}}_p$), $V \otimes_{\mathbb{Z}} V \subset \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} \sigma(V)V$. Let e_σ for the idempotent of $\sigma(V)V$. Writing $D_V \subset \mathrm{Gal}(K/\mathbb{Q})$ for the decomposition subgroup of V, unless $\sigma \in D_V$ (i.e., $\sigma(V) = V$), $\sigma(V)V = K$. Since $V \subset \mathbf{h}_{k(P)+1,\psi_P}$, we regard $e_\sigma \in \mathbf{h}_{k(P)+1,\psi_P} \otimes_{\mathbb{Z}} V$. Since $U(p)$ is invertible in $\mathbf{h}_{k(P)+1,\psi_P}$, the image of $e_\sigma(U(p) \otimes 1)$ is invertible in $K = \sigma(V)V$, but that does not mean $e_\sigma(U(p) \otimes 1)$ is a p-adic unit. Define $E_P = \lim_{n\to\infty}(U(p) \otimes 1)^{n!}$ under the p-adic topology $\mathcal{T}_P$ of $\mathbf{h}_{k(P)+1,\psi_P}\otimes_{\mathbb{Z}}V$ inducing the natural topology on $1\otimes V \subset \mathbf{h}_{k(P)+1,\psi_P}\otimes_{\mathbb{Z}}V$. Then E_P is orthogonal to e_σ if $e_\sigma(U(p)\otimes 1)$ is p-adically nilpotent under the p-adic topology $\mathcal{T}_P$ of $\mathbf{h}_{k(P)+1,\psi_P}\otimes_{\mathbb{Z}}V$. The idempotent $e_P = \lim_{n\to\infty} U(p)^{n!}$ in $h_{k(P)+1,\psi_P}$ (for $\psi_P = \psi_{k(P)}\varepsilon_P$) is only defined over $\overline{\mathbb{Q}}$; so, e may not commute with some σ. In other words, we could have $e_P \otimes 1 \neq E_P$, and $E_P = \sum_{\tau:|i_p(\tau(a_P(p)))|_p=1} e_\tau$. We can embed $\mathbf{h}$ into $\prod_P \mathbf{h}_{k(P)+1,\psi_P} \subset \prod_P h_{k(P)+1,\psi_P}$ for an infinite set $\mathcal{A}$ of arithmetic points P of $W[[T]]$ sending $T(n)$ to diagonal $T(n)$ in the product of right-hand-side. The tensor product $\mathbf{h} \otimes_{\mathbb{Z}} K$ is embedded in $\prod_P(h_{k(P)+1,\psi_P} \otimes_{\mathbb{Z}} K)$. We write $E = \prod_P E_P$, which is an idempotent of $\prod_P(h_{k(P)+1,\psi_P} \otimes_{\mathbb{Z}} K)$ but may not be in $(\prod_P h_{k(P)+1,\psi_P}) \otimes_{\mathbb{Z}} K$. The closure $\widehat{\mathbf{h}\otimes_{\mathbb{Z}} K}$ of $\mathbf{h} \otimes_{\mathbb{Z}} K$ inside $\prod_P(h_{k(P)+1,\psi_P} \otimes_{\mathbb{Z}} K)$ contains E, and $E(\widehat{\mathbf{h}\otimes_{\mathbb{Z}} K})$ is free of finite rank over $W[[T]][\frac{1}{p}]$ (though $\widehat{\mathbf{h}\otimes_{\mathbb{Z}} K}$ could be huge). Each irreducible component of $E(\widehat{\mathbf{h}\otimes_{\mathbb{Z}} K})$ gives rise to another p-adic analytic family of slope 0.

Pick an arithmetic point P, and write $\alpha = a_P(p)$. Take an irreducible component $\mathrm{Spec}(\mathbb{I}^\circ_\sigma)$ of $\mathrm{Spec}(\mathbb{I}_\sigma) \cap \mathrm{Spec}(E(\widehat{\mathbf{h}\otimes_{\mathbb{Z}} K}))$. Let P_τ be a factor of $P \otimes_{\mathbb{Z}} K \subset \mathbb{I} \otimes_{\mathbb{Z}} K = \prod_\sigma \mathbb{I}_\sigma$ corresponding to $\mathbb{I}^\circ_\sigma$. Regarding $P_\tau : \mathbb{I}^\circ_\sigma \to \overline{\mathbb{Q}}_p$, we have $P_\tau(\alpha) = \tau(\alpha)$ and $f_{P_\tau} = f_P^\tau$. Since $\mathbb{I}_\sigma \subset E(\widehat{\mathbf{h}\otimes_{\mathbb{Z}} K})$, we have $|\tau(\alpha)|_p = 1$. The image $a_\sigma(p)$ of $a(p) \otimes 1$ in $\mathbb{I}_\sigma$ modulo P_τ gives the unit $\tau(a_P(p))$; so, $a_\sigma(p)$ is a unit in the integral closure of $W[[T]]$ in $\mathbb{I}_\sigma$.

Here is a more down-to-earth proof of the fact that $\mathbb{I}^\circ_\sigma$ above gives rise to another analytic family $\mathcal{F}_\sigma$ containing f_P^τ. Start with another arithmetic $(Q : \mathbb{I} \to \overline{\mathbb{Q}}_p) \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$, but regarding Q as a prime divisor of $\mathrm{Spec}(\mathbb{I})$, $\mathbb{I}/Q$ has a unique embedding $\mathbb{I}/Q \subset \overline{\mathbb{Q}}_p$ induced by $Q : \mathbb{I} \to \overline{\mathbb{Q}}_p$. Then $\mathbb{I}^\circ_\sigma/Q_{\tau'} \subset \mathbb{I}/P \otimes_{\mathbb{Z}} K$ for corresponding $Q_{\tau'} \in \mathrm{Spec}(\mathbb{I}^\circ_\sigma)(\overline{\mathbb{Q}}_p)$. Indeed, tensoring K to the exact sequence $\mathrm{Ker}(Q) \hookrightarrow \mathbb{I} \twoheadrightarrow \mathrm{Im}(Q)$, we get another exact sequence: $\mathrm{Ker}(Q) \otimes_{\mathbb{Z}} K \hookrightarrow \prod_\sigma \mathbb{I}_\sigma \twoheadrightarrow \mathrm{Im}(Q) \otimes_{\mathbb{Z}} K$, and $\mathrm{Im}(Q) \otimes_{\mathbb{Z}} K$ contains $\sigma(K)K$ canonically and τ' coincides with σ on $K \cap \mathbb{Q}(f_Q)$ and induces $\tau' = Q_{\tau'}|_{\overline{\mathbb{Q}}\cap W} : \overline{\mathbb{Q}} \cap W \hookrightarrow \overline{\mathbb{Q}}_p$. Then we have $f_{Q_{\tau'}} = f_Q^{\tau'}$ which is a classical modular form. It is slope 0 with respect to i_p (i.e., with respect to the product topology $\prod_P \mathcal{T}_P$) because of $E \cdot \mathbb{I}^\circ_\sigma = \mathbb{I}^\circ_\sigma$. Thus $\mathcal{F}_\sigma$ is another slope 0 family. We rewrite

$\sigma_{Q,\sigma}$ for τ'. Let $\pi_\sigma : \mathbb{I} \otimes_{\mathbb{Z}} K \to \mathbb{I}^\circ_\sigma$ be the projection. We have a commutative diagram

$$\begin{array}{ccc} \mathbb{I}/Q & \xrightarrow{\pi_\sigma} & \mathbb{I}^\circ_{\mathfrak{p}}/Q_{\tau'} \\ \uparrow \cup & & \uparrow \cup \\ \widehat{K} & \xrightarrow[\tau'=\sigma_{Q,\sigma}]{} & \widehat{\sigma(K)K}, \end{array}$$

where $\widehat{K}$ is the closure of K in $\mathbb{I}/Q$ and $\widehat{\sigma(K)K}$ is the closure of $\sigma(K)K$ in $\mathbb{I}^\circ_\sigma/Q_\tau$.

Take K to be the maximal real subfield of M (not to have complex conjugation c with $|a_P(p)^c|_p < 1$). Take the starting P to be P_0. Write simply Σ_0 for Σ_{α_0}. Then the set I of embeddings of K into $\overline{\mathbb{Q}}_p$ is in bijection to Σ_0, and $\sigma_{P_0,\sigma}|_M \in \Sigma_0$. By the assumption (2), any prime $\mathfrak{p}|p$ in K splits as $\mathfrak{p} = \mathfrak{P}\overline{\mathfrak{P}}$ in M and $M_{\mathfrak{P}} = K_{\mathfrak{p}} = M_{\overline{\mathfrak{P}}}$; so, $M \subset \widehat{K}$ non-canonically. Since $\alpha_0 = a_{P_0}(p)$ generates M and $\{K \hookrightarrow \sigma(K)K \big| \sigma \in \Sigma_0\}$ cover all conjugates of K inside $\overline{\mathbb{Q}}$, for any $\sigma \neq \sigma'$ in I we find $\sigma_{P_0,\sigma}(\alpha_0) \neq \sigma_{P_0,\sigma'}(\alpha_0)$. Thus we have at least $|I|$ distinct families: $\{\mathcal{F}_\sigma\}_{\sigma\in I}$. In other words, the set Σ_Q of p-adic embeddings of M induced by $\{\sigma_{Q,\sigma}\}_{\sigma\in I}$ for $Q \in \mathcal{A}$ is a p-adic CM type of M. Here a p-adic CM type is a CM type $\Sigma = \{\sigma : M \hookrightarrow \overline{\mathbb{Q}}_p\}$ of M such that, writing Σ_p for the set of p-adic places induced by $\sigma \in \Sigma$, $\Sigma_p \cap \Sigma_p^c = \emptyset$ for complex conjugation c on M.

Since there are only finitely many p-adic CM types of M, replacing $\mathcal{A}$ by an infinite subset, we may assume that Σ_P is identical to a p-adic CM type Σ for all $P \in \mathcal{A}$. This forces $(a_P(p)) = \prod_{\mathfrak{p}\in\Sigma_p^c} \mathfrak{p}^{e(\mathfrak{p})k(P)}$ for the absolute ramification index $e(\mathfrak{p})$ of $\mathfrak{p}/(p)$.

As before we choose an infinite sequence in $\mathcal{A}$

$$P_1, P_2, \cdots, P_n, \ldots$$

with increasing weight $k(P_1) < k(P_2) < \cdots$ such that

$$(a_{P_j}(p)) = \prod_{\mathfrak{p}\in\Sigma_p^\rho} \mathfrak{p}^{e(\mathfrak{p})k(P_j)}$$

for all $j > 0$. Then $a_{P_j}(p)/\langle\alpha\rangle^{k(P_j)}$ is a Weil number of weight 0, that is, it is an algebraic integer with all its conjugates having absolute value 1. Then by Kronecker's theorem, we find $a_{P_j}(p) = \zeta_{P_j}\langle\alpha\rangle^{k(P_j)}$ for a root of unity ζ_{P_j}. Note that $\langle\alpha\rangle$ is contained in a finite extension K'/K. Since there are finitely many roots of unity in K', we have only finitely many possibilities of ζ_{P_j}. Therefore, replacing $\{P_j\}_j$ by its subsequence, we find an infinite sequence $P_1, P_2, \cdots, P_n, \cdots$ of increasing weights such that $a_{P_j}(p) = \zeta\langle\alpha\rangle^{k(P_j)}$ for all $j = 1, 2, \ldots$ for a fixed root of unity ζ. By the same argument as before, we conclude $A = \Phi_\alpha$, as desired. □

2.2. **Proof of the vertical theorem.** Suppose that $\mathcal{V}_{\mathcal{A}}(\mathbb{I})$ is a finite extension and the existence of an arithmetic point P_0 as in the theorem. Therefore the assumption (2) of Proposition 2.3 is met. By Proposition 2.3, we find a Weil number α of weight 1 and a power series $\Phi_\alpha(X) \in W[[X]]$ such that $a(p, f_P) = \Phi_\alpha(\varepsilon_P(\gamma)\gamma^{k(P)} - 1) = \zeta(\varepsilon_P(\gamma))^{\log_p(\alpha)/\log_p(\gamma)}\langle\alpha\rangle^{k(P)}$ for all arithmetic P, where ζ is a root of unity independent of P; in short, $a(p) = \Phi_\alpha \in W[[X]] \subset \mathbb{I}$. Then, for the entire set $\mathcal{B}$ of arithmetic points P with $k(P) = 1$, we find $\mathcal{H}_{\mathcal{B}}(\mathbb{I}) \subset \mathbb{Q}(\mu_{p^\infty(p-1)})(\zeta, \alpha)$ which is a finite extension of $\mathbb{Q}(\mu_{p^\infty})$. Then by the horizontal theorem, $\mathbb{I}$ has complex multiplication. The converse is easy. This finishes the proof of Theorem 2.2.

We could make the following conjecture which is a vertical version of Corollary 1.9:

Conjecture 2.4. *Let $\mathcal{A} \subset \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ be an infinite set of arithmetic points P with bounded level $r(P) \leq r$. Suppose that $\mathbb{I}$ does not have complex multiplication. Then we have*

$$\limsup_{P \in \mathcal{A}} [\mathbb{Q}(a(p, f_P)) : \mathbb{Q}] = \infty.$$

3. Lecture 3: Constancy of adjoint $\mathcal{L}$-invariant

Consider a cuspidal slope 0 family of Hecke eigenforms $\mathcal{F} = \{f_P | P \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)\}$ indexed by points of $\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ and its family of Galois representations $\{\rho_P\}_P$. For each p-decomposition subgroup $D \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have $\rho_P|_D \cong \left(\begin{smallmatrix} \epsilon_P & * \\ 0 & \delta_P \end{smallmatrix}\right)$ with unramified quotient character δ_P (e.g., [GME] Theorem 4.2.6). Here, for each $P \in \mathrm{Spec}(\mathbb{I})$, f_P is a p-adic modular form of slope 0 of level $Np^{r(P)+1}$ for a fixed prime to p-level N ($p \nmid N$). Consider the adjoint representation $Ad(\rho_P)$ realized in the trace zero subspace in $\mathfrak{sl}_2(\kappa(P)) \subset M_2(\kappa(P))$ by conjugation action. Thus $Ad(\rho_P)(Frob_p)$ has an eigenvalue 1; so, $L_p(s, Ad(\rho_P))$ has an exceptional zero of order 1 at $s = 1$. For the $\mathcal{L}$-invariant $\mathcal{L}(Ad(\rho_P))$ defined by Greenberg [Gr] (see also [HMI] §1.5.2), his conjecture $\mathcal{L}^{an}(Ad(\rho_P)) \stackrel{?}{=} \mathcal{L}(Ad(\rho_P))$ is still an open question. Anyway we get a function $P \mapsto \mathcal{L}(Ad(\rho_P))$ defined on the set of arithmetic points of $\mathrm{Spec}(\mathbb{I})$. This function is interpolated analytically on $\mathrm{Spec}(\mathbb{I})$. We still write $P \mapsto \mathcal{L}(Ad(\rho_P))$ for this analytic function (see [H04b]). Supposing almost known Conjecture 3.5, we prove in this lecture

Theorem 3.1. *The analytic function $P \mapsto \mathcal{L}(Ad(\rho_P))$ is constant if and only if the family $\mathcal{F}$ has CM.*

By this theorem, if $\mathcal{F}$ is a non CM family, $P \mapsto \mathcal{L}(Ad(\rho_P))$ is a non-constant function; so, except for finitely many Galois representations in the family, the conjecture of Greenberg (see [Gr]) predicting the non-vanishing of $\mathcal{L}(Ad(V))$ is true.

Conjecture 3.2. *For a slope 0 parallel weight family (i.e., a cyclotomic family) of Hilbert modular Galois representations $\{\rho_P\}_{P \in \mathrm{Spec}(\mathbb{I})}$, $P \mapsto \mathcal{L}(Ad(\rho_P))$ is constant if and only if the family $\mathcal{F}$ has CM.*

The conjecture implies that for a non-CM component, $P \mapsto \mathcal{L}(\mathrm{Ind}_F^{\mathbb{Q}} Ad(\rho_P))$ is non-constant; so, it vanishes only on a thin proper Zariski closed set in the component.

The Galois representation $\rho_{\mathbb{I}}$ restricted to the p-decomposition group D is reducible. We write $\rho_{\mathbb{I}}^{ss}$ for its semi-simplification over D. Then $\rho_{\mathbb{I}}$ satisfies, for primes $l \nmid Np$,

$$\text{(Gal)} \quad \mathrm{Tr}(\rho_{\mathbb{I}}(Frob_l)) = a(l), \quad \rho_{\mathbb{I}}^{ss}([\gamma^s, \mathbb{Q}_p]) \sim \left(\begin{smallmatrix} (1+T)^{-s} & 0 \\ 0 & 1 \end{smallmatrix}\right), \quad \rho_{\mathbb{I}}^{ss}([p, \mathbb{Q}_p]) \sim \left(\begin{smallmatrix} * & 0 \\ 0 & a(p) \end{smallmatrix}\right),$$

where $\gamma^s = (1+p)^s \in \mathbb{Z}_p^\times$ for $s \in \mathbb{Z}_p$ and $[x, \mathbb{Q}_p]$ is the local Artin symbol.

Recall that the family has CM if one of the following four conditions is satisfied:

(1) there exists an arithmetic point $P \in \mathrm{Spec}(\mathbb{I})$ and a nontrivial Galois character χ such that $\rho_P \otimes \chi \cong \rho_P$,
(2) for all arithmetic points $P \in \mathrm{Spec}(\mathbb{I})$ and a nontrivial Galois character χ, we have $\rho_P \otimes \chi \cong \rho_P$,

(3) there exists an arithmetic point $P \in \mathrm{Spec}(\mathbb{I})$ such that f_P is a theta series of a binary quadratic form,
(4) for all arithmetic points $P \in \mathrm{Spec}(\mathbb{I})$, f_P is a theta series of a binary quadratic form.

If $\mathcal{F}$ has CM, χ cuts out an imaginary quadratic field M, and $\rho_{\mathbb{I}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \Psi$ for a character $\Psi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \mathbb{I}^\times$. The decomposition $(\rho_{\mathbb{I}}|_D)^{ss} = \epsilon \oplus \delta$ can only happen if p splits into $\mathfrak{p}\overline{\mathfrak{p}}$ in M so that Ψ ramifies at $\mathfrak{p}$ and $\Psi^c(\sigma) = \Psi(c\sigma c^{-1})$ is unramified at $\mathfrak{p}$. Then D is the decomposition grup of $\mathfrak{p}$, $\epsilon = \Psi$ and $\delta = \Psi^c$. Write R for the integer ring of M. At an arithmetic point, f_P is the theta series of a Hecke character λ_P whose p-adic avatar $\Psi_P = P \circ \Psi$ has p-type $\Psi_P([x, M_{\mathfrak{p}}]) = \psi_1 \varepsilon_P(x)\langle x\rangle^{-k(P)}$ $(x \in R_{\mathfrak{p}}^\times)$ identifying $R_{\mathfrak{p}}$ with $\mathbb{Z}_p$, and $\Psi_P^c([\mathfrak{p}, M_{\mathfrak{p}}]) = \Psi_P^c([p, M_{\mathfrak{p}}]) = a(p)$; so,

$$a(p) = \zeta_0 (1+T)^{\log_p(\overline{\mathfrak{p}})/\log(\gamma)}$$

for a root of unity ζ_0, where $\log_p(\overline{\mathfrak{p}}) = \frac{1}{h}\log_p(\alpha)$ taking h such that $\overline{\mathfrak{p}}^h = (\alpha)$ with $\alpha \in M$.

Here is a version of Lemma 1.6 ([C] Theorem 4.3) I explained in the first lecture:

Lemma 3.3. *Let $\overline{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$. If a power series $\Phi(T) \in \mathcal{O}_{\widehat{\mathbb{G}}_m} = \overline{\mathbb{F}}_p[[T]]$ regarded as a function of $t = 1+T$ satisfies $\Phi(t^z) = \Phi(t)^z$ for z in a open subgroup of $\mathbb{Z}_p^\times$, then $\Phi(t) = c \cdot t^s$ for $s \in \mathbb{Z}_p$ with a constant $c \in \overline{\mathbb{F}}_p$.*

3.1. **Proof of Theorem 3.1.** By (1.6) of [H04b], $\mathcal{L}(Ad(\rho_P))$ is a constant multiple of

$$\left(a(p)^{-1}\frac{da(p)}{dX}\right)\Big|_{X=0},$$

where if $P \cap \Lambda = (X)$ for $X = \gamma^{-k}\zeta^{-1}t - 1$ for $t = 1+T$. After proving the theorem assuming this formula, we recall the proof of the formula. By variable change (as $T = \log_p(t) \mod T^2$), we get

$$\left(a(p)^{-1}\frac{da(p)}{dX}\right)\Big|_{X=0} = \left(a(p)^{-1}t\frac{da(p)}{dt}\right)\Big|_{t=\zeta\gamma^k}.$$

Thus the constancy of $\mathcal{L}(Ad(\rho_P))$ implies the constancy of

$$a(p)^{-1}(1+T)\frac{da(p)}{dT} = a(p)^{-1}t\frac{da(p)}{dt} = s \in W.$$

Thus $t\frac{da}{dt} = s \cdot a$ for $a(t) = a(p)(t)$ for $s \in W$. In other words, putting $b(x) = \log_p \circ a(\exp_p(x))$ (for $x = \log_p(t)$), as $dx = \frac{dt}{t}$, we get from the chain rule,

$$\frac{db}{dx} = \frac{da}{dx}\frac{db}{da} = \frac{da}{dx}\frac{d\log_p(a)}{da} = s \cdot a \cdot \frac{1}{a} = s.$$

Thus b is a linear function of x with slope s:

$$\log_p(a) = sx + c \Leftrightarrow a = C\exp_p(s \cdot \log_p(t)) = Ct^s \quad (C = \exp_p(c)).$$

Then $a(p) = Ct^s \in K[[T]] \cap \mathbb{I} = W[[T]]$ $(t^s = \exp_p(s \cdot \log_p(t)))$ for the quotient field K of W, and $t^s \in W[[T]]$. Taking $\Phi(t) := t^s \mod \mathfrak{m}_W$ in $\mathbb{F}[[T]]$, we find $\Phi(t^z) = \Phi(t)^z$ for $z \in \mathbb{Z}_p$. Thus by Chai's lemma above, we conclude $s \in \mathbb{Z}_p$. Write $f_\zeta = f_P$ for $P = (X)$ $(X = \gamma^{-k}\zeta^{-1}t - 1)$ with $\zeta \in \mu_{p^r}$. The form f_ζ is a Hecke eigenform in $S_k(\Gamma_1(Np^{r+1}))$, and we have $a(p, f_\zeta) = C\gamma^{ks}\zeta^s$. Take $\zeta = 1$. Then $a(p, f_1) = C\gamma^{ks}$ is a Weil number α of weight k. This shows that for any $\zeta \in \mu_{p^\infty}$, $a(p, f_\zeta) = \alpha$ up to

p-power roots of unity. Thus the field generated by $a(p, f_\zeta)$ for all $\zeta \in \mu_{p^\infty}$ is a finite extension of $\mathbb{Q}[\mu_{p^\infty}]$. Then by the horizontal theorem, we conclude that $\mathcal{F}$ is a CM family.

Conversely, we suppose $\mathcal{F}$ is a CM family. Then we find a Galois character $\Psi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \mathbb{I}^\times$ for an imaginary quadratic field M such that $\rho_P = \mathrm{Ind}_M^{\mathbb{Q}} \Psi \mod P$ for all $P \in \mathrm{Spec}(\mathbb{I})$ and Ψ is unramified at a unique factor $\mathfrak{p}|p$ in M. Then $a(p)$ is the value of the character $\Psi^c(Frob_{\mathfrak{p}})$ at the Frobenius element $Frob_{\mathfrak{p}}$ at $\mathfrak{p}$. As already explained, we have $\Psi^c(Frob_{\mathfrak{p}}) = t^{\log_p(\overline{\mathfrak{p}})/\log_p(\gamma)}$ up to a root of unity. This shows the constancy of $\mathcal{L}$-invariant for the CM family. $\square$

3.2. **Recall of $\mathcal{L}$-invariant.** According to Mazur–Tate–Teitelbaum [MTT], the $\mathcal{L}$–invariant times the archimedean L-value give the leading term of the Taylor expansion of a given p–adic motivic L–function at an exceptional zero. For an elliptic curve $E_{/\mathbb{Q}}$ with multiplicative or ordinary good reduction modulo p, its p–adic L–function $L_p(s, E)$ has the following evaluation formula at $s = 1$:

$$L_p(1, E) = (1 - a_p^{-1})\frac{L_\infty(1, E)}{\text{period}},$$

where $L_\infty(s, E)$ is the archimedean L–function of E, and a_p is the eigenvalue of the arithmetic Frobenius element at p on the unramified quotient of the p–adic Tate module $T(E)$ of E. If E has *split* multiplicative reduction, $a_p = 1$, $L_p(s, E)$ has zero at $s = 1$. This type of zero of a p–adic L–function resulted from the modification Euler p–factor is called an *exceptional zero*, and it is believed that if the archimedean L–values does not vanish, the order of the zero is the number e of such Euler p–factors; so, in this case, $e = 1$. Then $L_p'(1, E) = \frac{dL_p(s,E)}{ds}|_{s=1}$ is conjectured to be equal to the archimedean value $\frac{L_\infty(1,E)}{\text{period}}$ times an error factor $\mathcal{L}^{an}(E)$, the so-called $\mathcal{L}$–invariant:

$$L_p'(1, E) = \mathcal{L}^{an}(E)\frac{L_\infty(1, E)}{\text{period}}.$$

The problem of $\mathcal{L}$–invariants is to find an explicit formula (without recourse to p–adic L–functions) for motivic p–adic Galois representations V. Writing $E(\overline{\mathbb{Q}}_p) = \overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}$ for the Tate period $q \in p\mathbb{Z}_p$, the solution conjectured by [MTT] and proved by Greenberg-Stevens [GS] is

$$\mathcal{L}^{an}(E) = \frac{\log_p(q)}{\mathrm{ord}_p(q)}.$$

Since E is modular, $L(s, E) = L(s, f_E)$ for an elliptic Hecke eigenform f_E of weight 2. In particular, $a(p, f_E) = a_p = 1$ and $a(1, f_E) = 1$. We can lift f_E to a unique family $\mathcal{F}_{\mathbb{I}}$ so that f_E is a specialization of $\mathcal{F}$ at an arithmetic P with $k(P) = 1$. Then one of the key ingredients of their proof is the following formula:

$$\mathcal{L}^{an}(E) = -2\log_p(\gamma)\frac{da(p)}{dX}\Big|_{X=0}.$$

Here is an analogous formula in [H04b]:

Theorem 3.4. *Let p be an odd prime, and assume* Conjecture 3.5 *in the following section. Then we have*

$$\mathcal{L}(Ad(\rho_P)) = -2\log_p(\gamma)a_P(p)^{-1}\frac{da(p)}{dX}\Big|_{X=0}.$$

3.3. **Galois deformation.** A main ingredient of the proof of Theorem 3.4 is Galois deformation theory. Since ρ_P is irreducible and $\mathrm{Tr}(\rho_{\mathbb{I}}) \in \mathbb{I}$, via pseudo representation, we arrange $\rho_{\mathbb{I}}$ to have values in $\mathbb{I}_P$. Let $\widehat{\mathbb{I}}_P = \varprojlim_n \mathbb{I}_P/P^n\mathbb{I}_P$. It is known that $\widehat{\mathbb{I}}_P \cong \kappa(P)[[X]]$ (see [HMI] Proposition 3.78). The character $\det(\rho_{\mathbb{I}})^{-1}\det(\rho)$ has values in the p-profinite group $1+\mathfrak{m}_{\mathbb{I}}$ for the maximal ideal $\mathfrak{m}_{\mathbb{I}}$ of $\mathbb{I}$, and hence we have its unique square root ψ with values in $1+\mathfrak{m}_{\mathbb{I}}$. Define a representation $\boldsymbol{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\widehat{\mathbb{I}}_P)$ with $\det(\boldsymbol{\rho}) = \det(\rho)$ by $(\rho_{\mathbb{I}} \otimes \psi)(\sigma) = \psi(\sigma)\rho_{\mathbb{I}}(\sigma)$. Note that $\boldsymbol{\rho} \equiv \rho_{\mathbb{I}} \mod P$. Fix a decomposition subgroup $D_p \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at p. Normalize ρ_P so that $\rho_P|_{D_p} = \left(\begin{smallmatrix} \epsilon_P & * \\ 0 & \delta_P \end{smallmatrix}\right)$ with unramified δ_P. Then $\epsilon_P \neq \delta_P$ and ϵ_P is ramified.

Simply write $\kappa := \kappa(P)$. Let S be the set of places of $\mathbb{Q}$ made up of all prime factors of Np and ∞. Consider the deformation functor into sets from the category of local artinian κ-algebras with residue field κ whose value at a local artinian κ-algebra A with maximal ideal $\mathfrak{m}_A$ is given by the set of isomorphism classes of 2-dimensional continuous Galois representations $\rho_A : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(A)$ unramified outside S:

(D1) $(\rho_A \mod \mathfrak{m}_A) \cong \rho_P$;

(D2) Writing $\iota : \kappa \to A$ for the structure homomorphism of κ-algebras, we have the identity of the determinant characters:
$$\iota \circ \det(\rho) = \det(\rho_A);$$

(D3) We have an exact sequence $\rho_A|_{D_p} \cong \left(\begin{smallmatrix} \epsilon_A & * \\ 0 & \delta_A \end{smallmatrix}\right)$ with $\delta_A \equiv \delta_P \mod \mathfrak{m}_A$.

The condition (D3) is the near ordinarity, and we call the character δ_A of D_p the *nearly ordinary character* of ρ. By the work started by Wiles/Taylor (and practically ended by Kisin), we know (e.g., [HMI] Corollary 3.77 for most cases) the following conjecture is true for almost all cases:

Conjecture 3.5. *The above functor is pro-represented by the pair* $(\widehat{\mathbb{I}}_P, \boldsymbol{\rho})$.

In the following sections, we start with a brief review of the definition by Greenberg of the Selmer group and his $\mathcal{L}$–invariant.

3.4. **Selmer Groups.** We describe the definition due to Greenberg of his Selmer group associated to the adjoint square Galois representation. For simplicity, we assume that $S = \{p, \infty\}$ (so, $N = 1$). One can find the definition in the general case in [Gr] and in [HMI] §1.2.3. We may assume that κ has p-adic integer ring W. Let $\mathbb{Q}^S$ be the maximal extension unramified outside S. All Galois cohomology groups are continuous cohomology groups in [MFG] 4.3.3. Write $\mathfrak{G}^S = \mathrm{Gal}(\mathbb{Q}^S/\mathbb{Q})$ and I_p for the inertia subgroup of the decomposition subgroup $D_p \subset \mathfrak{G}^S$.

Write V for the space of ρ_P. Let $\mathfrak{G}^S$ act on $\mathrm{End}_\kappa(V)$ by conjugation and put $Ad(V) \subset \mathrm{End}_\kappa(V)$ (the trace 0 subspace of dimension 3). We have a filtration:

$$V \supsetneq F^+V \supsetneq \{0\} \tag{ord}$$

stable under the decomposition group D_p such that D_p acts on the quotient V/F^+V by δ_P. Then $Ad(V)$ has the following three step filtration stable under D_p:

$$Ad(V) \supset F^-Ad(V) \supset F^+Ad(V) \supset \{0\}, \tag{F}$$

where

$$F^-Ad(V) = \{\phi \in Ad(V) | \phi(F^+V) \subset F^+V\} \ \ \text{(upper triangular)},$$
$$F^+Ad(V) = \{\phi \in Ad(V) | \phi(F^+V) = 0\} \ \ \text{(upper nilpotent)}.$$

Note that D_p acts trivially on $F^-Ad(V)/F^+Ad(V)$; so, $F^-Ad(V)/F^+Ad(V) \cong \kappa$; so, the p-adic L-function of $Ad(V)$ has an exceptional zero at $s=1$. Put

$$U_p(Ad(V)) = \mathrm{Ker}(\mathrm{Res} : H^1(D_p, Ad(V)) \to H^1(I_p, \frac{Ad(V)}{F^+(Ad(V))})).$$

Then we define

$$\mathrm{Sel}(Ad(V)) = \mathrm{Ker}(H^1(\mathfrak{G}^S, Ad(V)) \to \frac{H^1(D_p, V)}{U_p(V)}). \tag{3.1}$$

Replacing $U_p(Ad(V))$ by the bigger

$$U_p^-(Ad(V)) = \mathrm{Ker}(\mathrm{Res} : H^1(D_p, Ad(V)) \to H^1(I_p, \frac{Ad(V)}{F^-(Ad(V))}))$$

for $\mathfrak{p}|p$, we can define a bigger "$-$" Selmer group $\mathrm{Sel}^-(Ad(V)) \supset \mathrm{Sel}(Ad(V))$.

In the above definition, replacing $\mathfrak{G}^S$ by the stabilizer $\mathfrak{G}^S_\infty$ of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$ and V by $A = V/L$ for a Galois stable lattice L, one can define the Selmer group $\mathrm{Sel}_{\mathbb{Q}_\infty}(A)$ whose characteristic power series $\Phi(T)$ is supposed to be the adjoint p-adic L-function $L_p(s, Ad(\rho_P))$ (the adjoint main conjecture). It is easy to see $\mathrm{Sel}^-(A)$ is sent (with possibly finite kernel) into $\mathrm{Sel}_{\mathbb{Q}_\infty}(A)$ (as p-ramification of cocycles giving $\mathrm{Sel}^-(A)$ projected to F^-A/F^+A is absorbed by the wild ramification of $\mathbb{Q}_\infty/\mathbb{Q}$). The image produces the exceptional zero of algebraic L-function $s \mapsto \Phi(\gamma^s - 1) =: L_p^{alg}(s, Ad(\rho_P))$ at $s = 1$. Greenberg's philosophy is therefore that the $\mathcal{L}$-invariant must be produced out of cocycles in $\mathrm{Sel}^-(A)$. Assuming $\mathcal{L}(Ad(\rho_P)) \neq 0$, $L_p^{alg}(s, Ad(\rho_P))$ has order 1 zero at $s = 1$ and $L_p'(1, Ad(\rho_P)) = \mathcal{L}(Ad(\rho_P))L(1, Ad(\rho_P))$/period up to units under mild conditions (see [Gr] Proposition 4, [H07b] Theorem 3.1 and [MFG] Theorem 5.20).

Taking the Tate-dual $Ad(V)^*(1) = \mathrm{Hom}_\kappa(Ad(V), \kappa)(1)$ with single Tate twist, and the filtration dual to (F), we define the dual Selmer group $\mathrm{Sel}(Ad(V)^*(1))$.

Lemma 3.6. *Assume Conjecture 3.5. We have* $\dim \mathrm{Sel}^-(Ad(V)) = 1$ *and*

$$\mathrm{Sel}(Ad(V)) = \mathrm{Sel}(Ad(V)^*(1)) = 0. \tag{V}$$

In the earlier article [H04b], the balanced Selmer group $\overline{\mathrm{Sel}}_{\mathbb{Q}}$ (see [Gr] (16) and [HMI] §1.5.1) is used to prove this type of result. However by definition $\mathrm{Sel}_{\mathbb{Q}}(Ad(V)) \supset \overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V))$ and by duality $\mathrm{Sel}_{\mathbb{Q}}(Ad(V)^*(1)) \subset \overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V)^*(1))$. Then by Greenberg (see [Gr] Proposition 2 or [HMI] Proposition 3.82), we have

$$\dim \overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V)) = \dim \overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V)^*(1)),$$

and therefore, to prove the vanishing of all such Selmer groups, we only need to show $\mathrm{Sel}_{\mathbb{Q}}(Ad(V)) = 0$.

Proof. Here is a sketch of the proof. For any derivation $\partial : \widehat{\mathbb{I}}_P \to \kappa$, consider $c_\rho := (\partial\boldsymbol{\rho})\rho_P^{-1} : \mathfrak{G}^S \to \mathrm{End}(V)$. Applying ∂ to $\boldsymbol{\rho}(\sigma)\boldsymbol{\rho}(\tau) = \boldsymbol{\rho}(\sigma\tau)$, we verify c_∂ is cocycle. Since $\det(\boldsymbol{\rho})$ is constant, c_ρ has values in $Ad(V)$. Since $\boldsymbol{\rho}|_{D_p}$ is upper triangular, $[c_\rho] \in \mathrm{Sel}^-(Ad(V))$. By universality, any such cocycle is of the form c_∂. Thus the tangent space $\mathcal{T}_P \cong \kappa$ of $\mathrm{Spec}(\widehat{\mathbb{I}}_P)$ at P is isomorphic to $\mathrm{Sel}^-(Ad(V))$; so, $\dim_\kappa \mathrm{Sel}^-(Ad(V)) = 1$. Since the diagonal entry of c_∂ is non-trivial, $\mathrm{Sel}(Ad(V))$ is a proper subspace of of $\mathrm{Sel}^-(Ad(V))$; so, it vanishes. By Greenberg, $\dim_\kappa \mathrm{Sel}(Ad(V)) = \dim_\kappa \mathrm{Sel}(Ad(V)^*(1))$

(strictly speaking $\dim_\kappa \overline{\mathrm{Sel}}(Ad(V)) = \dim_\kappa \overline{\mathrm{Sel}}(Ad(V)^*(1))$ as remarked; see [HMI] Lemma 1.84); so, the desired vanishing also follows for the dual. $\square$

We have the Poitou-Tate exact sequence (e.g., [MFG] Theorem 4.50 (5)):

$$0 \to \mathrm{Sel}(Ad(V)) \to H^1(\mathfrak{G}^S, Ad(V)) \to \frac{H^1(D_p, Ad(V))}{U_p(Ad(V))} \to \mathrm{Sel}(Ad(V)^*(1))^*.$$

Thus by (V), we have

$$H^1(\mathfrak{G}^S, Ad(V)) \cong \frac{H^1(D_p, Ad(V))}{U_p(Ad(V))}. \tag{I}$$

3.5. **Greenberg's $\mathcal{L}$–invariant.** Greenberg defined in [Gr] his invariant $\mathcal{L}(Ad(V))$ in the following way. Write $F^-H^1(D_p, Ad(V))$ for the image of $H^1(D_p, F^-Ad(V))$ in $H^1(D_p, Ad(V))$. By the definition of $U_p(Ad(V))$, the subspace $\frac{F^-H^1(D_p,Ad(V))}{U_p(Ad(V))}$ inside the right-hand side of (I) is isomorphic to $\mathrm{Sel}^-(Ad(V)) \cong \kappa$. Namely, we have

$$\mathrm{Sel}^-(Ad(V)) \xrightarrow[\mathrm{Res}]{\sim} \frac{F^-H^1(D_p, Ad(V))}{U_p(Ad(V))} \subset \frac{H^1(D_p, Ad(V))}{U_q(Ad(V))}.$$

Then by projecting down to $F^-Ad(V)/F^+Ad(V) \cong \kappa$ with trivial D_p-action, cocycles in $\mathrm{Sel}^-(Ad(V))$ gives rise to a subspace L of

$$\mathrm{Hom}(D_p^{ab}, F^-Ad(V)/F^+Ad(V)) = \mathrm{Hom}(D_p^{ab}, \kappa).$$

Note that

$$\mathrm{Hom}(D_p^{ab}, \kappa) \cong \kappa \times \kappa$$

canonically by $\phi \mapsto (\frac{\phi([u,\mathbb{Q}_p])}{\log_p(u)}, \phi([p, \mathbb{Q}_p]))$ for any $u \in \mathbb{Z}_p^\times$ of infinite order. Here $[x, \mathbb{Q}_p]$ is the local Artin symbol (suitably normalized).

If a cocycle c representing an element in $\mathrm{Sel}^-(Ad(V))$ is unramified, it gives rise to an element in $\mathrm{Sel}(Ad(V))$. By the vanishing (V) of $\mathrm{Sel}(Ad(V))$, this implies $c = 0$; so, the projection of L to the first factor κ (via $\phi \mapsto \phi([u, \mathbb{Q}_p])/\log_p(u)$) is surjective. Thus this subspace L is a graph of a κ–linear map

$$\mathcal{L} : \kappa \to \kappa,$$

which is given by the multiplication by an element $\mathcal{L}(Ad(V)) \in \kappa$.

3.6. **Proof of Theorem 3.4.** Write $\boldsymbol{\rho}|_{D_p} \cong \left(\begin{smallmatrix}\boldsymbol{\epsilon} & * \\ 0 & \boldsymbol{\delta}\end{smallmatrix}\right)$ with nearly ordinary character $\boldsymbol{\delta}$. We know that c_∂ for $\partial = \frac{d}{dX}$ gives a nontrivial element in $\mathrm{Sel}^-(Ad(V))$. The image of c_∂ in $\mathrm{Hom}(D_p^{ab}, \kappa)$ is $\delta_P^{-1}\partial\boldsymbol{\delta}|_{X=0}$. We know that $\delta_P^{-1}\boldsymbol{\delta}([p, \mathbb{Q}_p]) = a_P(p)^{-1}a(p)$ and $\delta_P^{-1}\boldsymbol{\delta}([u, \mathbb{Q}_p]) = (\zeta\gamma^k)^{-\log_p(u)/2\log_p(\gamma)}t^{\log_p(u)/2\log_p(\gamma)}$ by our construction. Then to get the desired result is just a simple computation.

4. Lecture 4: Image of Λ-adic Galois representations modulo p

We call a prime ideal $P \subset \mathbb{I}$ a *prime divisor* if $\mathrm{Spec}(\mathbb{I}/P)$ has codimension 1 in $\mathrm{Spec}(\mathbb{I})$. Put $\Phi(N) = N^2 \prod_{l|N}(1 - \frac{1}{l^2})$ for an integer $N > 1$ and its prime factors l.

Theorem 4.1. *Take a non CM component $\mathbb{I}$ of cube-free prime-to-p level N, and let $P \in \mathrm{Spec}(\mathbb{I})$ be a prime divisor above $(p) \subset \mathbb{Z}_p[[T]]$. If $p \nmid \Phi(N)$, the image of ρ_P contains an open subgroup of $SL_2(\mathbb{F}_p[[T]])$.*

Recall, for primes $l \nmid Np$,

$$\text{(Gal)}\quad \mathrm{Tr}(\rho_{\mathbb{I}}(Frob_l)) = a(l), \quad \rho_{\mathbb{I}}^{ss}([\gamma^s, \mathbb{Q}_p]) \sim \begin{pmatrix} (1+T)^{-s} & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho_{\mathbb{I}}^{ss}([p, \mathbb{Q}_p]) \sim \begin{pmatrix} * & 0 \\ 0 & a(p) \end{pmatrix}.$$

We have a unique decomposition $\mathbb{I}^\times = \langle \mathbb{I}^\times \rangle \times \mu^{(p)}$, where $\mu^{(p)}$ is a finite group of order prime to p and $\langle \mathbb{I}^\times \rangle$ is a p-profinite group. Write $a \mapsto \langle a \rangle$ for the projection to $\langle \mathbb{I}^\times \rangle$. Since $p \geq 5$, $a \in \langle \mathbb{I}^\times \rangle$ has a unique square root $\sqrt{a} \in \langle \mathbb{I}^\times \rangle$. We put $\rho' = \rho_{\mathbb{I}} \otimes \sqrt{\langle \det(\rho_{\mathbb{I}}) \rangle}^{-1}$. Then $\det(\rho')$ has finite image. Since $\mathrm{Im}(\rho_{\mathbb{I}}) \cap SL(2) = \mathrm{Im}(\rho') \cap SL(2)$, we may replace $\rho_{\mathbb{I}}$ by ρ' to prove the theorem. Note here $\mathrm{Im}(\rho')$ contains $\begin{pmatrix} (1+T)^{-s/2} & * \\ 0 & (1+T)^{s/2} \end{pmatrix}$ for all $s \in \mathbb{Z}_p$ by (Gal).

Here is an outline of the proof. For a prime divisor P above $(p) \subset \mathbb{Z}_p[[T]]$, let $\overline{\kappa}(P)$ be an algebraic closure of $\kappa(P)$. The Zariski closure of the image $\mathrm{Im}(\rho'_P) \cap SL(2)$ in $SL(2)_{/\overline{\kappa}(P)}$ is an algebraic subgroup G_P of $SL(2)_{/\overline{\kappa}(P)}$ defined over $\kappa(P)$. Let G_P° be the connected component of G_P. Then G_P° is either Borel subgroup, a torus or a unipotent group. Since $G_P^\circ(\kappa(P))$ contains $\begin{pmatrix} (1+T)^{-s/2} & * \\ 0 & (1+T)^{s/2} \end{pmatrix}$, G_P° is not a unipotent group. If G_P° is a Borel subgrup or a torus, we prove that P has to be either an Eisenstein ideal or the family has congruence modulo P with a CM component $\mathbb{I}'$ having CM by an imaginary quadratic field M. In the Eisenstein case, by a result of Mazur–Wiles [MW] and Ohta [O1], P divides the Iwasawa power series of a Kubota-Leopoldt p-adic L-function. This is impossible as the Kubota–Leopoldt p-adic L-function has trivial μ-invariant [FeW]. In the CM case, P divides $L_p(Ad(\rho_{\mathbb{I}'})) = h \cdot L_p(\Psi_{\mathbb{I}'}^-)$ (congruence criterion) for the class number h of M as remarked in Lecture 1, where $L_p(\Psi_{\mathbb{I}'}^-)$ is the anticyclotomic p-adic Hecke L-function constructed by de Shalit, Yager and Katz (see [K] and [H07b]). By [Fi] and [H10], the anticyclotomic p-adic Hecke L-function has trivial μ-invariant (under $p \nmid \Phi(N)$); so, if $p \nmid h$, this proves the theorem. If $p|h$, by computation of the congruence power series, we prove that the congruence between CM components exhausts the p-part of the congruence power series, and thereby, we conclude that G_P is $SL(2)$, and (Gal) implies, by a result of Pink [P], that ρ_P to have the open image property.

This type of results, asserting $\mathrm{Im}(\rho_P)$ contains an open subgroup of $SL_2(\mathbb{Z}_p)$ for non CM arithmetic primes P was proven by Ribet [R] long ago. If $p|\Phi(N)$, the theorem could fail. We make the following conjecture in the Hilbert modular case over a totally real field F with integer ring O:

Conjecture. *Let $\mathcal{F}_{\mathbb{I}}$ be a non CM parallel weight Hilbert modular family (in* [H88b]*) of prime-to-p level $\mathfrak{N}$ for a totally real field F. Suppose $p \geq 5$, and let P be a prime divisor of $\mathbb{I}$ over $(p) \subset \mathbb{Z}_p[[T]]$. Then we have*

1. *The mod P Galois representation ρ_P is irreducible over $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$.*
2. *Suppose $p \nmid \Phi_F(\mathfrak{N}) = N(\mathfrak{N})^2 \prod_{\mathfrak{l}|\mathfrak{N}}(1 - \frac{1}{N(\mathfrak{l})^2})$ and that $\mathfrak{N}$ is prime to p and cube free. If either $\dim_F F[\mu_p] > 2$ or the strict class number of F is odd, ρ_P*

contains a subgroup isomorphic to an open subgroup of $SL_2(\mathbb{F}_p[[T]])$, *where* $\det(\rho_{\mathbb{I}}([\gamma_F^s, \mathbb{Q}_p])) = (1+T)^s$ *for a generator* γ_F *of* $\gamma^{\mathbb{Z}_p} \cap N_{F/\mathbb{Q}}(O_p^\times)$.

If $\dim_F F[\mu_p] = 2$ and F has a CM quadratic extension unramified everywhere, the μ-invariant of the anticyclotomic p-adic Hecke L-function could be positive [H10] (M1–3); so, irreducibility is at most we could expect under such circumstance. The above conjecture is almost equivalent to vanishing of the μ-invariant of Deligne–Ribet p-adic L and of Katz p-adic L restricted to anticyclotomic parallel weight variable.

Here is a general fact from the theory of new/old forms:

Proposition 4.2. *Let* $\pi = \otimes_l \pi_l$ *be an irreducible cuspidal automorphic representation of* $GL_2(\mathbb{A})$ *of weight* $k+1$ *with central character* ψ. *Write* $C(\pi)$ *for the conductor of* π. *Fix a prime* l, *and write* π_l *for its* l*-component. For a new vector* $f \in \pi$, *write* $f|T(l) = a \cdot f$ *and defining* α, β *to be the two roots of* $X^2 - aX + \psi(l)l^k = 0$ *if* π_l *is spherical. Then the following is the list of all Hecke eigenvectors in* π *whose eigenvalues for* $T(q)$ *with* $q \neq l$ *coincide with those for* f:

(1) *If* π_l *is spherical, in addition to* f, *we have* f_α, f_β, f_0 *such that* $f_x|U(l) = x \cdot f_x$ *(here* $f_\alpha = f_\beta$ *if* $\alpha = \beta$*), where the minimal level of* f_α, f_β, f_0 *are, respectively,* $C(\pi)l, C(\pi)l$ *and* $C(\pi)l^2$;
(2) *If* π_l *is Steinberg, we have* $f_a = f, f_0$ *under the same convention as above, where the minimal level of* f_a, f_0 *are, respectively,* $C(\pi)$ *and* $C(\pi)l$;
(3) *If* π_l *is supercuspidal,* $f = f_0$.

The above vector f_x *is determined by* x *up to constant multiple.*

In the spherical case (1), if f is a new form in π, $f_\alpha(z) = f(z) - \beta f(lz)$. If $\alpha = \beta$, $U(l)$ gives a nontrivial nilpotent. If f is of weight 2 and $l^3 \nmid C(\pi)$, $\alpha \neq \beta$ by Coleman–Edixhoven [CE]; so, $U(l)$ on such π is semi-simple if $l^3 \nmid C(\pi)$. For simplicity, we assume that $\mathbf{h}$ is a reduced algebra (which is true if N is cube-free by [CE]).

4.1. **CM components.** Let $\mathrm{Spec}(\mathbb{I}^M_{cm})$ be the union inside $\mathrm{Spec}(\mathbf{h})$ of all irreducible components having CM by a fixed imaginary quadratic field M. Consider the ray class group $Cl_M(\mathfrak{c}\mathfrak{p}^r)$ modulo $\mathfrak{c}\mathfrak{p}^r$ (of M) for $\mathfrak{c}$ prime to p and put $C = \varprojlim_r Cl_M(\mathfrak{c}\mathfrak{p}^r)$. Let $M_{\mathfrak{c}}/M$ be the ray class field with $\mathrm{Gal}(M_{\mathfrak{c}}/M) \cong C$. If $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbb{I}^{cm}_M)$, we have a unique ideal $\mathfrak{c} = \mathfrak{c}(\mathbb{I})$ prime to p such that $\mathfrak{c}\bar{\mathfrak{c}}D_M|N$ and $\rho_{\mathbb{I}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \Psi$ for a character $\Psi : \mathrm{Gal}(M_{\mathfrak{c}}/M) \to \mathbb{I}^\times$. Since $\mathfrak{c}\bar{\mathfrak{c}}D_M|N$, each prime factor $\mathfrak{l}$ of $\mathfrak{c}$ divides N. The ideal $\mathfrak{c}(\mathbb{I})$ is determined in the following way:

(1) If $(l) = \mathfrak{l}\bar{\mathfrak{l}}$ and $a(l) \neq 0$, we have one of factors of l, say $\bar{\mathfrak{l}}$ such that $a(l) = \Psi(\bar{\mathfrak{l}})$, and in this case, $\mathfrak{c}$ is prime to $\bar{\mathfrak{l}}$ and $\mathrm{ord}_{\mathfrak{l}}(\mathfrak{c}) = \mathrm{ord}_l(N)$, where $\mathfrak{c} = \prod_{\mathfrak{l}} \mathfrak{l}^{\mathrm{ord}_{\mathfrak{l}}(\mathfrak{c})}$ and $N = \prod_l l^{\mathrm{ord}_l(N)}$.
(2) If $(l) = \mathfrak{l}\bar{\mathfrak{l}}$ and $a(l) = 0$, $\mathrm{ord}_{\mathfrak{l}}(\mathfrak{c}) = \mathrm{ord}_{\bar{\mathfrak{l}}}(\mathfrak{c}) = 1$ and $\mathrm{ord}_l(N) = 2$.
(3) If $\mathfrak{l} = (l)$ is inert and $a(l) \neq 0$, we have $a(l) = \pm\sqrt{\Psi(l)}$, $\mathrm{ord}_{\mathfrak{l}}(\mathfrak{c}) = 0$ but $1 \leq \mathrm{ord}_l(N) \leq 2$.
(4) If $\mathfrak{l} = (l)$ is inert and $a(l) = 0$, $\mathrm{ord}_l(\mathfrak{c}) = 1$ and $\mathrm{ord}_l(N) = 2$.
(5) If $\mathfrak{l}^2 = (l)$ and $a(l) \neq 0$, $a(l) = \Psi(\mathfrak{l})$, $\mathrm{ord}_{\mathfrak{l}}(\mathfrak{c}) = 0$ but $1 \leq \mathrm{ord}_l(N) \leq 2$.
(6) If $\mathfrak{l}^2 = (l)$ and $a(l) = 0$, $\mathrm{ord}_{\mathfrak{l}}(\mathfrak{c}) = 1$ but $\mathrm{ord}_l(N) = 2$.

For any prime $\mathfrak{a}$ prime to $\mathfrak{c}\mathfrak{p}$, we write $[\mathfrak{a}]$ for the class lof $\mathfrak{a}$ in C. If $\mathfrak{a}$ is not prime to $\mathfrak{c}\mathfrak{p}$, we put $[\mathfrak{a}] = 0$ in $W[[C]]$. Let C_p be the Sylow p-part of C. Then $C = C^{(p)} \times C_p$ with finite group $C^{(p)}$ of order prime to p. We write Δ for the maximal finite subgroup of C_p, and put $\Gamma_M := C_p/\Delta \cong \mathbb{Z}_p$. Pick a CM irreducible component $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbf{h})$, and let $\mathrm{Spec}(\mathbb{T})$ be the connected component of $\mathrm{Spec}(\mathbf{h})$ containing $\mathrm{Spec}(\mathbb{I})$. We assume $W = \overline{\mathbb{Q}}_p \cap \mathbb{I}$. We define $\mathrm{Spec}(\mathbb{T}_{cm}) \subset \mathrm{Spec}(\mathbb{T})$ by the union of all CM components of $\mathrm{Spec}(\mathbb{T})$. Let Q be the quotient field of $\mathbb{Z}_p[[T]]$ and $\overline{Q}$ be an algebraic closure of Q, and regard $\mathbb{I}$ as a subalgebra of $\overline{Q}$ by a fixed embedding over $W[[T]]$.

We list here easy consequences of explicit form of CM components: Let M and L be distinct imaginary quadratic fields in which p splits.

Fact 1. If $P \in \mathrm{Spec}(\mathbb{I}^M_{cm}) \cap \mathrm{Spec}(\mathbb{I}^L_{cm})$ is a prime divisor, P contains T; so, it is prime to (p).

Fact 2. Let $\mathbb{I}$ and $\mathbb{I}'$ be two distinct CM components in $\mathbb{T}_{cm}$, and write $a(l)$ and $a'(l)$ for the image of $T(l)$ in $\mathbb{I}$ and $\mathbb{I}'$, respectively. If $a(l) = \sigma(a'(l))$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ for almost all l, any prime divisor $P \in \mathrm{Spec}(\mathbb{I}) \cap \mathrm{Spec}(\mathbb{I}')$ is prime to (p).

Fact 3. By the explicit form of theta series of M,

$$\mathbf{h} \ni T(l) \mapsto \begin{cases} [\mathfrak{l}] + [\bar{\mathfrak{l}}] & \text{if } (l) = \mathfrak{l}\bar{\mathfrak{l}} \text{ with } \mathfrak{l} \neq \bar{\mathfrak{l}}, \\ [(l)] & \text{if } (l) \text{ is a prime in } M \text{ outside } N \text{ or } (l)|\mathfrak{c}, \\ \pm\sqrt{[(l)]} & \text{if } (l)|N \text{ is a prime in } M \text{ outside } \mathfrak{c}, \\ [\mathfrak{l}] & \text{if } (l) = \mathfrak{l}^2 \text{ in } M \end{cases}$$

gives a ring homomorphism $\mathbf{h} \to W[[C]]$ inducing $\mathbb{T}_{cm,(p)} \cong W[[C_p]]_{(p)}$; so, $\mathbb{T}_{cm,P}$ for any prime P over (p) is a local complete intersection, and for an irreducible component $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbb{T}_{cm})$, $\mathbb{I}_P \cong W[[\Gamma_M]]_{(p)}$ which is regular. See [H86c].

4.2. **Irreducibility and Gorenstein-ness.** We would like to prove

Theorem 4.3. *If ρ_P is absolutely irreducible and $\rho_P|_{I_p} \cong \left(\begin{smallmatrix} \epsilon_P & * \\ 0 & 1 \end{smallmatrix}\right)$ with $\epsilon_P \neq 1$ for the inertia group $I_p \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at p, then the localization $\mathbb{T}_P$ is a Gorenstein ring.*

To prove this, we apply Mazur's argument proving Lemma 15.1 of [M]: irreducibility $\Rightarrow$ Gorenstein-ness, that is,

$$\mathrm{Hom}_{W[[T]]_P}(\mathbb{T}_P, W[[T]]_P) \cong \mathbb{T}_P$$

as $\mathbb{T}_P$ modules.

We prepare some notation and a proposition. Let $J_1(Np^r)$ be the jacobian of the modular curve $X_1(Np^r)_{/\mathbb{Q}}$. We consider its Tate module $T_pJ_1(Np^r)$ and its limit $\varprojlim_r T_pJ_1(Np^r)$ via Albanese functoriality. The limit is a Galois module. The ordinary part J of $\varprojlim_r T_pJ_1(Np^r)$ (that is the image of $e = \lim_{n\to\infty} U(p)^{n!}$ of the limit) still carries the Galois action. By Diamond operators, $(\mathbb{Z}/N\mathbb{Z})^\times \times \mu_{p-1} \subset (\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times$ acts on J. We can take the maximal quotient L of $J \otimes_{\mathbb{Z}_p} W$ on which $(\mathbb{Z}/N\mathbb{Z})^\times \times \mu_{p-1}$ acts by ψ_2. The Galois module L is naturally an $\mathbf{h}[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module.

Over the valuation ring $A_r = \mathbb{Z}_p[\mu_{p^r}]^{\mathrm{Ker}(\psi_2)}$, we have a well defined multiplicative component of the Barsotti-Tate group of $J_1(Np^r)[p^\infty] \otimes_{\mathbb{Z}_p} W$ (see [AME] Chapter 14). Thus regarding the Poltryagin dual of L as the injective limit of the generic fiber of these Barsotti–Tate groups over A_∞, we have a connected-étale/ramified-unramified exact sequence: $L^{mult}_{/\mathbb{Z}_p} \hookrightarrow L_{/\mathbb{Z}_p} \twoheadrightarrow L^{et}_{/\mathbb{Z}_p}$. A seen in [H86b] Theorem 9.3 (when $\psi_2 \neq 1$) and by Ohta [O] otherwise, we have

Proposition 4.4. *$L^{mult} \cong \mathbf{h}$, and $L^{et} \cong \mathrm{Hom}_{W[[T]]}(\mathbf{h}, W[[T]])$ as $\mathbf{h}$-modules.*

Proof of Theorem 4.3. We follow the proof of [M] Lemma 15.1 and Corollary 15.2. Take a prime $P \in \mathrm{Spec}(\mathbb{T}) \subset \mathrm{Spec}(\mathbf{h})$ as in the theorem and put $V = L_P/PL_P$ as Galois module. Then, by [O] Theorem (where actually the Galois module $V' := V \otimes \det(\rho_P)^{-1}$ is studied), $V^{mult} := L^{mult}/PL^{mult}$ (isomorphic to ${V'}^{I_p}$ just as vector spaces) is the eigen subspace of L on which the inertia group acts by the nontrivial character ϵ_P. By the above lemma, V^{mult} is 1 dimensional over $\kappa(P)$. If V is two dimensional, we have $\dim(L^{et}_P/PL^{et}_P) = 1$, and hence by Nakayama's lemma $L^{et}_P \cong \mathbb{T}_P = \mathbf{h}_P$. Since $L^{et} \cong \mathrm{Hom}_{W[[T]]}(\mathbf{h}, W[[T]])$, this shows

$$\mathbb{T}_P = \mathbf{h}_P \cong \mathrm{Hom}_{W[[T]]_P}(\mathbf{h}_P, W[[T]]_P) \cong \mathrm{Hom}_{W[[T]]_P}(\mathbb{T}_P, W[[T]]_P)$$

as desired.

Let $\Phi_l(X) = \det(X - \rho_{\mathbb{I}}(Frob_l)) \in \mathbb{I}[X]$ for primes l outside Np. Since L is killed by $\Phi_l(Frob_l)$, by the irreducibility of $\rho_{\mathbb{I}}$, V is killed by $\Phi_l(Frob_l)$; so, irreducible subquotients of V are all isomorphic to ρ_P. Thus the semi-simplification V^{ss} is isomorphic to ρ_P^m for $m > 0$. The subspace $V^{mult} := L^{mult}_P/PL^{mult}_P \subset V$ is the unique 1-dimensional subspace on which I_p acts by ϵ_P. Then I_p acts trivially on $L^{et}_P/PL^{et}_P = V/V^{mult}$. Since multiplicity of ϵ_P on V^{ss} is m, we have $m = 1$ and hence $\dim L_P/PL_P = 2$, which finishes the proof. □

4.3. **Congruence modules.** Pick a prime divisor P in $\mathrm{Spec}(\mathbb{T}_{cm})$ over (p). Since $\Psi_{\mathbb{I}} \mod P$ restricted to $I_{\mathfrak{p}}$ has infinite order and is unramified at $\overline{\mathfrak{p}}$, ρ_P is absolutely irreducible (so, $\mathbb{T}_P$ is Gorenstein by Theorem 4.3). By Fact 1, we have $\mathbb{T}^M_{cm,P} = \mathbb{T}_{cm,P}$, and $\mathbb{T}_{cm,P}$ is a local complete intersection (and hence Gorenstein). For the torsion-free part $\Gamma_M := C_p/\Delta$ of C_p, $\mathbb{I} = W[[\Gamma_M]]$; so, $\mathbb{I}$ is a regular ring. We have therefore the projection maps

$$\mathbb{T}_P \twoheadrightarrow \mathbb{T}_{cm,P} \twoheadrightarrow \mathbb{I}_P$$

where all rings involved are Gorenstein rings.

Theorem 4.5. *Suppose $p \nmid \Phi(N)$ and that N is cube free. Let $P \in \mathrm{Spec}(\mathbb{T}_{cm})$ be a prime divisor over $(p) \subset \mathbb{Z}_p[[X]]$. Then we have $\mathbb{T}_P = \mathbb{T}_{cm,P}$.*

We prepare some notation and two lemmas and a proposition for the proof of the theorem. For simplicity, we write the sequence $\mathbb{T}_P \twoheadrightarrow \mathbb{T}_{cm,P} \twoheadrightarrow \mathbb{I}_P$ as $R \xrightarrow{\theta} S \xrightarrow{\phi} A$ and we put $\lambda = \phi \circ \theta : R \to A$. Since $\mathbb{T}$ is reduced, we have the following (unique) decomposition

(1) $\mathrm{Spec}(R) = \mathrm{Spec}(R') \cup \mathrm{Spec}(S)$ with complementary component $\mathrm{Spec}(R')$ of $\mathrm{Spec}(S)$. Put $C_0(\theta, S) := R' \otimes_R S$; so, $\mathrm{Spec}(R') \cap \mathrm{Spec}(S) = \mathrm{Spec}(C_0(\theta, S))$.
(2) $\mathrm{Spec}(S) = \mathrm{Spec}(S') \cup \mathrm{Spec}(A)$ with complementary component $\mathrm{Spec}(R')$ of $\mathrm{Spec}(A)$. Put $C_0(\phi, A) := S' \otimes_S A$; so, $\mathrm{Spec}(S') \cap \mathrm{Spec}(S) = \mathrm{Spec}(C_0(\phi, A))$.
(3) $\mathrm{Spec}(R) = \mathrm{Spec}(R'') \cup \mathrm{Spec}(A)$ with complementary component $\mathrm{Spec}(R'')$. Put $C_0(\lambda, A) := R'' \otimes_R A$; so, $\mathrm{Spec}(R'') \cap \mathrm{Spec}(A) = \mathrm{Spec}(C_0(\lambda, A))$.

By Gorenstein-ness we have verified, we have

$$\mathrm{Hom}_\Lambda(R, \Lambda) \cong R,\ \mathrm{Hom}_\Lambda(S, \Lambda) \cong S \text{ and } \mathrm{Hom}_\Lambda(A, \Lambda) \cong A \text{ as } R\text{-modules.}$$

Under this circumstances, as proved in [H88a] Theorem 6.6, we have

Lemma 4.6. *We have the following exact sequence of R-modules:*

$$0 \to C_0(\phi; A) \to C_0(\lambda; A) \to C_0(\theta; S) \otimes_S A \to 0.$$

Moreover we have $C_0(\lambda; A) = A/c_\lambda A$ for $c_\lambda \in A$, $C_0(\phi; A) = A/c_\phi A$ for $c_\phi \in A$ and $C_0(\theta; S) = S/c_\theta S$ for $c_\theta \in S$ (so, $C_0(\theta; S) \otimes_S A = A/\phi(c_\theta)A$).

We have a morphism $(\mathbb{Z}/(\mathfrak{c}\cap\mathbb{Z}))^\times \to Cl_M(\mathfrak{c})$ sending ideal $0 < n \in \mathbb{Z}$ to its class in $Cl_M(\mathfrak{c})$, and we write $h^-(\mathfrak{c})$ for the order of cokernel $Cl^-_M(\mathfrak{c})$ of this map. Now write $\mathfrak{c}$ for the prime to p conductor of $\Psi_{\mathbb{I}}$.

Lemma 4.7. *We have $c_\phi = h^-(\mathfrak{c} \cap \overline{\mathfrak{c}})$ up to units in $\mathbb{I}_P$.*

We have a natural inclusion $\Gamma = 1 + p\mathbb{Z}_p \hookrightarrow R^\times_{\mathfrak{p}} \to C_p$, which gives rise to the Λ-algebra structure $\Lambda \hookrightarrow W[[C_p]]$. Since S is the p-localization of the group algebra $W[[C_p]]$, it is well known that c_ϕ is the index of Γ in C_p (up to p-units; see for example, [H86c] Lemma 1.9 and Lemma 1.11).

Let $\Psi^-_{\mathbb{I}}(\tau) = \Psi_{\mathbb{I}}(c\tau c^{-1}\tau^{-1})$ for complex conjugation c be the anticyclotomic projection of $\Psi_{\mathbb{I}}$ and $L_p(\Psi^-_{\mathbb{I}})$ be the primitive anticyclotomic Katz p-adic L-function as in [H06] and [H07b]. We regard $L_p(\Psi^-_{\mathbb{I}}) \in \mathbb{I}$.

Proposition 4.8. *If $p \nmid \Phi(N)$, we have $c_\lambda = h^-(\mathfrak{c} \cap \overline{\mathfrak{c}})L_p(\Psi^-_{\mathbb{I}})$ up to units in $\mathbb{I}_P$.*

Proof. Write $\mathrm{Spec}(\mathbb{T}) = \mathrm{Spec}(\mathbb{I}) \cup \mathrm{Spec}(\mathbb{X})$ for the complementary component $\mathbb{X}$. For general $P \in \mathrm{Spec}(\mathbb{I})$, as long as $\mathbb{T}_P$ is Gorenstein, we have $\mathrm{Spec}(\mathbb{I}_P) \cap \mathrm{Spec}(\mathbb{X}_P) = \mathrm{Spec}(\mathbb{I}_P/(L_p))$. The L-function $L(s, Ad(f_P))$ may not be a primitive L-function if $\mathbb{I}$ is an old component. Thus writing $L_p(s, Ad(\rho_P))$ for the primitive L-function,

$$L(s, Ad(f_P)) = E(s)L(s, Ad(f_P)) = E(1)h(\mathfrak{c} \cap \overline{\mathfrak{c}})L(1, \Psi^-_P)$$

for a product $E(s)$ of Euler-like factors over inert prime factors of $N/\mathfrak{c}\overline{\mathfrak{c}}$. As

$$\Phi^-_P(Frob_{(l)}) = \Phi_P(Frob_{(l)})/\Phi_P(c \cdot Frob_{(l)}c^{-1}) = 1$$

for inert l, $E(1)$ is a constant independent of P. We compute $E(1) = 2(1 + \frac{1}{l})$ which is a factor of $\Phi(N)$ in $\mathbb{I}$. Thus if $p \nmid \Phi(N)$, we get the desired result. □

Proof of Theorem 4.5. Note that the assertion of the theorem is equivalent to the vanishing $C_0(\theta; S) = 0$, which is in turn, by Nakayama's lemma, equivalent to $C_0(\theta; S) \otimes_R A = 0$. We study $C_0(\theta; S) \otimes_R A$. By the above two lemmas and the proposition, we find that $\phi(c_\theta) = c_\lambda/c_\phi$; so, $\phi(c_\theta) = L_p(\Psi^-_{\mathbb{I}})$ up to units in A. Let p^μ ($0 \le \mu \in \mathbb{Q}$) be the exact power dividing $L_p(\Psi^-_{\mathbb{I}})$ in A. Then $\phi(c_\theta) = 1$ (up to units in A) $\Leftrightarrow C_0(\theta; S) \otimes_R A = 0 \Leftrightarrow \mu = 0$. The vanishing of μ is proven in [H10] and [Fi] under $p \nmid \Phi(N)$ and the theorem follows. □

4.4. **Proof of the theorem.** We first prove

Proposition 4.9. *Suppose $p \nmid \Phi(N)$ and that N is cube-free. If $\mathbb{I}$ is a non CM component of the Hecke algebra $\mathbf{h}$, for each prime divisor $P \in \mathrm{Spec}(\mathbb{I})$ over $(p) = p\mathbb{Z}_p[[T]]$, G°_P is isomorphic to $SL(2)_{/\overline{\kappa}(P)}$.*

Proof. Replace $\rho_{\mathbb{I}}$ by $\rho' := \rho_{\mathbb{I}} \otimes \sqrt{\langle\det(\rho_{\mathbb{I}})\rangle}^{-1}$. Then $\det(\rho')$ has finite image; so, the Zariski closure G_P of $\mathrm{Im}(\rho')$, has connected component G°_P in $SL(2)$. The semi-simplification of $\rho_{\mathbb{I}}|_{I_p}$ has values in a split torus in GL_2 containing a matrix with two distinct eigenvalues (which are 1 and $(1+T)^s$ for some $s \neq 0$). Thus the semisimplification of $\rho'|_{I_p}$ has values in a split torus of SL_2. We need to prove $G_P^\circ = SL(2)$. Since $\rho'(I_p)$ is an infinite group by (Gal), $\dim G_P > 0$. There are only three possibilities: either G_P° is isomorphic to a split torus $\mathcal{T}$, or is contained in the Borel subgroup $\mathcal{B}$, or $G_P^\circ = SL(2)$. If $G_P^\circ \subset \mathcal{T}$, we conclude that $\rho'_P = \mathrm{Ind}_M^{\mathbb{Q}} \phi$ for an imaginary quadratic field M and a Galois character $\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to (\mathbb{I}/P)^\times$. We can lift by class field theory ϕ to a character $\Psi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to W[[C_p]]^\times$ with $\mathrm{Im}(\Psi) \supset C_p$ without changing its ramification outside p. Then $\mathrm{Spec}(\mathbb{I})$ and $\mathrm{Spec}(\mathbb{I}_{cm}^M)$ intersect at P, which is impossible by Theorem 4.5. Thus we now assume that $G_P^\circ \subset \mathcal{B}$ and G_P° has nontrivial nilpotent radical. Since conjugation by $\rho'(\sigma)$ has to preserve G_P° and its nilpotent radical, ρ' has to be reducible; so, P is an Eisenstein prime of $\mathbf{h}$. By [O1] Theorem 2.4.10, under the assumption $p \nmid \varphi(N)$ for the Euler function $\varphi(N)$, any Eisenstein ideal is killed by a Kubota-Leopoldt p-adic L-function, which has trivial μ-invariant by a theorem of Ferrero-Washington [FeW]. Thus ρ' cannot be upper triangular. The only remaining possibility is $G_P^\circ = SL(2)$. □

We need the following result of Pink (Proposition 0.6 and Theorem 0.7 in [P]).

Theorem 4.10 (Pink)**.** *Write $Ad : PSL(2) \to \mathrm{End}(\mathfrak{sl}(2))$ for the adjoint representation. Let $\mathcal{G}$ be a compact subgroup Zariski dense in $PSL_2(\mathbb{F}((x)))$ for a characteristic p finite field $\mathbb{F}$, and define $E \subset \mathbb{F}((x))$ be a closed subfield generated by $\mathrm{Tr}(Ad(g))$ for all $g \in \mathcal{G}$. If the Zariski closure of $\mathcal{G}$ is $PSL(2)$, there exists an algebraic group $H_{/E}$ such that $H \times_E \mathbb{F}((x)) = PSL(2)$ and that $\mathcal{G}$ contains an open subgroup of $H(E)$.*

Proof of Theorem 4.1. Let $\rho'_P = \rho' \mod P$ for ρ' in the proof of the above proposition. We now apply Pink's results to $\mathcal{G}$ given by $\mathrm{Im}(\rho'_P) \cap SL(2)$ modulo center. By the above proposition, the Zariski closure of $\mathrm{Im}(\rho'_P) \cap SL(2)$ is the full group $SL(2)$ (so, the Zariski closure of $\mathcal{G}$ is $PSL(2)$). Since $\kappa(P)$ is a local function field of characteristic p, the integral closure of $\mathbb{F}_p[[T]]$ in $\kappa(P)$ is isomorphic to $\mathbb{F}[[x]]$ for a variable $x \in \kappa(P)$ with a finite field extension $\mathbb{F}/\mathbb{F}_p$; so, $\kappa(P) = \mathbb{F}((x))$. Thus we may assume that the image $\mathcal{G}$ is contained in $PSL_2(\mathbb{F}[[x]])$. Let $Ad(\rho'_P) = Ad(\rho_P) = Ad \circ \rho_P$ be the adjoint representation of ρ_P on $\mathfrak{sl}(2)$. By (Gal), we have $Tr(Ad(\rho_P)([\gamma^s, \mathbb{Q}_p])) = 1 + (1+T)^s + (1+T)^{-s}$. Thus $\mathbb{F}_p((T))$ is the closed subfield in $\mathbb{F}((x))$ generated by $\mathrm{Tr}(Ad(\rho_P)|_{I_p})$ over $\mathbb{F}_p$ in $\mathbb{I}/P$, and we get $E \supset \mathbb{F}_p((T))$. Again by (Gal), the semi-simple part of $\rho'_P([\gamma^s, \mathbb{Q}_p])$ is conjugate to $\begin{pmatrix} (1+T)^{-s/2} & 0 \\ 0 & (1+T)^{s/2} \end{pmatrix}$. Therefore the Zariski closure of the semi-simplification of $\rho'_P|_{I_p}$ is a split torus $\mathcal{T}$ of $SL(2)_{/\mathbb{F}((T))}$. Thus its Zariski closure $\overline{\mathcal{T}}$ in $H_{/E}$ is still split over E, and the group H is split; so, $H_{/E} \cong PSL(2)_{/E}$. This shows the Galois image contains an open subgroup of $SL_2(E)$ for $E \supset \mathbb{F}_p((T))$.

Remark 4.1. If $\Psi_{\mathbb{I}}^-$ modulo $\mathfrak{m}_{\mathbb{I}}$ is unramified at an inert prime l but $\Psi_{\mathbb{I}}^-$ ramifies at l (this happens when $p|\Phi(N)$), the μ-invariant of $L(\Psi_{\mathbb{I}}^-)$ is positive as explained at the end of [H10]. Therefore, we have a mod p congruence of the CM component of $\Psi_{\mathbb{I}}$ and a non CM component. Thus for this non CM component, its Galois representation does not have the open image property modulo p.

5. Lecture 5: Vanishing of the μ-invariant of p-adic Katz L-functions

The last two lectures are an introductory discussion of problems concerning vanishing of the Iwasawa μ-invariant of p-adic L-functions. This type of results for Kubota-Leopoldt p-adic L has found applications in divisibility problems of class numbers (see [ICF] Chapter 7), in proofs of the main conjectures in Iwasawa's theory and in proving open image property of mod p Λ-adic modular Galois representations. Recently, new methods of proving the vanishing emerged in the work of Vatsal, Finis and myself. See [V] for an overview. We describe a geometric method, which was started by Sinnott in [S] and [S1] and has been generalized in [H04a], [H07b] and [H10] via the theory of Shimura varieties. We rely on a general philosophical principle (proposed by Chai, Oort and others): "A Hecke invariant subvariety of a Shimura variety is a Shimura subvariety". For any power series $\Phi(x_1, \dots, x_d) \in W[[x_1, \dots, x_d]]$, define $\mu(\Phi) \in \mathbb{Z}$ by the exact power $p^{\mu(\Phi)} \parallel \Phi(X)$ in $W[[x_1, \dots, x_d]]$. The W-valued measure space on $\mathbb{Z}_p$ can be identified with one variable power series ring $W[[\mathcal{T}]]$ by $\varphi \mapsto \Phi(\mathcal{T}) = \int_{\mathbb{Z}_p} (1+\mathcal{T})^s d\varphi(s) \in W[[\mathcal{T}]]$.

Let $p > 2$ be a prime. Let M be a CM field of degree $2d$ in which p is *unramified.* We assume to be able to split primes of M over p into a disjoint union $\Sigma_p \sqcup \Sigma_p^c$ for complex conjugation c on M. Then Katz associated to Σ_p and each finite order branch character ψ of p-power conductor a p-adic L-function $L_p = L_p(\psi)$. Recall fixed embeddings $\mathbb{C} \overset{i_\infty}{\hookleftarrow} \overline{\mathbb{Q}} \overset{i_p}{\hookrightarrow} \overline{\mathbb{Q}}_p$. We have a CM type associated $\Sigma = \{\sigma : M \hookrightarrow \mathbb{C}\}$ to Σ_p (so, $\mathrm{Hom}_{\mathrm{field}}(M, \mathbb{C}) = \Sigma \sqcup \Sigma^c$). We may view the p-adic L-function as a power series $L_p(x_\sigma, y)_{\sigma \in \Sigma} \in W[[x_\sigma, y]]$ of $d+1$ variables for the p-adic big unramified complete DVR $W \subset \mathbb{C}_p$ with algebraic closed residue field $\mathbb{F} = \overline{\mathbb{F}}_p$. For each fractional ideal $\mathfrak{a}$ of M prime to p, its power $\mathfrak{a}^h$ becomes principal generated by $\alpha \in M^\times$. Define $\langle \mathfrak{a}^\sigma \rangle \in \overline{\mathbb{Q}}_p^\times$ by $\exp_p(\frac{1}{h} \log_p(\alpha^\sigma))$ for the p-adic logarithm $\log_p$. Then

$$\widehat{\lambda}_{\kappa,k} : \mathfrak{a} \mapsto \langle \mathfrak{a}^{-k\Sigma - \kappa(1-c)} \rangle := \prod_{\sigma \in \Sigma} \langle \mathfrak{a}^{-k\sigma - \kappa_\sigma \sigma(1-c)} \rangle$$

is the p-adic avatar of an arithmetic Hecke character $\lambda_{\kappa,k}$ of conductor at most p with infinity type $\sum_{\sigma \in \Sigma} k\sigma + \kappa_\sigma(1-c)\sigma$. For $\kappa \geq 0 (\Leftrightarrow \kappa_\sigma \geq 0\ \forall \sigma \in \Sigma)$ and $k > 0$, we have

$$\frac{L_p(\widehat{\lambda}_{\kappa,k})}{\Omega_p^{k\Sigma+2\kappa}} := \frac{L_p(\gamma_\sigma^{\kappa_\sigma} - 1, \gamma^k - 1)}{\Omega_p^{k\Sigma+2\kappa}} = *E(\psi\lambda_{\kappa,k}) \frac{\pi^\kappa L(0, \psi\lambda_{\kappa,k})}{\Omega_\infty^{k\Sigma+2\kappa}} \quad \text{for } \gamma_\sigma = \gamma = 1+p.$$

Here $\Omega_? = (\Omega_{?,\sigma})_{\sigma \in \Sigma}$ is the p-adic/complex Néron period of CM abelian variety of CM type Σ (with ordinary good reduction at p), $*$ is a simple constant with $|*|_p = 1$ including the Γ/ϵ-factor, and $E(\lambda) = \prod_{\mathfrak{p} \in \Sigma_p} (1 - \lambda(\mathfrak{p}^c))(1 - N(\mathfrak{p})^{-1}\lambda(\mathfrak{p})^{-1})$. Limiting ourselves to the case of imaginary quadratic M, we describe a sketch of the proof of

Theorem 5.1. $p \nmid L_p(x_\sigma, y)$ in $W[[x_\sigma, y]]$ *(so* $\mu(L_p(\psi)) = 0$*).*

For a weight $k > 0$, we prove $\sup_{\zeta \in \mu_{p^\infty}} \mu(L_p(\psi)(x_\sigma, \zeta\gamma^k - 1)) = 0$, which implies $\mu(L_p(\psi)(x_\sigma, y)) = 0$. Since the proof is the same for any choice of F, for simplicity, we assume

(1) $F = \mathbb{Q}$; so, M is an imaginary quadratic field with integer ring O,
(2) M has class number prime to p with $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ and $\Sigma_p = \{\mathfrak{p}\}$,
(3) $p \geq 5$, $\psi = 1$, any ring to have $\frac{1}{6}$ and $|O^\times| = 2$.

5.1. **Eisenstein series.** For any lattice $L = \mathbb{Z}w_1 + \mathbb{Z}w_2 \subset \mathbb{C}$, we can think about

$$\frac{(2\pi i)^k}{(k-1)!}G_k(L) = \frac{1}{2}\sum_{\ell \in L-\{0\}} \frac{1}{\ell^k} = \frac{1}{2}\zeta(1-k) + \sum_{n=1}^{\infty}(\sum_{0<d|n} d^{k-1})q^n \quad \text{(Eisenstein series)},$$

which is a function of lattices satisfying $G_k(\alpha L) = \alpha^{-k}G_k(L)$. The quotient $\mathbb{C}/L$ gives rise to an elliptic curve $X(L) \subset \mathbf{P}^2$ by Weierstrass theory. Since $\Omega_{X(L)/\mathbb{C}}$ is generated by du for the variable u of $\mathbb{C}$ and we can recover out of $(X(L), du)$ the lattice L as $\{\int_\gamma du | \gamma \in \pi_1(E)\}$, we regard G_k as a function of the pairs (E, ω) of an elliptic curve E with a generator ω of $\Omega_{E/\mathbb{C}}$ satisfying $G_k(E, \alpha\omega) = \alpha^{-k}G_k(E, \omega)$. For a given base ring $B_{/\mathbb{Z}[\frac{1}{6}]}$, a modular form f defined over B of weight k and of level 1 can be interpreted as a functorial rule assigning a number in A to the isomorphism class of a pair $(E, \omega)_{/A}$ of an elliptic curve E over a B-algebra A and a differential with $H^0(E, \Omega_{E/A}) = A\omega$ such that

(1) $f(E, \omega) \times_{A,\rho} A') = \rho(f(E, \omega))$ for any B-algebra homomorphism $\rho : A \to A'$,
(2) $f(E, a\omega) = a^{-k}f(E, \omega)$ for $a \in A^\times$,
(3) f is finite at cusps (the value at the Tate curve at each cusp lands in $B[[q]]$).

If a modular form f defined over $\mathbb{C}$ has q-expansion in $B[[q]]$ at the infinity cusp, f is actually defined over B (assuming $B \subset \mathbb{C}$). Indeed, then f is an isobaric polynomial $\Phi(g_2, g_3)$ in $B[g_2, g_3]$, and if (E, ω) is defined over A by $y^2 = 4x^3 - g_2(E, \omega)x - g_3(E, \omega)$ with $\omega = \frac{dx}{y}$, $f(E, \omega) = \Phi(g_2(E, \omega), g_3(E, \omega)) \in A$. We take $B := \mathcal{W} = W \cap \overline{\mathbb{Q}}$.

Removing p-coefficients, $\mathcal{G}_k(z) = \sum_{n>0, p\nmid n}(\sum_{0<d|n} d^{-1}\langle d\rangle^k)q^n$ gives rise to a p-adic analytic family with $\psi_1 = \omega^{-1}$. It is a part of the family $\{\mathcal{G}_P\}_{P\in\mathrm{Spec}(\Lambda)}$ such that $a(n, \mathcal{G}_P) = \sum_{0<d|n} \epsilon_P(d)d^{-1}\langle d\rangle^k$ if $P = (1 + T - \epsilon_P(\gamma)\gamma^{k-1})$. Often we write this $\mathcal{G}_P$ as $\mathcal{G}_{k,\zeta}$ for $\zeta = \varepsilon_P(\gamma) \in \mu_{p^\infty}(\overline{\mathbb{Q}}_p)$ and also $\varepsilon_\zeta = \varepsilon_P$. The form $\mathcal{G}_{k,\zeta}$ is also an Eisenstein series with possibly nontrivial Nebentypus. Since the mod $\mathfrak{p}^\infty$ class group C of M has splitting $C = Cl \times O_\mathfrak{p}^\times/\{\pm 1\}$ by our assumptions, we may regard ε_ζ as a character $\widetilde{\varepsilon}_\zeta$ of C projecting down C to $O_\mathfrak{p}^\times = \mathbb{Z}_p^\times$ (so, we have $(1 + T) = (1 + y)\gamma^{-1}$).

The CM curve $X(\mathfrak{a})$ is defined over $\mathcal{W}$ and has a differential $\omega(\mathfrak{a})$ with $\omega(\mathfrak{a}) = \pi^*\omega(O)$ for a fixed $\omega(O)$, where $\pi : X(\mathfrak{a}) \to X(O)$ is an étale isogeny of degree $[R : \mathfrak{a}]$. Fix a generator $\alpha \in \pi_1(X(O))$, and put $\Omega_\infty = \int_\alpha \omega(O)$. We find $\frac{\mathcal{G}_{k,\zeta}(\mathfrak{a})}{\Omega_\infty^k} = \mathcal{G}_{k,\zeta}(\Omega_\infty\mathfrak{a}) = \mathcal{G}_{k,\zeta}(X(\mathfrak{a}), \omega(\mathfrak{a})) \in \mathcal{W}[\zeta]$ and

$$\frac{\mathcal{G}_k(\mathfrak{a})}{\lambda_{0,k}(\mathfrak{a})} = \frac{1}{2\lambda_{0,k}(\mathfrak{a})}\sum_{\alpha\in\mathfrak{a},(a)+(p)=O}\langle\alpha\rangle^{-k} \doteqdot \sum_{\alpha\in\mathfrak{a}}\lambda_{0,k}(\alpha\mathfrak{a}^{-1})N(\alpha\mathfrak{a}^{-1})^{-s}|_{s=0} \doteqdot L_{\mathfrak{a}^{-1}}(0, \lambda_{0,k})$$

$$\frac{\mathcal{G}_{k,\zeta}(\mathfrak{a})}{\widetilde{\varepsilon}_\zeta\lambda_{0,k}(\mathfrak{a})} \doteqdot L_{\mathfrak{a}^{-1}}(0, \widetilde{\varepsilon}_\zeta\lambda_{0,k}),$$

where "$\doteqdot$" indicates that we need to multiply Euler-like factor $E(?)$.

Applying the invariant differential operator (of Maass–Shimura)

$$\delta_k = \frac{1}{2\pi i}\left(\frac{k}{2iy} + \frac{\partial}{\partial z}\right) \quad \text{and} \quad \delta_k^\kappa = \overbrace{\delta_{k+2\kappa-2}\cdots\delta_k}^{\kappa},$$

we have, by Shimura,

$$\frac{\delta_k^\kappa\mathcal{G}_{k,\zeta}(\mathfrak{a})}{\widetilde{\varepsilon}_\zeta\lambda_{\kappa,k}(\mathfrak{a})} \doteqdot L_{\mathfrak{a}^{-1}}(0, \widetilde{\varepsilon}_\zeta\lambda_{\kappa,k}) \quad (\textit{only dependent on the class of } \mathfrak{a}).$$

This can be seen as follows: For $z_0 = z_0(\mathfrak{a})$ with $\mathfrak{a} = \mathbb{Z}z_0 + \mathbb{Z}$ (and $\mathrm{Im}(z_0) > 0$), define $\rho = \rho_{\mathfrak{a}} : M \to M_2(\mathbb{Q})$ by $\rho(\alpha)\binom{z_0}{1} = \binom{z_0}{1}\alpha$. Then $\rho(\alpha)(z_0) = z_0$. We take a local parameter t around z_0 so that $\rho(\alpha)(t) = \alpha^{1-c}t$ and $t = 0 \leftrightarrow z = z_0$ (for example, if $z_0 = i = \sqrt{-1}$, $t = \frac{z-i}{z+i}$). Then we find, regarding $\langle \mathfrak{a}^{1-c}\rangle \in \mathbb{C}^\times$

$$\frac{\delta_k^\kappa(\mathcal{G}_k(\langle \mathfrak{a}^{1-c}\rangle t))|_{t=0}}{\lambda_{0,k}(\mathfrak{a})} = \frac{\langle \mathfrak{a}^{1-c}\rangle^\kappa \delta_k^\kappa(\mathcal{G}_k(z_0(\mathfrak{a})))}{\lambda_{0,k}(\mathfrak{a})} = \frac{\delta_k^\kappa(\mathcal{G}_k(z_0(\mathfrak{a})))}{\lambda_{\kappa,k}(\mathfrak{a})} \doteqdot L_{\mathfrak{a}^{-1}}(0, \lambda_{\kappa,k}).$$

There is a canonical p-adic Serre–Tate parameter τ around z_0 (as a point of a modular curve). Heuristically, $\log_p(\tau)$ behaves like t: $t = 0 \Leftrightarrow \tau = 1$ and $\tau \circ \rho(\alpha) = \tau^{\alpha^{1-c}}$. For $\theta := \tau \frac{d}{d\tau}$, by Katz, with a specific p-adic period $\Omega_p \in W^\times$ of $X(O)$ (we recall later),

$$\frac{L_p(\widehat{\lambda}_{\kappa,k})}{\Omega_p^{k+2\kappa}} = \sum_{\mathfrak{a}} \frac{\theta^\kappa(\mathcal{G}_k(\tau^{\langle \mathfrak{a}^{1-c}\rangle}))|_{\tau=1}}{\lambda_{0,k}(\mathfrak{a})} = \sum_{\mathfrak{a}} \frac{\delta_k^\kappa(\mathcal{G}_k(\Omega_\infty \mathfrak{a}))}{\lambda_{\kappa,k}(\mathfrak{a})} \doteqdot \frac{\pi^\kappa L(0, \lambda_{\kappa,k})}{\Omega_\infty^{k+2\kappa}}$$

for $\mathfrak{a}$ running through ideal classes. Thus, we can compute the Taylor expansion of $E = \sum_{\mathfrak{a}} \frac{\mathcal{G}_k(\tau^{\langle \mathfrak{a}^{1-c}\rangle})}{\lambda_{0,k}(\mathfrak{a})}$ with respect to $x' = \log_p(\tau)$ by computing the derivative with respect to θ. Since E is defined over W, out of this identification of the Taylor expansion, we conclude that $L_p(x, \gamma^k - 1)$ is almost the expansion with respect to $\mathcal{T} = \tau - 1$ of E. Strictly speaking, first, the $\mathcal{T}$-expansion is the expansion of the measure given by E as a measure on $\mathbb{Z}_p$ not on $1 + p\mathbb{Z}_p$. Second, we want to know the non-vanishing of the $\mathcal{T}$-expansion modulo p of the restriction of the measure on $Cl(p^\infty)$ to $1 + pO_p \cong \Gamma^2$. Thus we need to replace $\mathcal{G} := \{\mathcal{G}_{k,\zeta}\}$ by a family $\{\mathcal{G}'_{k,\zeta,\mathfrak{b}}\}$ of Eisenstein series of level p^2. Since $L_{\mathfrak{a}^{-1}}(s, \lambda)$ (resp. $\mathcal{G}$) can be further decomposed into a sum of partial L-functions for a class modulo p (resp. a sum of Eisenstein series of level p^2), we have $L_{\mathfrak{a}^{-1}}(s, \lambda) = \sum_{\mathfrak{b} \equiv \mathfrak{a} \mod p, [\mathfrak{b}] \in Cl_M(p)} L_{\mathfrak{b}^{-1}}(s, \lambda)$, and

$$E_\zeta = \sum_{\mathfrak{b} \in Cl_M(p)} \frac{\mathcal{G}'_{k,\zeta,\mathfrak{b}}(\tau^{\langle \mathfrak{b}^{1-c}\rangle})}{\widetilde{\varepsilon}_\zeta \lambda_{0,k}(\mathfrak{b})}$$

gives rise to the exact power series $L_p(\mathcal{T}, \gamma^k\zeta - 1)$ as a measure on $\mathbb{Z}_p$.

Note that $\mathcal{T}$ is the local parameter around $z_0(O)$. Suppose the following fact (which will be proven at the end of this lecture):

Theorem 5.2. *For any non-zero non-constant mod p-modular form $f_{\mathfrak{b}}$ of weight k indexed by ideal classes, $\{f_{\mathfrak{b}}(\tau^{\langle \mathfrak{b}^{1-c}\rangle})\}_{[\mathfrak{b}] \in Cl_M(p)/\sim}$ are linearly independent over $\mathbb{F}$ in $\mathbb{F}[[\mathcal{T}]]$, where $\{[\mathfrak{b}]\}$ is a representative set of ray classes modulo p under the equivalence: $[\mathfrak{b}] \sim [\mathfrak{c}] \Leftrightarrow \langle \mathfrak{b}^{1-c}\rangle = \alpha(\mathfrak{c})^{1-c}\langle \mathfrak{c}^{1-c}\rangle$ for $\alpha(\mathfrak{c}) \in M^\times$.*

Indeed, $\{\tau^{\langle \mathfrak{b}^{1-c}\rangle}\}_{\mathfrak{b}}$ is algebraically independent in $\mathbb{F}[[\mathcal{T}]]$ over $\mathbb{F}$, we can compute the $\mu(L_p(x, \zeta\gamma^k - 1)) = \mu(L_p(\mathcal{T}, \zeta\gamma^k - 1))$ by q-expansion of $f_{\zeta,\mathfrak{b}} = \sum_{\mathfrak{c} \sim \mathfrak{b}} \mathcal{G}'_{k,\zeta,\mathfrak{b}}(\tau^{\alpha(\mathfrak{c})^{c-1}})$: $\mu(L_p(x, \gamma^k - 1)) = \min(\mathrm{ord}_p(f_{\zeta,\mathfrak{b}}))_{\mathfrak{b}}$, where $\mathrm{ord}_p(f) = \min_n(\mathrm{ord}_p(a(n, f)))$. This goes as follows. Note that $p^{\mu(\mathfrak{b})} \parallel f_{\zeta,\mathfrak{b}}(\mathcal{T}) \in W[[\mathcal{T}]] \Leftrightarrow p^{\mu(\mathfrak{b})} \parallel f_{\zeta,\mathfrak{b}}(q) \in W[[q]]$. Thus dividing E_ζ by p^μ for $\mu = \min_{\mathfrak{b}} \mu(\mathfrak{b})$, and applying Theorem 5.2 to $p^{-\mu} f_{\zeta,\mathfrak{b}}$, we find $\mu(L_p(x, \zeta\gamma^k - 1)) = \mu(L_p(\mathcal{T}, \zeta\gamma^k - 1)) = \mu$, where $L_p(\mathcal{T}, \zeta\gamma^k - 1)$ is the $\mathcal{T}$-expansion of E_ζ (or equivalently the $\mathcal{T}$-expansion of the measure corresponding to $L_p(x, y)$). For $\zeta \in \mu_{p^\infty}(\overline{\mathbb{Q}}_p)$, we prove $\sup_{\zeta,k} \mathrm{ord}_p(f_{\zeta,\mathfrak{b}}) = 0$, and $p \nmid L_p(x, y)$ follows as $\mu(L_p(x, y)) \le \mu(L_p(x, \zeta\gamma^k - 1))$. If $\mathfrak{b} = \rho^{-1}\mathfrak{a}$ for $\rho \in (\mathfrak{a}/p\mathfrak{a})^\times \cong (O/pO)^\times$, $\mathcal{G}'_{k,\zeta,\mathfrak{b}}$ is "something like" the sum over $\alpha \in \mathfrak{a}$ with $\alpha \equiv \rho \mod p$. Thus for a suitable prime l, the q-expansion coefficient $a(l, f_{\zeta,\mathfrak{b}})$ is $1+\varphi_{k,\zeta}(l)l^{k-1}$ for a suitable character $\varphi_{k,\zeta}(l) \doteqdot \zeta^{\log_p(l)/\log_p(\gamma)}$ up to p-adic units. Thus $\min(\mathrm{ord}_p(f_{\zeta,\mathfrak{b}}))_{\mathfrak{b}} \le \min_\zeta(\mathrm{ord}_p(a(l, f_{\zeta,\mathfrak{b}}))) = 0$.

5.2. **Modular Curves as Shimura variety.** To prove Theorem 5.2, we study subvariety of self product of modular curves stable under the diagonal "toric" action by $\rho(\alpha)$. Write $G = GL(2)_{/\mathbb{Z}}$.

We study classification problem of elliptic curves $E_{/A}$ over a ring $A_{/B}$ for $B = \mathbb{Z}[\frac{1}{N}, \mu_N]$ (with specific primitive root $\zeta \in \mu_N$), looking into the following moduli functor of level $\Gamma(N)$ and writing "$[\cdot]$" for "$\{\cdot\}/\cong$",

$$\mathcal{E}_{\Gamma(N),\zeta}(A) = \left[(E, \phi_N : (\mathbb{Z}/N\mathbb{Z})^2 \cong E[N])_{/A} \middle| \langle\phi_N(1,0), \phi_N(0,1)\rangle = \zeta\right],$$

which is represented by geometrically irreducible curve $Y_\zeta(N)$. Here $\langle\cdot,\cdot\rangle$ is the Weil pairing. We know classically $\mathcal{E}_{\Gamma(N),\zeta}(\mathbb{C}) \cong \Gamma(N)\backslash\mathfrak{H} = Y_\zeta(N)(\mathbb{C})$. If we remove the contribution upon ζ and consider the functor $\mathcal{E}_{\Gamma(N)}(A) = \left[(E, \phi_N)_{/A}\right]$ defined on the category of $\mathbb{Z}[\frac{1}{N}]$-algebras, we have $\mathcal{E}_{\Gamma(N)} = \bigsqcup_\zeta \mathcal{E}_{\Gamma(N),\zeta}$, and this functor is represented by a geometrically non-connected curve $Y(N) = \bigsqcup_\zeta Y_\zeta(N)$ defined over $\mathbb{Z}[\frac{1}{N}]$ if $N \ge 3$.

We can let $\alpha \in G(\mathbb{Z}/N\mathbb{Z})$ act on $Y(N)$ by $(E, \phi) \mapsto (E, \phi\circ\alpha)$. Thus the group $G(\widehat{\mathbb{Z}}) = \varprojlim_N G(\mathbb{Z}/N\mathbb{Z})$ acts on the limit $Y = \varprojlim_N Y(N)$ (which is a pro-scheme defined over $\mathbb{Q}$), and $SL_2(\widehat{\mathbb{Z}})$ preserves the connected component $Y_{\zeta_\infty} = \varprojlim_N Y_{\zeta_N}(N)$.

A remarkable fact Shimura found is that this action of $G(\widehat{\mathbb{Z}})$ can be extended to the finite adele group $G(\mathbb{A}^{(\infty)}) = G(\mathbb{A})/G(\mathbb{R})$ (see [IAT] Chapter 6). An interpretation by Deligne of this fact is equally remarkable (see [PAF] 4.2.1): To explain Deligne's idea, we consider the Tate module $T(E) = \varprojlim_N E[N]$ for an elliptic curve $E_{/A}$ for a $\mathbb{Q}$-algebra A. Then $T(E) \cong \widehat{\mathbb{Z}}^2$ and $V(E) = T(E)\otimes_{\mathbb{Z}}\mathbb{Q} \cong (\mathbb{A}^{(\infty)})^2$. Deligne realized that Y represents the following functor defined over $\mathbb{Q}$-algebras:

$$\mathcal{E}^{(\infty)}(A) = \{(E, \eta : (\mathbb{A}^{(\infty)})^2 \cong V(E))_{/A}\}/\text{isogenies}.$$

Here $\mathbb{A}^{(\infty)}$ is the finite adele ring. Then $g \in G(\mathbb{A})$ sends a point $(E,\eta)_{/A} \in \mathcal{E}^{(\infty)}(A)$ to $(E, \eta\circ g^{(\infty)})_{/A}$ for the projection $g^{(\infty)}$ of g to $\mathbb{A}^{(\infty)}$.

Take the quotient $Y^{(p)} = \varprojlim_{p\nmid N} Y(N) = Y/G(\mathbb{Z}_p)$. Put $V^{(p)}(E) = T(E)\otimes_{\widehat{\mathbb{Z}}}\mathbb{A}^{(p\infty)}$, and consider the prime-to–p level structure $\eta^{(p)} : (\mathbb{A}^{(p\infty)})^2 \cong V^{(p)}(E)$. Then $Y^{(p)}$ over $\mathbb{Z}_{(p)}$ represents the following functor defined over $\mathbb{Z}_{(p)}$-algebras:

$$\mathcal{E}^{(p)}(A) = \{(E, \eta^{(p)} : (\mathbb{A}^{(p\infty)})^2 \cong V^{(p)}(E))_{/A}\}/\text{prime-to–}p\text{ isogenies},$$

where an isogeny ϕ is prime to p if $\deg(\phi)$ is prime to p. On $Y^{(p)}$ and its p-fiber $Y^{(p)}_{/\mathbb{F}}$ over $\mathrm{Spec}(\mathbb{F})$, again $g \in G(\mathbb{A})$ acts by $\eta \mapsto \eta\circ g^{(p\infty)}$.

If we have a prime-to–p **non-central** endomorphism $\alpha : E \to E$, then E has complex multiplication by $M = \mathbb{Q}[\alpha]$, and we can write $\alpha\circ\eta^{(p)} = \eta^{(p)}\circ\rho^{(p)}(\alpha)$ for $\rho^{(p)}(\alpha) \in G(\mathbb{A}^{(p\infty)})$. Thus if $z_0 = (E,\eta) \in Y^{(p)}(A)$ ($A = \mathcal{W}$ and $\mathbb{F}$), we find that $\rho^{(p)}(\alpha)(z_0) = z_0$, and

$$O^\times_{(p)}/\mathbb{Z}^\times_{(p)} \xrightarrow[\rho]{\sim} \{g \in \mathrm{Aut}(Y^{(p)}) | g(z_0) = z_0\}.$$

Pick the elliptic curve $X := X(O)_{/\mathcal{W}}$ with CM by the integer ring O of M. Since $\Sigma_p^c = \{\overline{\mathfrak{p}}\}$, we have $\mathfrak{p} = O\cap\mathfrak{m}_{\mathcal{W}}$ and $\mathcal{W}/\mathfrak{m}_{\mathcal{W}} = \overline{\mathbb{F}}_p$, and $X[\overline{\mathfrak{p}}^\infty]$ is étale constant and $X[\mathfrak{p}^\infty] \cong \mu_{p^\infty}$ over $\mathcal{W}$. We fix a level p-structure $\eta_p^\circ : \mu_{p^\infty} \cong X[\mathfrak{p}^\infty]$ and η_p^{et} :

$\mathbb{Q}_p/\mathbb{Z}_p \cong X[\overline{\mathfrak{p}}^\infty]$. Then η_p° induces an isomorphism of formal groups: $\widehat{\eta}_p^\circ : \widehat{\mathbb{G}}_m = \mathrm{Spf}(\widehat{W[t,t^{-1}]}) \cong \widehat{X}$; so, we have $\omega(O) = \Omega_p \cdot (\widehat{\eta}^\circ_{p,*}\frac{dt}{t})$ for $\Omega_p \in W^\times$. This is the p-adic period. Write $\eta_p = (\eta^\circ, \eta_p^{et}) : \mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p \cong X[\mathfrak{p}^\infty] \times X[\overline{\mathfrak{p}}^\infty]$, and define a homomorphism ρ_p of $O_{(p)}^\times$ into the diagonal torus of $G(\mathbb{Z}_p)$ by $\alpha \circ \eta_p = \eta_p \circ \rho_p(\alpha)$ for $\alpha \in O_{(p)}$. Thus $\eta_p^\circ \circ \rho_p(\alpha) = \alpha\eta_p$ identifying $O_\mathfrak{p}$ with $\mathbb{Z}_p$ and $\eta_p^{et} \circ \rho_p(\alpha) = \alpha^c \eta_p^{et}$.

Fix a base w_1, w_2 of $\widehat{O}^{(p)} \cong T^{(p)}(X)$ over $\widehat{\mathbb{Z}}^{(p)}$, and identify $M_\mathbb{A}^{(p\infty)}$ with $(\mathbb{A}^{(p\infty)})^2$. The choice induces prime-to–p level structure $\eta^{(p)} : (\mathbb{A}^{(p\infty)})^2 \cong O \otimes_\mathbb{Z} \mathbb{A}^{(p\infty)} = V^{(p)}(X)$. We put $\eta = \eta_p \times \eta^{(p)}$. Define $\rho : O_{(p)}^\times \to G(\mathbb{Z}_p \times \mathbb{A}^{(p\infty)})$ by $\eta \circ \rho(\alpha) = \alpha \circ \eta$. Since $\alpha \in O_{(p)}^\times$ induces an isogeny $\alpha : X \to X$ sending $\alpha\eta^{(p)} = \eta^{(p)}\rho^{(p)}(\alpha)$, the point $z_0(O) = (X(O), \eta) \in Y^{(p)} = Y/GL_2(\mathbb{Z}_p)$ is fixed by $\rho(\alpha)$. Pick a fractional ideal $\mathfrak{a} \subset M$ prime to p; so, $\mathfrak{a} = (a\widehat{O}) \cap M$ for an idele $a \in M_\mathbb{A}^\times$ with $a_p = a_\infty = 1$. Then we have $z_0(\mathfrak{a}) = (X(\mathfrak{a}), \eta(\mathfrak{a})) = \rho(a)^{-1}(z_0(O))$.

Consider the formal completion $\widehat{Y} = \widehat{Y}_{z/W}$ of $Y^{(p)}_{/\mathcal{W}}$ along $z = z_0(\mathfrak{a}) \in Y^{(p)}(\mathbb{F})$. Then by the universality of $Y^{(p)}$, $\widehat{Y}$ satisfies

$$\widehat{Y}(A) \cong \widehat{\mathcal{E}}(A) := \left\{E_{/A} \middle| E \otimes_A \mathbb{F} = X(\mathfrak{a})_{/\mathbb{F}}\right\} / \cong,$$

where A runs through p-profinite local W-algebras with $A/\mathfrak{m}_A = W/\mathfrak{m}_W = \mathbb{F}$. By the deformation theory of Serre–Tate, $\widehat{Y} \cong \widehat{\mathbb{G}}_m$ canonically. Indeed, first $E_{/A} \in \widehat{\mathcal{E}}(A)$ is determined by the extension $E[p^\infty]^\circ \hookrightarrow E[p^\infty] \twoheadrightarrow E[p^\infty]^{et}$ of the Barsotti-Tate groups. By Serre–Tate, such an extension over A is classified by

$$\mathrm{Ext}(E[p^\infty]^{et}, E[p^\infty]^\circ) \cong \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_{p/A}, \mu_{p^\infty/A}) = \varprojlim_n \mu_{p^n}(A) = \widehat{\mathbb{G}}_m(A).$$

For this identification, we used $\eta_p^\circ : \mu_{p^\infty} \cong X(\mathfrak{a})[\mathfrak{p}^\infty]$ and its dual inverse $\eta_p^{et} : \mathbb{Q}_p/\mathbb{Z}_p \cong X(\mathfrak{a})[\overline{\mathfrak{p}}^\infty]$. Since $a_p = 1$, the above identification is independent of a and $\mathfrak{a}$. Since $\rho(\alpha)$ fix $z_0(\mathfrak{a})$, it acts on $\widehat{Y}$. As already remarked ([H10] Proposition 3.4):

Lemma 5.3. *Identifying $\widehat{Y}$ with $\widehat{\mathbb{G}}_m = \mathrm{Spf}(\varprojlim_n W[\tau, \tau^{-1}]/(\tau-1)^n)$, if $\alpha \in M^\times$, we have $\rho(\alpha)(\tau) = \tau^{\alpha^{1-c}}$ for complex conjugation c.*

5.3. **Hecke invariant subvarieties.** We write $I_\mathfrak{a}$ for the irreducible component of $Y^{(p)}_{/\mathbb{F}} = Y^{(p)} \times_\mathcal{W} \mathbb{F}$ containing $z_0(\mathfrak{a})$. Let $\mathfrak{a}$ be a fractional ideal prime to p of M with $\widehat{\mathfrak{a}} = a\widehat{O}$ for $a \in M_\mathbb{A}^\times$ with $a_p = a_\infty = 1$. Then $\rho(a)$ gives an isomorphism of $I := I_O$ onto $I_\mathfrak{a}$ sending $z_0(O)$ to $z_0(\mathfrak{a})$. Thus we identify $I = I_\mathfrak{a}$ for any $\mathfrak{a}$. Then for any $\alpha, \beta \in O_{(p)} \cap M^\times$, we have a skew diagonal $\Delta_{\alpha,\beta} = \mathrm{Im}(\rho(\alpha) \times \rho(\beta) : I \to I \times_\mathbb{F} I)$ in $I \times_\mathbb{F} I$ for $\alpha, \beta \in O_{(p)} \cap M^\times$.

Theorem 5.4. *Let $H \subsetneq \overbrace{I \times_\mathbb{F} \cdots \times_\mathbb{F} I}^{n}$ (with $n \geq 1$) be a proper closed irreducible subscheme with a dominant projection to the product of the first $n-1$ factor and to the last factor. If $z_0(O)^n \in H$ and H is stable under the diagonal action of a p-adic open subgroup of $O_{(p)}^\times/\mathbb{Z}_{(p)}^\times$, up to permutations of the first $(n-1)$ factors, we have*

$$H = \overbrace{I \times \cdots \times I}^{n-2} \times \Delta_{\alpha,\beta}.$$

This can be proven via Chai's theory of Hecke invariant subvariety of Shimura variety (see [H10] Corollaries 3.16 and 3.19). We recall the proof in the last lecture.

5.4. **Conclusion.** First we prove Theorem 5.2: Let $a_j \in \mathbb{Z}_p^\times$ $(j = 1, 2, \dots, h)$. Regard $a = a_j \in \mathrm{Aut}(\widehat{Y}) = \mathrm{Aut}_{gp}(\widehat{\mathbb{G}}_m)$ given by $\tau \mapsto \tau^a$. Let $z = z_0(O)$ and $\mathcal{O}_z$ for the stalk of $z \in Y^{(p)}$ mod p. Suppose that the algebra homomorphism: $\mathcal{O}_z^{\otimes h} := \overbrace{\mathcal{O}_z \otimes_{\mathbb{F}} \mathcal{O}_z \otimes \cdots \otimes_{\mathbb{F}} \mathcal{O}_z}^{h} \to \mathbb{F}[[\mathcal{T}]] = \mathcal{O}_{\widehat{\mathbb{G}}_{m/\mathbb{F}}}$ given by $f_1(\tau)\otimes\cdots\otimes f_h(\tau)$ to $\prod_j f_j(\tau^{a_j})$ has a nontrivial kernel $\mathfrak{K}$. The schematic closure H of $\mathrm{Spec}(\mathcal{O}_z^{\otimes h}/\mathfrak{K})$ in I^h is stable under the action of $\rho(O_{(p)}^\times)$. Thus by Theorem 5.4, there exist $i \neq j$ such that $O_p^\times/\mathbb{Z}_p^\times \ni a_i/a_j \in (O_{(p)}^\times \cap M^\times)/\mathbb{Z}_{(p)}^\times$. Let $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ be the representatives of $Cl_M(p)/\sim$. Let $a_j = \langle \mathfrak{a}_j^{1-c} \rangle$. Then $a_i/a_j \notin (O_{(p)} \cap M^\times)/\mathbb{Z}_{(p)}^\times$ for all $i \neq j$. This proves Theorem 5.2. $\square$

We have $L_p(\mathcal{T}, \gamma^k\zeta - 1) = \sum_j f_{\zeta,\mathfrak{a}_j}(\tau^{a_j})$ for the sum of Eisenstein series $f_{\zeta,\mathfrak{a}_j}$ of weight $k = p - 1$ with q-expansion $\sum_{n=0}^\infty a(n, f_{\zeta,\mathfrak{a}_j})q^n$. Dividing $f_{\zeta,\mathfrak{a}_j}$ by the Hasse invariant h does not change q-expansion and the value of $f_{\zeta,\mathfrak{a}_j}$. Thus we have

$$\mu(L_p(\mathcal{T}, \gamma^k\zeta - 1)) \overset{\text{Theorem 5.2}}{=} \max_{n,j}(\mathrm{ord}_p(a(n, f_{\zeta,\mathfrak{a}_j}))$$

as $\mathcal{T}$ is a local parameter at $z = z_0(O)$ and q is a local parameter at the cusp ∞ of the irreducible modular curve I. By computation, we can find a prime ℓ and index j such that $a(\ell, f_{\zeta,\mathfrak{a}_j}) = 1 + \zeta^{\log_p(\ell)/\log_p(\gamma)}\ell^{k-1}$ independent of the choice of ζ. Thus

$$0 \le \mu(L_p) \le \sup_\zeta \mu(L_p(\mathcal{T}, \zeta\gamma^k - 1)) \le \sup_{\zeta \in \mu_{p^\infty}(\overline{\mathbb{Q}}_p)} (\mathrm{ord}_p(1 + \zeta^{\log_p(\ell)/\log_p(\gamma)}\ell^{k-1})) = 0$$

as the p-power order of the root of unity $\zeta^{\log_p(\ell)/\log_p(\gamma)}$ grows indefinitely. This conclude the proof of the theorem. $\square$

Scrutinizing $a(n, f_{\zeta,\mathfrak{a}_j})$ more, we can prove

Corollary 5.5. *Suppose $F = \mathbb{Q}$. Then the μ-invariant of the anticyclotomic Katz p-adic L-function $L_p^-(x) = L_p(x, 0)$ also vanishes.*

When $F \neq \mathbb{Q}$, writing $L_p^-(x_\sigma) = L_p(x_\sigma, 0)$, $\mu(L_p^-)$ could be positive, though $\mu(L_p(x_\sigma, y)) = 0$ always. This possibility only occur if $[F : F[\mu_p]] = 2$ and M/F is unramified everywhere at finite places (see (M1–M3) in [H10] for a precise set of conditions for $\mu(L_p^-) > 0$).

6. Lecture 6: Hecke invariant subvariety

In this last lecture, we provide a sketch of the proof of the specific case (we used) of the conjecture asserting that "*a Hecke invariant subvariety of modulo p Shimura variety is a Shimura subvariety.*" We can prove this (conjectural) principle for the Hilbert modular variety and its self-products, but in this lecture, we only deal with modular curves and their self-products for notational simplicity. Any essential ingredients for the proof of the general case show up in this simpler case. Write $G = GL(2)_{/\mathbb{Z}}$ with center $Z \cong \mathbb{G}_{m/\mathbb{Z}}$. In this lecture, the word "variety" mean a reduced scheme of finite type over $\mathbb{F}$.

We recall the following lemma we mentioned already

Lemma 6.1. *Identifying $\widehat{Y}$ with $\widehat{\mathbb{G}}_m = \mathrm{Spf}(\varprojlim_n W[\tau, \tau^{-1}]/(\tau - 1)^n)$, if $\alpha \in M^\times$, we have $\rho(\alpha)(\tau) = \tau^{\alpha^{1-c}}$ for complex conjugation c.*

Note that if $\alpha \in M^\times$ is not prime to p, the action of $\rho(\alpha)$ is an endomorphism of $Y^{(p)}$ not an automorphism. A proof of this can be found in [H10] as Proposition 3.4. Then the action of $\rho(\alpha)$ on the Serre–Tate coordinate is given by $\tau \mapsto \tau^{\alpha^{1-c}}$ factoring through $G(\mathbb{A}^{(p\infty)})/Z(\mathbb{Q})$, since $Z(\mathbb{Q})$ acts trivially on the Shimura variety $Y^{(p)}$.

6.1. **Hecke invariant subvarieties.** We write I for the irreducible component of $Y^{(p)}_{/\mathbb{F}} = Y^{(p)} \times_{\mathcal{W}} \mathbb{F}$ containing $z_0 = z_0(O)$; so, the formal completion along z_0 is $\widehat{Y} = \widehat{I}$.

We want to give a sketch of a proof of the following two theorems ([H10] Corollaries 3.16 and 3.19):

Theorem 6.2. *Suppose that $H \subsetneq I \times_{\mathbb{F}} I$ is a closed irreducible subvariety of codimension 1 containing $(z_0, z_0) \in I \times_{\mathbb{F}} I$ stable under the action of a p-adic open subgroup of $O^\times_{(p)}/\mathbb{Z}^\times_{(p)} \overset{1-c}{\hookrightarrow} \mathbb{Z}_p^\times$. Then either $H = z_0 \times I$ or $H = I \times z_0$ or $H = \Delta_{\alpha,\beta}$ for $\alpha, \beta \in O_{(p)} \cap M^\times$.*

Theorem 6.3. *Let $H \subset \overbrace{I \times_{\mathbb{F}} \cdots \times_{\mathbb{F}} I}^{n}$ $(n \geq 2)$ containing z_0^n be a closed irreducible subvariety with a dominant projection to the product of the first $n-1$ factor and to the last factor. If H is of codimension 1 stable under the diagonal action of a p-adic open subgroup of $O^\times_{(p)}/\mathbb{Z}^\times_{(p)} \overset{1-c}{\hookrightarrow} \mathbb{Z}_p^\times$, up to permutations of the first $(n-1)$ factors, we have $H = \overbrace{I \times \cdots \times I}^{n-2} \times \Delta_{\alpha,\beta}$.*

6.2. **Rigidity lemma and proofs.** We start with general lemmas. Let $T \subset O^\times_{(p)}/\mathbb{Z}^\times_{(p)}$ be the open subgroup (under p-adic topology) fixing H by the diagonal action of $\rho(\alpha) \times \cdots \times \rho(\alpha)$ $(\alpha \in T)$. Then the formal completion $\widehat{H}$ along z_0^n is also stable under T, since z_0^n is fixed by T. By the Serre–Tate theory, $\widehat{H} \subset \widehat{I}^n \cong \widehat{\mathbb{G}}^n_{m/\mathbb{F}}$.

As we have seen, if a power series $\Phi(\mathcal{T}) = \Phi(\tau)$ $(\mathcal{T} = \tau - 1)$ satisfies $\Phi(\tau^z) = \Phi(\tau)^z$ for all z in an open subgroup of $\mathbb{Z}_p^\times$, then $\Phi(\tau) = \tau^s$ for $s \in \mathbb{Z}_p$ (Lemma 3.3). Note

$$\widehat{\mathbb{G}}_m = \mathrm{Spf}(\widehat{W[\tau, \tau^{-1}]}) = \mathrm{Spf}(W[[\mathcal{T}]]).$$

The cocharacter group of $\mathbb{G}_m^n$ is isomorphic to $\mathbb{Z}^n$, which we write $X_*(\mathbb{G}_m^n)$. Then by tautology, $\mathbb{G}_m^n = \mathbb{G}_m \otimes_{\mathbb{Z}} X_*(\mathbb{G}_m^n)$. Similarly in the formal setting, putting $X_*(\widehat{\mathbb{G}}_m^n) = X(\mathbb{G}_m^n) \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathbb{Z}_p^n$ (the formal cocharacter group), we have $\widehat{\mathbb{G}}_m^n = \widehat{\mathbb{G}}_m \otimes_{\mathbb{Z}_p} X_*(\widehat{\mathbb{G}}_m^n)$. A slightly more general version of Chai's rigidity lemma can be stated as follows (e.g., [H10] Lemma 3.7):

Lemma 6.4 (C.-L. Chai)**.** *If $Z \subset \widehat{\mathbb{G}}^n_{m/\mathbb{F}}$ is a reduced equidimensional formal subscheme of dimension r stable under the diagonal action of an open subgroup of $\mathrm{Aut}_{gp}(\widehat{\mathbb{G}}_m) = \mathbb{Z}_p^\times$, then*

$$Z = \bigcup_L \widehat{\mathbb{G}}_m \otimes_{\mathbb{Z}_p} L \subset \widehat{\mathbb{G}}^n_{m/\mathbb{F}},$$

where L runs over (finitely many) $\mathbb{Z}_p$-direct summand of $X_*(\widehat{\mathbb{G}}_m^n)$ of rank r.

The proof is given in [C] but is technical and long; so, we admit this lemma.

We apply this to the formal completion $\widehat{H}$ along $z_0^n = (z_0, z_0, \ldots, z_0) \in I^n$ inside $\widehat{I}^n = \widehat{\mathbb{G}}_m^n$. Since H is stable under $\tau \mapsto \tau^{\alpha^{1-c}}$ for $\alpha \in O^\times_{(p)}/\mathbb{Z}^\times_{(p)} \overset{1-c}{\hookrightarrow} \mathbb{Z}_p^\times$, by continuity,

$\widehat{H}$ is stable under the closure $\mathbb{Z}_p^\times$ of $\{\alpha^{1-c}|\alpha \in O_{(p)}^\times\}$. Since H is an excellent irreducible scheme, $\widehat{H}$ is reduced equidimensional of dimension $n-1$. Thus, by the above lemma,

$$\widehat{H} = \bigcup_L \widehat{\mathbb{G}}_m \otimes_{\mathbb{Z}_p} L \subset \widehat{\mathbb{G}}_m^n = \widehat{I}^n, \tag{6.1}$$

where L runs over (finitely many) $\mathbb{Z}_p$-direct summand of $X_*(\widehat{I}^n)$ of rank $n-1$. Let $\mathcal{H} \to H$ be the normalization of H. Since H is irreducible, $\mathcal{H}$ is irreducible. By (6.1), each point over z_0^n of $\mathcal{H}$ is indexed by $\{L\}$, and for the point $y_L \in \mathcal{H}$ over z_0^n corresponding to L, $\widehat{\mathcal{H}}_{y_L}$ is étale over $\widehat{\mathbb{G}}_m \otimes L$. Write $I^n = I' \times I''$ for $I' = I^{n-1}$ and $I'' = I$ for the last component.

Lemma 6.5. *The scheme $\mathcal{H}$ is finite flat over I' around z_0^{n-1}. In particular, each L is of rank $n-1$ and projects down to an open subgroup of $X_*(\widehat{\mathbb{G}}_m^{n-1}) \cong \mathbb{Z}_p^{n-1}$. If one of L surjects down onto $X_*(\widehat{I'})$ ($\widehat{I'} = \widehat{\mathbb{G}}_m^{n-1}$), all of L surjects down onto $X_*(\widehat{I'})$, and the projection $\mathcal{H} \to I'$ is étale finite around z_0^{n-1}.*

Proof. Since the projection of the first $(n-1)$-factor $I' = I^{n-1}$ is dominant, at least one of L, call it L_0, projects down to an open $\mathbb{Z}_p$-submodule of $X_*(\widehat{\mathbb{G}}_m^{n-1})$. If there is L with image in $X_*(\widehat{I'})$ of rank $< n-1$, the non-flat locus $\mathcal{H}^{nf} \subset \mathcal{H}$ of $\mathcal{H} \to I'$ is a nonempty proper closed subscheme of $\mathcal{H}$. Since $\dim \widehat{\mathbb{G}}_m \otimes L = \operatorname{rank} L = n-1$, $\mathcal{H}^{nf}$ has dimension $n-1$ equal $\dim \mathcal{H}$; so, $\mathcal{H}$ has to be reducible, a contradiction. Thus $\mathcal{H} \to I'$ is finite flat around z_0^{n-1} via faithfully flat descent from $\widehat{\mathcal{H}}/\widehat{I'}$ to $\mathcal{H}/I'$.

If one of L, call it L_0, surjects down to $X_*(\widehat{I'})$ and another L_1 has image smaller than $X_*(\widehat{I'})$, the ramified locus $\mathcal{H}^{ram}$ of $\mathcal{H} \to I'$ is nontrivial proper closed subscheme of dimension $n-1$, again a contradiction to the irreducibility of $\mathcal{H}$; so, $\mathcal{H} \to I'$ is étale finite around z_0^{n-1}, again via faithfully flat descent from $\widehat{\mathcal{H}}/\widehat{I'}$ to $\mathcal{H}/I'$. $\square$

When $n=2$, by applying a power of the p-power Frobenius or its dual to H (that is, applying $\rho(\alpha)$ for α generating $\mathfrak{p}O_{(p)}$ or its dual $\rho(\overline{\alpha})$), we may assume that at least one L surjects down to $X_*(\widehat{I'})$; so, by the above lemma, all L surjects down to $X_*(\widehat{I'})$. Thus we may assume that $\mathcal{H} \to I'$ is étale finite around z_0^{m-1}. Now assume $n=2$. Then, over an open dense subscheme $U \subset \mathcal{H}$ containing all points above z_0^2, the two projections $\pi_L : U \to I' = I$ and $\pi_R : U \to I'' = I$ are étale finite.

We consider the universal elliptic curve $(\mathbf{E}, \boldsymbol{\eta})_{/I}$. We pull it back to $\mathcal{H}$: $(\mathbf{A}, \eta_A) = \pi_L^*(\mathbf{E}, \boldsymbol{\eta})$ and $(\mathbf{B}, \eta_B) = \pi_R^*(\mathbf{E}, \boldsymbol{\eta})$. For a point $y \in \mathcal{H}$ over z_0^2, $\widehat{\mathcal{H}} := \widehat{\mathcal{H}}_y = \{(\tau^b, \tau^a)|t \in \widehat{I} = \widehat{\mathbb{G}}_m\} \subset \widehat{I} \times \widehat{I}$. Since $\pi_j : \mathcal{H} \to I$ is étale finite around y, we may assume that $a, b \in \mathbb{Z}_p^\times$; so, we may assume that $b = 1$. Let $X = X(O)$. The map $\widehat{I} \ni \tau \mapsto \tau^a \in \widehat{I}$ is induced on $\tau \in \widehat{I} = \mathrm{Hom}_{gp}(X[\overline{\mathfrak{p}}^\infty], X[\mathfrak{p}^\infty])$ by regarding a as an endomorphism of $X[\mathfrak{p}^\infty]$. Thus identifying $X = X(O)_{/\mathbb{F}}$ with the fibers $\mathbf{A}_y = \mathbf{B}_y$ of $\mathbf{A}$ and $\mathbf{B}$ at y, we regard the unit $a \in \mathrm{End}(X[\mathfrak{p}^\infty])$ as a O_p-linear map $a : \mathbf{A}_y[p^\infty] = X[p^\infty] \to X[p^\infty] = \mathbf{B}_y[p^\infty]$ inducing identity on $X[\overline{\mathfrak{p}}^\infty]$. We note the following fact (see [H10] Proposition 3.15):

Lemma 6.6 (C.-L. Chai)**.** *Further shrinking the open neighborhood U of y in $\mathcal{H}$, we may assume that the isomorphism $a : \mathbf{A}_y[p^\infty] = X[p^\infty] \to X[p^\infty] = \mathbf{B}_y[p^\infty]$ extends to $\widetilde{a} : \mathbf{A}_{/U}[p^\infty] \to \mathbf{B}_{/U}[p^\infty]$. This implies that $\widehat{\mathcal{H}}_u \cong \widehat{\mathbb{G}}_m$ by $(\tau, \tau^{\widetilde{a}}) \leftrightarrow \tau$ at any point $u \in U(\mathbb{F})$.*

Here is a sketch of a proof of the above lemma. Since a can be approximated p-adically by $\alpha_n \in R_{(p)}$ modulo p^n, a can be extended to $\rho(\alpha_n) : \mathbf{A}[p^n]_{\widehat{\mathcal{H}}} \to \mathbf{B}[p^n]_{\widehat{\mathcal{H}}}$. Passing to a limit, we have an extension $\widehat{a} : \mathbf{A}[p^\infty]_{\widehat{\mathcal{H}}} \to \mathbf{B}[p^\infty]_{\widehat{\mathcal{H}}}$. Write $\mathcal{O}$ for the stalk of $\mathcal{O}_{\mathcal{H}}$ at y; so, $\widehat{\mathcal{H}} = \mathrm{Spf}(\widehat{\mathcal{O}})$. Since $\widehat{a}$ is determined by its restriction a to $\mathbf{A}_y[p^\infty]$, it is a unique extension of a. Since $\widehat{\mathcal{O}} \otimes_{\mathcal{O}} \widehat{\mathcal{O}}$ is reduced (because of excellency of $\mathcal{O}$), the pull-backs of $\widehat{a}$ by two projections $\widehat{\mathcal{H}} \times_{\mathcal{H}} \widehat{\mathcal{H}} \to \widehat{\mathcal{H}}$ and three projections $\widehat{\mathcal{H}} \times_{\mathcal{H}} \widehat{\mathcal{H}} \times_{\mathcal{H}} \widehat{\mathcal{H}} \to \widehat{\mathcal{H}} \times_{\mathcal{H}} \widehat{\mathcal{H}}$ coincides; so, $\widehat{a}$ satisfies the descent datum with respect to $\widehat{\mathcal{O}}/\mathcal{O}$, getting desired U. □

Proof of Theorem 6.2. Since the two projections $\pi_j : \mathcal{H} \to I$ $(j = L, R)$ are dominant, we have $\mathrm{End}(\mathbf{A}) \otimes \mathbb{Q} = \mathrm{End}(\mathbf{B}) \otimes \mathbb{Q} = \mathbb{Q}$. Let $\mathbf{Y}_{/\mathcal{H}} = \mathbf{A} \times_{\mathcal{H}} \mathbf{B}$. Thus there are only two possibilities of $\mathrm{End}^{\mathbb{Q}}(\mathbf{Y}) = \mathrm{End}(\mathbf{Y}_{/\mathcal{H}}) \otimes \mathbb{Q}$: Either $\mathrm{End}^{\mathbb{Q}}(\mathbf{Y}) = \mathbb{Q} \times \mathbb{Q}$ or $\mathrm{End}^{\mathbb{Q}}(\mathbf{Y}) = M_2(\mathbb{Q})$. Suppose that $\mathrm{End}^{\mathbb{Q}}(\mathbf{Y}) = M_2(\mathbb{Q})$. By semi-simplicity of the category of abelian schemes, we have two commuting idempotent $e_? \in \mathrm{End}^{\mathbb{Q}}(\mathbf{Y})$ such that $e_A(\mathbf{Y}) = \mathbf{A}$ and $e_B(\mathbf{Y}) = \mathbf{B}$. Since $\mathrm{End}^{\mathbb{Q}}(\mathbf{Y}) = M_2(\mathbb{Q})$, we can find an invertible element $\widetilde{\beta}$ in $GL_2(\mathbb{Z}_{(p)}) \subset M_2(\mathbb{Q})$ such that $\widetilde{\beta} \circ e_A = e_B$; so, $\widetilde{\beta} : \mathbf{A} \to \mathbf{B}$ is an isogeny with $\widetilde{\beta} \circ \eta_A = \eta_B$, whose specialization to the fiber of $\mathbf{A}$ and $\mathbf{B}$ at y gives rise to an endomorphism $\beta \in \mathrm{End}(X(O)) \otimes \mathbb{Q}$. Thus the isogeny $\widetilde{\beta}$ is induced by $\rho(\beta)$, and we conclude $\Delta_{1,\beta} = H$.

We suppose $\mathrm{End}^{\mathbb{Q}}(\mathbf{Y}) = \mathbb{Q} \times \mathbb{Q}$ and try to get a contradiction (in order to prove that $\mathrm{End}^{\mathbb{Q}}(\mathbf{Y}) = M_2(\mathbb{Q})$). We pick a sufficiently small open compact subgroup $K \subset G(\mathbb{A}^{(p\infty)})$ maximal at p so that the normalization $\mathcal{H}_K$ of $H_K \subset Y_K \times Y_K$ is smooth at the image of y. The variety Y_K is naturally defined over a finite extension $\mathbb{F}_q/\mathbb{F}_p$ as the solution of the moduli problem $\mathcal{E}^{(p)}/K$. The universal elliptic curve $\mathbf{E}_K$ is therefore defined over $I_{K/\mathbb{F}_q}$, and $\mathcal{H}_K$ is a variety of finite type over $\mathbb{F}_q$. Let η be the generic point of $\mathcal{H}_{K/\mathbb{F}_q}$, and write $\overline{\eta}$ for the geometric point over η and $\mathbb{F}_q(\overline{\eta})^{sep}$ for the separable algebraic closure $\mathbb{F}_q(\overline{\eta})^{sep}$ of $\mathbb{F}_q(\eta)$ in $\mathbb{F}_q(\overline{\eta})$. Take an odd prime $\ell \neq p$, and consider the ℓ–adic Tate module $T_\ell(\mathbf{Y}_{\overline{\eta}})$ for the generic fiber $\mathbf{Y}_{\overline{\eta}}$ of $\mathbf{Y}$. We consider the image of the Galois action $\mathrm{Im}(\mathrm{Gal}(\mathbb{F}_q(\overline{\eta})^{sep}/\mathbb{F}_q(\eta)))$ in $GL_{O_\ell \times O_\ell}(T_\ell(\mathbf{Y}_{\overline{\eta}}))$. Then by a result of Zarhin ([DAV] Theorem V.4.7), the Zariski closure over $\mathbb{Q}$ of $\mathrm{Im}(\mathrm{Gal}(\mathbb{F}_q(\overline{\eta})^{sep}/\mathbb{F}_q(\eta)))$ is a reductive subgroup $\mathcal{G}$ of $GL_{\mathbb{Q}_\ell \times \mathbb{Q}_\ell}(T_\ell(\mathbf{Y}_{\overline{\eta}}) \otimes \mathbb{Q})$, and $\mathrm{Im}(\mathrm{Gal}(\mathbb{F}_q(\overline{\eta})^{sep}/\mathbb{F}_q(\eta)))$ is an open subgroup of $\mathcal{G}(\mathbb{Q}_\ell)$. Moreover, by Zarhin's theorem, the centralizer of $\mathcal{G}$ in $\mathrm{End}_{\mathbb{Q}_\ell \times \mathbb{Q}_\ell}(T_\ell(\mathbf{Y}_{\overline{\eta}}) \otimes \mathbb{Q})$ is $\mathrm{End}(\mathbf{Y}) \otimes \mathbb{Q}_\ell$. Since the reductive subgroups of $GL(2)$ are either tori or contain $SL(2)$, the derived group $\mathcal{G}_1(\mathbb{Q}_\ell)$ of $\mathcal{G}(\mathbb{Q}_\ell)$ has to be $SL_2(\mathbb{Q}_\ell \times \mathbb{Q}_\ell)$. By Chebotarev's density, we can find a set of closed points $u \in \mathcal{H}_K(\mathbb{F})$ with positive density such that the Zariski closure in $\mathcal{G}$ of the subgroup generated by the Frobenius element $Frob_u \in \mathrm{Im}(\mathrm{Gal}(\mathbb{F}_q(\overline{\eta})^{sep}/\mathbb{F}_q(\eta)))$ at u with $\pi_j(u) = u_j$ $(u_j \in I_K(\mathbb{F}))$ is a torus containing a maximal torus $T_u = (T_{u_1} \times T_{u_2}) \cap \mathcal{G}_1$ of the derived group $\mathcal{G}_1$ of $\mathcal{G}$. In particular the centralizer of T_u in $\mathcal{G}_1$ is itself. Thus $\mathbf{Y}_u$ is isogenous to a product of two non-isogenous elliptic curves $Y_1 = E_{u_1}$ and $Y_2 = E_{u_2}$ defined over a finite field. The endomorphism algebra $M_j = \mathrm{End}^{\mathbb{Q}}(Y_j)$ is an imaginary quadratic field of $\mathbb{Q}$ generated over $\mathbb{Q}$ by the relative Frobenius map ϕ_j induced by $Frob_u$, and $M_1 \neq M_2$. The relative Frobenius map $Frob_u$ acting on $X_*(\widehat{I}_{u_1}) \cong \mathbb{Z}_p$ has one eigenvalue: $\phi_1^{(1-c)\sigma}$ for the CM type $\Sigma_1 = \{\sigma\}$ of Y_1, which differ from the eigenvalues of $\phi_2 \in \mathrm{End}(Y_2)$ on $X_*(\widehat{I}_{u_2}) \cong \mathbb{Z}_p$. Since we have proven that over the open dense subscheme U of $\mathcal{H}$, the formal completion of U at $u \in U$ with $u = (u_1, u_2) \in X \subset V^2$ is canonically isomorphic to a formal subtorus $\widehat{Z} \subset \widehat{I}_{u_1} \times \widehat{I}_{u_2}$ with co-character group $X_*(\widehat{Z}) \cong \mathbb{Z}_p$, we may assume that our point $u = (u_1, u_2)$ as above is in the (open dense) image U_K of U in H_K. Projecting $X_*(\widehat{Z})$ down to the left and the right factors I_K, the projection map $X_*(\widehat{Z}) \to X_*(\widehat{I}_{u_j})$ is actually an injection commuting with the action of $Frob_u$. Thus $Frob_u$ has more than one distinct eigenvalues on $X_*(\widehat{Z})$ of rank 1, which is a contradiction. Thus we conclude that $\mathrm{End}^{\mathbb{Q}}(\mathbf{Y}) = M_2(\mathbb{Q})$ for any choice of small open compact subgroups K maximal at p.

As we have remarked at the beginning, $\widehat{\mathcal{H}}_y \subset \widehat{H}_{z_0^2} \subset \widehat{I} \times \widehat{I}$ is given by $\{\tau, \tau^{\beta^{1-c}})|t \in \widehat{\mathbb{G}}_m\}$ for nonzero $\beta \in O_{(p)}$. Suppose that y corresponds to L; so, $\widehat{\mathcal{H}}_y \subset \widehat{I} \times \widehat{I}$ coincides with $\widehat{\mathbb{G}}_m \otimes L$. On the other hand, we have the skew-diagonal $\Delta_\beta = \Delta_{1,\beta} = \{(z, \rho(\beta)(z))|z \in I\} \subset I \times I$. The formal completion $\widehat{\Delta}_\beta$ along (z_0, z_0) therefore coincides with $\widehat{\mathcal{H}}_y$ and $\widehat{\Delta}_\beta = \widehat{\mathbb{G}}_m \otimes L \subset \widehat{H}_{(z_0,z_0)}$ inside $\widehat{I}^2$. Thus $\Delta_\beta \subset H$. By the irreducibility of H, we conclude $H = \Delta_\beta$. □

There are two ways of proving Theorem 6.3. One is an induction reducing things to Theorem 6.2, and another is to prove that $\mathrm{End}(\mathbf{Y}) \otimes \mathbb{Q} = M_2(\mathbb{Q}) \times \mathbb{Q}^{n-2}$ for $\mathbf{Y} = \prod_j \pi_j^* \mathbf{E}$ for the projection π_j of $\mathcal{H}$ to j-th component I (after a permutation of the factors I).

References

Books

[ABV] D. Mumford, *Abelian Varieties*, TIFR Studies in Mathematics, Oxford University Press, 1994

[AME] N. M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Ann. of Math. Studies **108**, Princeton University Press, 1985

[DAV] G. Faltings and C.-L. Chai, *Degeneration of Abelian Varieties*, Springer, 1990

[GME] H. Hida, *Geometric Modular Forms and Elliptic Curves*, 2000, World Scientific Publishing Co., Singapore (a list of errata available at `www.math.ucla.edu/~hida`)

[HMI] H. Hida, *Hilbert modular forms and Iwasawa theory*, Oxford University Press, 2006 (a list of errata available at `www.math.ucla.edu/~hida`)

[IAT] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, NJ, and Iwanami Shoten, Tokyo, 1971.

[ICF] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Text in Mathematics, **83**, Springer, New York, 1980.

[LFE] H. Hida, *Elementary Theory of L–functions and Eisenstein Series*, LMSST **26**, Cambridge University Press, Cambridge, England, 1993

[MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, Cambridge University Press, Cambridge, England, 2000. (a list of errata available at `www.math.ucla.edu/~hida`)

[PAF] H. Hida, *p-Adic Automorphic Forms on Shimura Varieties*, Springer Monographs in Mathematics, 2004, Springer

Articles

[C] C.-L. Chai, A rigidity result for p–divisible formal groups, Asian J. Math. **12** (2008), 193–202 (available at: `www.math.upenn.edu/~chai`)

[C1] C.-L. Chai, Families of ordinary abelian varieties: canonical coordinates, p-adic monodromy, Tate-linear subvarieties and Hecke orbits, preprint 2003 (available at: `www.math.upenn.edu/~chai`)

[CE] R. F. Coleman and B. Edixhoven, On the semi-simplicity of the U_p-operator on modular forms. Math. Ann. **310** (1998), 119–127

[FeW] B. Ferrero and L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. **109** (1979), 377–395

[Fi] T. Finis, The μ-invariant of anticyclotomic L-functions of imaginary quadratic fields, Journal für die reine und angewandte Mathematik. Volume **2006**, Issue 596, 131-152

[Gr] R. Greenberg, Trivial zeros of p–adic L–functions, Contemporary Math. **165** (1994), 149–174

[GS] R. Greenberg and G. Stevens, p-adic L–functions and p–adic periods of modular forms, Inventiones Math. **111** (1993), 407–447

[H86a] H. Hida, Iwasawa modules attached to congruences of cusp forms, Ann. Sci. Ec. Norm. Sup. 4th series **19** (1986), 231–273.

[H86b] H. Hida, Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, Inventiones Math. **85** (1986), 545–613.

[H86c] H. Hida, Hecke algebras for GL_1 and GL_2, Sém. de Théorie des Nombres, Paris 1984-85, Progress in Math. **63** (1986), 131–163

[H88a] H. Hida, Modules of congruence of Hecke algebras and L-functions associated with cusp forms, Amer. J. Math. **110** (1988), 323–382

[H88b] H. Hida, On p-adic Hecke algebras for GL_2 over totally real fields, Ann. of Math. **128** (1988), 295–384.

[H89] H. Hida, Nearly ordinary Hecke algebras and Galois representations of several variables, Proc. JAMI Inaugural Conference, Supplement to Amer. J. Math. (1989), 115–134

[H04a] H. Hida, Non-vanishing modulo p of Hecke L–values, in: "*Geometric Aspects of Dwork's Theory, II*" (edited by Alan Adolphson, Francesco Baldassarri, Pierre Berthelot, Nicholas Katz, and Francois Loeser), Walter de Gruyter, 2004, pp. 735–784 (preprint available at www.math.ucla.edu/~hida)

[H04b] H. Hida, Greenberg's $\mathcal{L}$-invariants of adjoint square Galois representations, IMRN, 2004 No.59, 3177–3189

[H06] H. Hida, Anticyclotomic main conjectures, Documenta Math, Extra Volume Coates (2006), 465–532 (preprint available at www.math.ucla.edu/~hida)

[H07a] H. Hida, Non-vanishing modulo p of Hecke L-values and application, In "L-functions and Galois representations", London Mathematical Society Lecture Note Series **320** (2007) 207-269 (preprint available at www.math.ucla.edu/~hida)

[H07b] H. Hida, On a generalization of the conjecture of Mazur-Tate-Teitelbaum, International Mathematics Research Notices **2007** : article ID rnm102, 49 pages, doi:10.1093/imrn/rnm102

[H10] H. Hida, The Iwasawa μ–invariant of p–adic Hecke L–functions, to appear in Annals of Mathematics, (preprint available at www.math.ucla.edu/~hida or at http://annals.math.princeton.edu/issues/AcceptedPapers.html)

[K] N. M. Katz, p-adic L-functions for CM fields, Inventiones Math. **49** (1978), 199–297.

[M] B. Mazur, Modular curves and the Eisenstein ideal, Publ. IHES **47** (1977), 33–186

[MTT] B. Mazur, J. Tate and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Inventiones Math. **84** (1986), 1–48

[MT] B. Mazur and J. Tilouine, Représentations galoisiennes, différentielles de Kähler et "conjectures principales", Publication IHES **71** (1990), 65–103

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of Q. Inventiones Math. **76** (1984), 179–330

[O] M. Ohta, Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves. II, Math. Ann. **318** (2000), 557-583

[O1] M. Ohta, Congruence modules related to Eisenstein series. Annales scientifiques de l'École Normale Supérieure, Series 4, **36** (2003), 225–269

[P] R. Pink, Compact subgroups of linear algebraic groups. J. Algebra **206** (1998), 438–504

[R] K. A. Ribet, On l-adic representations attached to modular forms. II. Glasgow Math. J. **27** (1985), 185–194

[S] W. Sinnott, On the μ–invariant of the Γ–transform of a rational function, Inventiones Math. **75** (1984), 273–282

[S1] W. Sinnott, On a theorem of L. Washington, Astérisque **147-148** (1987), 209–224

[V] V. Vatsal, Special values of L-functions modulo p. International Congress of Mathematicians. Vol. II, 501–514, Eur. Math. Soc., Zürich, 2006

Department of Mathematics, UCLA, Los Angeles, CA 90095-1555, U.S.A.
E-mail address: hida@math.ucla.edu