CM COMPONENTS OF THE 'BIG' HECKE ALGEBRA

HARUZO HIDA

Contents

Date: December 14, 2010.

A series of 5 lectures at Hokkaido university from 12/13/2010 to 12/17/2010; the author is partially supported by the following NSF grants: DMS 0753991 and DMS 0854949 and by Clay Mathematics Institute as a Senior Scholar for 2010–2011.

Often we get the non-vanishing/non-triviality theorems of arithmetic invariant out of spreading out an invariant over to a bigger geometric object, i.e., the multiplicative group, Shimura variety and the spectrum of a large Hecke algebra. Here we describe a method using the spectrum of Hecke algebra as the bigger geometric object. This often work with non CM components. See my lectures at Kyoto about the use of multiplicative groups and Shimura varieties.

1. Overview: Is characterizing CM component important?

Fix a prime p and for simplicity, assume $p \geq 5$. Consider the space of cusp forms $S_{k+1}(\Gamma_0(Np^{r+1}), \psi)$ with $(p \nmid N, r \geq 0)$. These spaces are defined in [IAT] §3.5 under the same notation. In the rest of this series of lectures, we write the weight of modular form as $k+1$ since the l-Frobenius eigenvalue has absolute value $l^{k/2}$ for the Galois representation of a cusp form f of weight $k+1$.

1.1. Hecke algebras and CM components.

First, we give here an axiomatic definition of the cuspidal 'big' ordinary Hecke algebra $\mathbf{h}$ necessary to state our objectives without proof. After this is done, we give a precise definition of the CM components.

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

$$h = \mathbb{Z}[\psi][T(n)|n = 1, 2, \cdots] \subset \mathrm{End}(S_{k+1}(\Gamma_0(Np^{r+1}), \psi)).$$

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. In other words, $\lim_{n\to\infty} U(p)^{n!}$ converges p-adically in $h_{k+1,\psi/W}$ to the idempotent e of $\mathbf{h}_{k+1,\psi/W} = e \cdot h_{k+1,\psi/W}$.

Exercise 1.1. *Let A be a p-adically complete algebra, and suppose that A is of finite type as a module over $\mathbb{Z}_p$. Prove that $\lim_{n\to\infty} a^{n!}$ for any $a \in A$ exists in A giving an idempotent of A.*

Let $\psi_1 = \psi_N \times$ the tame p-part of ψ. Then we have a unique 'big' Hecke algebra $\mathbf{h} = \mathbf{h}_{\psi_1/W}$ characterized by the following two conditions:

(1) $\mathbf{h}$ is free of finite rank over $\Lambda := W[[T]]$ with $T(n) \in \mathbf{h}$,
(2) if $k \geq 1$ and $\varepsilon : \mathbb{Z}_p^\times \to \mu_{p^\infty}(W)$ is a character, as W-algebras,

$$\mathbf{h}/(1 + T - \psi(\gamma)\varepsilon(\gamma)\gamma^k)\mathbf{h} \cong \mathbf{h}_{k+1,\varepsilon\psi_k} \ (\gamma = 1 + p) \text{ for } \psi_k := \psi_1\omega^{1-k},$$

sending $T(n)$ to $T(n)$, where ω is the Teichmüller character.

We take an irreducible component $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbf{h})$ (thus $\mathbb{I}$ is a torsion-free algebra over Λ and is a Λ-module of finite type).

A (normalized) Hecke eigenform in $S_{k+1}(\Gamma_0(Np^{r+1}), \psi)$ has slope $\alpha \in \mathbb{Q}$ if $f|U(p) = a \cdot f$ with $|a|_p = p^{-\alpha}$. We simply put $\alpha = \infty$ if $a = 0$. Since $\lim_{n\to\infty} a^{n!} = 1 \Leftrightarrow \alpha = 0$, the algebra $\mathbf{h}_{k+1,\varepsilon\psi_k}$ acts non-trivially on a Hecke eigen cusp form f in $S_{k+1}(\Gamma_0(N), \varepsilon\psi_k; \overline{\mathbb{Q}}_p)$ if and only if

f has slope 0. A slope 0 form is also called an *ordinary from*. An important consequence of the above two facts is

(B) *The number of slope* 0 *Hecke eigenforms of level* Np^{r+1}*, of weight* $k+1$ *and of a 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 $f|T = \lambda(T)f$ for $T \in h$ factors through $h_{k+1,\psi}$ and $f = \sum_{n=1}^{\infty} a(n,f)q^n = \sum_{n=1}^{\infty} \lambda(T(n))q^n$. 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 $\mathbb{Q}(f) = \mathbb{Q}(\lambda(n)|n = 1, 2, \dots)$.

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 $\mathrm{Tr}(\rho_P(Frob_l)) = (T(l) \mod P)$ for almost all primes ℓ (see [GME] §4.2 for the construction of the Galois representation). 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 a W-algebra homomorphism $(P : \mathbb{I} \to \overline{\mathbb{Q}}_p) \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$, we get a Hecke eigenform $f_P \in S_{k+1}(\Gamma_0(Np^{r(P)+1}), \varepsilon\psi_k)$ 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 $\varepsilon_P = \varepsilon$, $\psi_P = \varepsilon\psi_k$, $r(P) = r$ 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 $P(a)$. Describing ρ_P, we have written $\mathrm{Tr}(\rho_P(Frob_l)) = (T(l) \mod P)$. The precise meaning of this is, for primes $l \nmid Np$,

$$\mathrm{Tr}(\rho_P(Frob_l)) = a(l)_P \ \text{ and } \ \det(\rho_P(Frob_l)) = \psi_P(l)l^{k(P)}. \tag{1.1}$$

We call a Galois representation ρ *CM* 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 $\mathbb{I}$ a *CM component* if $\rho_{\mathbb{I}}$ has CM.

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)

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

The assumptions are that the connected component of $\mathrm{Spec}(\mathbf{h})$ containing $\mathrm{Spec}(\mathbb{I})$ is a Gorenstein scheme and that $\mathrm{Spec}(\mathbb{I})$ is normal (see [H10c] §3.1 for more explanation).

If we interpolate L-values adding the cyclotomic variable, i.e, adding a variable s interpolating $L(m, Ad(\rho_P))$ varying integer m, we need to multiply the L-value by a nontrivial 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.

1.2. **Examples of characterization.** Here is a list of such characterizations (possibly conjectural):

- A cuspidal $\mathbb{I}$ has CM $\Leftrightarrow$ cuspidal $\mathbb{I}$ is a CM component $\Leftrightarrow$ there exist an imaginary quadratic field $M = \mathbb{Q}[\sqrt{-D}]$ in which p splits into $\mathfrak{p}\overline{\mathfrak{p}}$ and a character $\Psi = \Psi_{\mathbb{I}} : G_M = \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \widetilde{\mathbb{I}}^{\times}$ of conductor $\mathfrak{c}\mathfrak{p}^{\infty}$ for an ideal $\mathfrak{c}$ with $\mathfrak{c}\overline{\mathfrak{c}}D_M|N$ such that $\rho_{\mathbb{I}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \Psi$, where D_M is the discriminant of M and $\mathrm{Spec}(\widetilde{\mathbb{I}})$ is the normalization of $\mathrm{Spec}(\mathbb{I})$. This should be well known; see [H11] (CM1–3) in §1. This implies $L_p = L_p(\Psi^-)L(0, \left(\frac{M/\mathbb{Q}}{\cdot}\right))$, 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 (e.g., [T89] and [MT90]) of the anticyclotomic main conjecture, different from the one given by Rubin [Ru91] and [Ru94] via Euler system.
- $\mathbb{I}$ has CM $\Leftrightarrow$ ρ_P has CM for a single arithmetic prime P. By Ribet [Ri85], if ρ_P has CM, ρ_P has complex multiplication or Eisenstein. Then P has to be on a CM component or on an Eisenstein component(see [H10d] Sections 3 and 4).
- $\mathbb{I}$ has CM $\Leftrightarrow$ $\rho_{\mathbb{I}} \mod p$ has CM. 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 $\mathbb{Q}$; see [H10a] and [H10b]). This is a main result in [H10d].
- (Strong vertical conjecture in [H11]) Consider the field $\mathcal{V}_r(\mathbb{I}) \subset \overline{\mathbb{Q}}$ generated by $a_P(p)$ for all arithmetic P with level $\leq Np^{r+1}$ for a fixed $r \geq 0$. Then $\mathbb{I}$ has CM $\Leftrightarrow$ $[\mathcal{V}_r(\mathbb{I}) : \mathbb{Q}] < \infty$. This was a question of L. Clozel asked to me in the early 1990s. This holds true if the family contains some weight 2 cusp form whose abelian variety has good ordinary reduction modulo p or more generally a weight $k \geq 2$ cusp form whose motive is potentially crystalline ordinary at p (see Theorem 3.21). Here a crystalline motive is ordinary if its Newton polygon of the crystalline Frobenius coincides with the Hodge polygon. By

applying this crystalline-ordinary criterion, the family $\mathcal{F}_\Delta$ containing Ramanujan's Δ-function has $\mathcal{V}_0(\mathbb{I})$ of infinite degree over $\mathbb{Q}$. In the 1970s, Y. Maeda made a conjecture asserting that $\mathbb{Q}(a(p,f))$ for any normalized Hecke eigenform in $S_k(SL_2(\mathbb{Z}))$ has degree equal to $d := \dim S_k(SL_2(\mathbb{Z}))$ with its Galois closure having Galois group isomorphic to the symmetric group $\mathfrak{S}_d$ of d letters. This conjecture is numerically verified for $p = 2$ up to weight ≤ 3000 and, of course, implies our conjecture if $N = 1$.

- (Strong horizontal theorem in [H11]) Fix $k \geq 1$ and consider the field $\mathcal{H}_k(\mathbb{I})$ generated by $a_P(p)$ over $\mathbb{Q}(\mu_{p^\infty})$ for all arithmetic P with a fixed weight $k \geq 1$. Then

  $\mathbb{I}$ has CM $\Leftrightarrow [\mathcal{H}_k(\mathbb{I}) : \mathbb{Q}(\mu_{p^\infty})] < \infty$ (see Theorem 2.1).

- $\rho_{\mathbb{I}}$ restricted to the decomposition group D_p at p is completely reducible $\Leftrightarrow$ $\mathbb{I}$ has CM. This is the result of Ghate–Vatsal in [GV05]. There is a conjecture by R. Greenberg asserting that $\rho_P|_{D_p}$ for some arithmetic P is completely reducible $\Leftrightarrow$ $\mathbb{I}$ has CM (the local non-semisimplicity conjecture).
- (Constancy theorem) For cuspidal $\mathbb{I}$, $\mathcal{L}(Ad(\rho_{\mathbb{I}}))$ is a constant function over $\mathrm{Spf}(\mathbb{I})$ if and only if $\mathbb{I}$ is a CM component. This is a corollary of Strong horizontal theorem, and we will give an outline at the end of this series of lectures.
- (Wild guess) Does a cuspidal component $\mathbb{I}$ have CM by an imaginary quadratic field M if

  $$\mathcal{L}(Ad(f_P)) = \log_p(\mathfrak{p}) \ \text{ (up to algebraic numbers)}$$

  for one arithmetic P for a prime factor $\mathfrak{p}$ of p in M? Here taking a high power $\mathfrak{p}^h = (\alpha)$, $\log_p(\mathfrak{p}) = \frac{1}{h}\log_p(\alpha)$ for the Iwasawa logarithm $\log_p$.
- (Another wild guess) If $\mathbb{Q}(f_P) = \mathbb{Q}$ with $k(P) + 1 \geq 28$, $\mathbb{I}$ has CM?

All statements seem to have good arithmetic consequences, and these examples convinced the author importance of giving as many characterizations of CM components as possible.

2. Summary of our strategy

We will give a fairly detailed proof of the horizontal theorem tomorrow. Today I describe the strategy.

2.1. **A theorem.** Pick an infinite set $\mathcal{A}$ of arithmetic points P with fixed weight $k(P) = k \geq 1$. Write $H_{\mathcal{A}}(\mathbb{I}) \subset \overline{\mathbb{Q}}$ for the field generated over $\mathbb{Q}(\mu_{p^\infty})$ by $\{a_P(p)\}_{P\in\mathcal{A}}$. Here is what we can prove:

Theorem 2.1. *The field $H_{\mathcal{A}}(\mathbb{I})$ is a finite extension of $\mathbb{Q}(\mu_{p^\infty})$ if and only if $\mathbb{I}$ is CM.*

Hereafter we fix $\mathcal{A}$ and assume that $[H_{\mathcal{A}}(\mathbb{I}) : K] < \infty$ for $K := \mathbb{Q}(\mu_{p^\infty})$. We try to prove that $\mathbb{I}$ is CM. Put $K(f_P) = K[a_P(n); n = 1, 2, \dots] \subset \overline{\mathbb{Q}}$. We add a lemma:

Lemma 2.2. *Let $K = \mathbb{Q}(\mu_{p^\infty})$ and fix $k \geq 1$. Then $[K(f_P) : K(a_P(p))]$ 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 $[K(f_P) : K(a_P(p))] \leq [K[\psi_1, \omega] : K] \mathrm{rank}_{\mathbb{Z}_p[[T]]} \mathbf{h}$. □

For a prime l outside Np, let $A(l)$ be a root of $\det(X - \rho_{\mathbb{I}}(Frob_l)) = 0$. Then $\alpha_{l,P} := (A(l) \mod P)$ 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 above lemma, $L_P = K[\alpha_{l,P}]$ has bounded degree independent of l and P for all $P \in \mathcal{A}$.

2.2. **Weil numbers.** We start preparing to give 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) α is an algebraic integer; (2) $|\alpha^\sigma| = l^{k/2}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

It is plain that the number of Weil l-numbers of a given weight k in $\mathbb{Q}(\mu_{p^\infty})$ is finite up to roots of unity. We call two nonzero numbers a and b equivalent (written as $a \sim b$) if a/b is a root of unity. Here is a slight improvement of this fact:

Proposition 2.3. *Let $\mathcal{K}_d$ be the set of all finite extensions of $\mathbb{Q}[\mu_{p^\infty}]$ of degree d inside $\overline{\mathbb{Q}}$ whose ramification at l is tame. Then there are only finitely many Weil l-numbers of a given weight in the set-theoretic union $\bigcup_{L\in\mathcal{K}_d} L$ (in $\overline{\mathbb{Q}}$) up to equivalence.*

2.3. **A rigidity lemma.** We start with a lemma whose characteristic p version was studied by Chai:

Lemma 2.4. *Let W be a p-adic valuation ring finite flat over $\mathbb{Z}_p$. Let $\Phi(T) \in W[[T]]$, and suppose that there is an infinite subset $\Omega \subset \mu_{p^\infty}(\overline{K})$ such that $\Phi(\zeta - 1) \in \mu_{p^{r(\zeta)}}$ for all $\zeta \in \Omega$, where $p^{r(\zeta)}$ is the order of ζ. Then there exists $\zeta_0 \in \mu_{p^\infty}(W)$ and $s \in \mathbb{Z}_p$ such that $\zeta_0^{-1}\Phi(T) = (1 + T)^s = \sum_{n=0}^\infty \binom{s}{n} T^n$.*

Here is a sketch of a proof. There is another more elementary proof supplied to me by Kiran Kedlaya whose exposition will be made later.

Proof. Let $t = 1+T$ and write $\Phi(t)$ instead of $\Phi(T)$. Then by a variable change $t \mapsto \zeta_0' t$ for a suitable $\zeta_0' \in \mu_{p^\infty}$ and dividing Φ by another p-power root of unity, we may assume $\Phi(1) = 1$. Then we regard Φ as a morphism of formal schemes $\widehat{\mathbb{G}}_m \to \widehat{\mathbb{G}}_m$. Then $\Phi(\zeta) \subset \mu_{p^\infty}(\overline{\mathbb{Q}}_p)$ for all $\zeta \in \Omega$. Then for any σ in an open subgroup $\Gamma \subset \mathrm{Gal}(W[\mu_{p^\infty}]/W) \subset \mathbb{Z}_p^\times$, we have $\Phi(\zeta^\sigma) = \sigma(\Phi(\zeta))$. Since $\mathrm{Aut}(\widehat{\mathbb{G}}_m) = \mathbb{Z}_p^\times \supset \Gamma$, σ is induced by $t \mapsto t^z$ ($z \in \Gamma$), and $\Phi(t)^z - \Phi(t^z)$ has infinite common zeros in Ω. Thus $\Phi(t^z) = \Phi(t)^z$ for all $z \in \Gamma = 1 + p^m\mathbb{Z}_p$. The graph Z of $t \mapsto \Phi(t)$ in $\widehat{\mathbb{G}}_m \times \widehat{\mathbb{G}}_m$ is therefore stable under the diagonal action of $\mathbb{Z}_p^\times$. Pick a point $(t_0, \Phi(t_0))$ of infinite order in Z, then $(t_0^{1+p^m z}, \Phi(t_0^{1+p^m z})) = (t_0^{1+p^m z}, \Phi(t_0)^{1+p^m z}) = (t_0, \Phi(t_0))(t_0, \Phi(t_0))^{p^m z} \in Z$ for all $s \in \mathbb{Z}_p$. Thus Z has to be a coset of a formal subgroup generated by $(t_0, \Phi(t_0))^{p^m}$. Since $(1,1) \in Z$, we conclude Z is a formal torus, and we find $s \in \mathbb{Z}_p$ with $\Phi(t) = t^s$. □

Extending $\mathbb{I}$, we assume that $\mathbb{I}$ is integrally closed.

Proposition 2.5. *Suppose $[H_{\mathcal{A}}(\mathbb{I}) : \mathbb{Q}(\mu_{p^\infty})] < \infty$. Fix a rational prime $l \nmid N$ tamely ramified in L_P/K for all $P \in \mathcal{A}$ (this is true for all sufficiently large l). Then, for the discrete valuation ring $W = \mathbb{I} \cap \overline{\mathbb{Q}}_p$, we have A in $W[[T]][(1+T)^{1/p^n}] \cap \mathbb{I}$ for some $0 \le n \in \mathbb{Z}$ and a Weil l-number α_1 of weight 1 and a root of unity ζ_0 such that $A(P) = \alpha_{l,P} = \zeta_0\langle\alpha_1\rangle^{k(P)-1}$ for all arithmetic P; in other words, $A(T) = \zeta_0(1+T)^s$ for $s = \frac{\log_p(\alpha_1)}{\log_p(\gamma)}$.*

Proof. We give a sketch of a proof assuming $\mathbb{I} = W[[T]]$. By Lemma 3.9, we have only a finite number of Weil l-numbers of weight k in $\bigcup_{P\in\mathcal{A}} L_P$ up to multiplication by 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 3.13, 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. □

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

Lemma 2.6. *Let A be an integral domain over $W[[T]]$ of characteristic different from 2. Assume that the endomorphism σ_2 on $W[[T]]$ 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.*

Heuristically, the assumption implies that $\sigma \mapsto \rho^2(\sigma)$ is still a representation; so, it has to have an abelian image. We can make this argument rigorous.

Proof of Theorem 2.1. For simplicity, assume that $\rho_{\mathbb{I}}$ has values in $GL_2(\mathbb{I})$. Let $K := \mathbb{Q}(\mu_{p^\infty})$ and $L_P = K(\alpha_{l,P})$ for a prime l. We need to prove that $[H_{\mathcal{A}}(\mathbb{I}) : K] < \infty \Rightarrow \mathcal{F}$ has complex multiplication. Thus suppose $[H_{\mathcal{A}}(\mathbb{I}) : K] < \infty$. For each arithmetic P with $k(P) = k$, by Lemma 3.2, $[K(f_P) : K(a_P(p))] < d$ for a positive integer d independent of P. Thus $[L_P : K] < 2d[H_{\mathcal{A}}(\mathbb{I}) : K]$ for each prime l. Therefore, any odd prime $l > 2d[H_{\mathcal{A}}(\mathbb{I}) : K]$ is at most tamely ramified in L_P/K. Take such an odd prime $l > 2d[H_{\mathcal{A}}(\mathbb{I}) : K]$ 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 3.14, 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 with $r(Q) = 1$. Note that ζ, ζ' is at most in a quadratic extension of $\mathbb{Q}(f_Q)$ which is a finite extension of $\mathbb{Q}$; so, 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 CM. $\square$

3. Horizontal theorem

First we give more details of the tools which will be used in the proof of

Theorem 3.1. *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 $K := \mathbb{Q}(\mu_{p^\infty})$ by $\{a_P(p)\}_{P\in\mathcal{A}}$. Then the field $\mathcal{H}_{\mathcal{A}}(\mathbb{I})$ is a finite extension of K if and only if $\mathbb{I}$ has CM. Moreover if $\mathbb{I}$ is not CM,*

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

We prepare a lemma:

Lemma 3.2. *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 $\mathbb{I}$ has CM. Put $K(f_P) = K[a_P(n); n = 1, 2, \dots] \subset \overline{\mathbb{Q}}$. 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 $l \gg 0$.

3.1. **Weil number.** We start preparing for a proof of the theorem. In this section, we gather some results on Weil numbers. Here is an example of natural appearance of Weil numbers. For any Hecke eigenform $f \in S_{k+1}(\Gamma_0(Np^{r+1}), \psi)$ with $f|T(l) = a_l f$, if l is prime to Np, then the roots of $X^2 - a_l X + \psi(l)l^k = 0$ are Weil numbers of weight k. When $k = 1$ (that is, for weight 2 cusp forms), the Hasse–Weil conjecture for $X_1(N)$ and the Ramanujan–Petersson conjecture were proven by Shimura by computing $L(s, X_1(N))$ as a product of $L(s, f)$ for Hecke eigenforms of weight 2 on $X_1(N)$ via the roots α, β of $X^2 - a_l X + \psi(l)l = 0$ (see [Sh58] and [IAT] §7.5) and then reducing the proof of $|\alpha| = |\beta| = \sqrt{p}$ to the work of Weil for curves. For

higher weight modular forms, Deligne went a similar path to prove the Ramanujan–Petersson conjecture, reducing it to his proof of Weil's conjecture for the fiber product $\overbrace{\mathbf{E}\times_X\mathbf{E}\times_X\cdots\times_X\mathbf{E}}^{k-2}$ (see [D69] and also [Sc90]). Thus one expects to have Weil number of weight k even for Hecke eigenvalues of $U(p)$ for a cusp form of weight $k+1\geq 2$, as "old" Hecke eigenform level p added to the original level $p\nmid N$ has α or β as $U(p)$-eigenvalue. This is not always true for eigenforms properly of level Np^{r+1} ($r\geq 0$) called *primitive* forms. For example, if p^{r+1} is bigger than the p-conductor of ψ, then a_p could be 0 or $\pm\sqrt{\psi_0(p)}p^{(k-1)/2}$ for the primitive character associated to ψ if ψ is imprimitive at p; so, Weil number of weight $k-1$).

On the other hand, if ψ has p-conductor p^{r+1} (with $r\geq 0$), writing $f|U(p)=a_p\cdot f$, a_p is a Weil number of weight k. This fact can be found in [MFM] Theorem 4.6.17). In this case, the proof is elementary without recourse to arithmetic geometry.

By these facts, Weil numbers have intimate relation to Diophantine geometry; so, it is natural to ask how often we find such numbers in a given algebraic number field of finite or infinite degree over $\mathbb{Q}$. This is what we study here. Here are two easy lemmas:

Lemma 3.3. *Let $K/\mathbb{Q}$ be a finite extension of $\mathbb{Q}$ in $\mathbb{C}$ stable under the "complex conjugation" c (so, write $c\in\mathrm{Aut}(K)$ for the field automorphism induced by the complex conjugation). If for any field embedding $\sigma: K\hookrightarrow\mathbb{C}$, we have $c\circ\sigma=\sigma\circ c$, K is a totally imaginary quadratic extension of a totally real field (in short, a CM field). In particular, if α is a Weil number, $\mathbb{Q}(\alpha)$ is contained in a CM field.*

Exercise 3.4. *Prove the above lemma.*

Here is another lemma due to Kronecker:

Lemma 3.5. *If ζ is a Weil number of weight 0, then there exists a positive integer N such that $\zeta^N=1$.*

Exercise 3.6.
(1) *First prove that a discrete subset of a compact set is finite.*
(2) *For a non-real Weil number ζ of weight 0, consider the field $K=\mathbb{Q}(\zeta)$. Show that $2\big|[K:\mathbb{Q}]$.*
(3) *Show that $K_{\mathbb{R}}:=K\otimes_{\mathbb{Q}}\mathbb{R}$ is isomorphic to $\mathbb{C}^d$ for $d=[K:\mathbb{Q}]/2$.*
(4) *Consider $C^d\subset\mathbb{C}^d=K_{\mathbb{R}}$ for $C=\left\{z\in\mathbb{C}\middle||z|=1\right\}$. Show that the subgroup generated G by the image of ζ in C^d is discrete.*
(5) *Using (1), show that G is a finite group, proving the above lemma.*

We call two nonzero algebraic numbers a and b equivalent (written as $a\sim b$) if a/b is a root of unity.

Lemma 3.7. *Let K be a finite field extension of $\mathbb{Q}(\mu_{p^\infty})$ inside $\overline{\mathbb{Q}}$. 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 $K = \mathbb{Q}(\mu_{p^\infty})$ and there is only one prime in $\mathbb{Z}[\mu_{p^\infty}]$ above (l) (for example, if $l = p$), any Weil l-number of weight k is equivalent to $(l^*)^{k/2}$ (as long as $(l^*)^{k/2} \in \mathbb{Q}[\mu_{p^\infty}]$), where $l^* = (-1)^{(l-1)/2}l$ if l is odd, and $l^* = 2$ if $l = 2$.

An analytic result of Loxton confirms that, up to equivalence, there are only finitely many Weil l-numbers of a given weight in the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ (see [L74] Lemma 7). We now give an algebraic proof.

Proof. The decomposition group of each prime l is of finite index in $\mathrm{Gal}(K/\mathbb{Q})$ (identifying $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_p^\times$ by the p-adic cyclotomic character, the decomposition group is generated by l if $l \neq p$, and otherwise $l = p$, p is fully ramified in $\mathbb{Q}[\mu_{p^\infty}]$; see [ICF] Chapter 2); so, 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, there are only finitely many possibilities of prime factorization of (α) if $l \neq p$. 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 (Lemma 3.5). If there is only one prime over l in $\mathbb{Z}[\mu_{p^\infty}]$, any Weil l-number of weight k is equivalent to $(l^*)^{k/2}$, as long as $(l^*)^{k/2} \in \mathbb{Q}[\mu_{p^\infty}]$. Thus the result follows from this if $K = \mathbb{Q}(\mu_{p^\infty})$.

Let $W(l,k)$ (resp. $W_K(l,k)$) be a complete set of representatives of Weil l-numbers in $\mathbb{Q}(\mu_{p^\infty})$ (resp. in K) of weight k under the equivalence. By the above argument, $W(l,k)$ is a finite set, and we want to prove that $W_K(l,k)$ is finite. Write $d = [K : \mathbb{Q}(\mu_{p^\infty})]$. If $\alpha \in K$ is such a Weil l-number, then $N_{K/\mathbb{Q}(\mu_{p^\infty})}(\alpha)$ is equivalent to a number in $W(l, kd)$. Thus $N_{K/\mathbb{Q}(\mu_{p^\infty})}$ induces a map $N : W_K(l,k) \to W(l,dk)$. Write L for the field generated by elements in $W(l,dk)$. Then $L/\mathbb{Q}$ is a finite abelian extension in $\mathbb{Q}(\mu_{p^\infty})$. Since no prime completely splits in $\mathbb{Q}(\mu_{p^\infty})$, the decomposition subgroup D of l in $\mathrm{Gal}(K/\mathbb{Q})$ is an open subgroup of finite index. Thus there are only finitely many valuations v of K with $v(l) = 1$. Let $\mathcal{V}$ be the set of valuations v of K with $v(l) = 1$, which is a finite set. For $v \in \mathcal{V}$ and $\alpha \in W_K(l,k)$, $v(\alpha) \in [0,k] \cap d^{-1}v(L)$, because $N_{K/\mathbb{Q}(\mu_{p^\infty})}(\alpha)$ is in $W(l,dk)$ up to roots of unity. Let $V := \prod_{v\in\mathcal{V}} ([0,k] \cap d^{-1}v(L))$, which is a finite set. We have a map $\mathrm{ord}_l : W_K(l,k) \to V$ sending α to $\mathrm{ord}_l(\alpha) = (v(\alpha))_{v\in\mathcal{V}}$. If $\mathrm{ord}_l(\alpha) = \mathrm{ord}_l(\beta)$ $(\alpha, \beta \in W_K(l,k))$, then α/β is an algebraic integer with complex absolute value $|(\alpha/\beta)^\sigma| = 1$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; so, by Kronecker's theorem (Lemma 3.5), $\alpha \sim \beta$. Thus ord_l is an injection, proving the finiteness of $W_K(l,k)$. □

To prove an improvement of the above fact, we first state a lemma:

Lemma 3.8. *Let $K = \mathbb{Q}_l[\mu_{p^\infty}]$ inside $\overline{\mathbb{Q}}_l$, and let K^t/K (resp. K^{ur}/K) be the maximal tamely l-ramified extension (resp. the maximal unramified extension inside K^t). Then we have K^t has the l-inertia group*

isomorphic to $\widehat{\mathbb{Z}}^{(l)}(1)$*, where* $\widehat{\mathbb{Z}}^{(l)}(1) = \varprojlim_{l\nmid N} \mu_N(\overline{\mathbb{Q}}_l)$ *as* $\mathrm{Gal}(K^{ur}/\mathbb{Q}_l)$*-modules, and we have*

$$\mathrm{Gal}(K^t/K) \cong \begin{cases} \widehat{\mathbb{Z}}^{(p)} \ltimes \widehat{\mathbb{Z}}^{(l)}(1) & \text{if } l \neq p, \\ \widehat{\mathbb{Z}} \ltimes \widehat{\mathbb{Z}}^{(l)}(1) & \text{if } l = p \end{cases} \tag{3.1}$$

a semi-direct product with $\mathrm{Gal}(K^t/K) \triangleright \widehat{\mathbb{Z}}^{(l)}(1)$*, and*

$$\mathrm{Gal}(K^{ur}/K) \cong \begin{cases} \widehat{\mathbb{Z}}^{(p)} & \text{if } l \neq p, \\ \widehat{\mathbb{Z}} & \text{if } l = p. \end{cases}$$

In particular, for a given $d > 0$*, there are finitely many extensions in* K^t/K *of degree* $\leq d$*.*

A proof can be found in most books on algebraic number theory.

Proposition 3.9. *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 (i.e., the ramification index over* $\mathbb{Q}[\mu_{p^\infty}]$ *is prime to* l*). Then there are only finitely many Weil* l*-numbers of a given weight, up to equivalence, 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 $K_l = K \otimes_{\mathbb{Q}} \mathbb{Q}_l$, by tameness, there are only finitely many isomorphism class of $K \otimes_{\mathbb{Q}} \mathbb{Q}_l$-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 a 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 $v_1, \ldots, v_n$. Indeed, for any composite X of two copies of L_l embedded as K_l-algebras inside a commutative semi-simple K_l-algebra, $a \otimes b \mapsto a \cdot b \in X$ extends to a surjective algebra homomorphism $L_l \otimes_{K_l} L_l \to X$ by the universality of tensor product. Considering $L_l \otimes_{K_l} L_l$, we can think of any possible composite containing α and β. Another important point is the the simple components of $L_l \otimes_{K_l} L_l$ are indexed by equivalence classes of valuations v_is (see [BCM] VI.8). These facts in mind, consider a tuple

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

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 (Lemma 3.5), $\alpha \sim \beta$. Since there are only finitely many possibilities of $V(\alpha)$, there are only finitely many classes.

Exercise 3.10.
(1) *For finite extensions* K *and* L *of* $\mathbb{Q}$*, prove that the algebra* $K \otimes_{\mathbb{Q}} L$ *is a product of finite extensions generated by the image of* K *and the image of* L*.*
(2) *Prove that any field generated by two fields one isomorphic to* K *and another isomorphic to* L *is isomorphic to a simple fctor of* $K \otimes_{\mathbb{Q}} L$*.*

It is not very difficult to prove

Lemma 3.11. *Let $\mathcal{K}_?$ be one of $\mathcal{K}_{\mathcal{L}}$, $\mathcal{K}_G$ and $\mathcal{K}_d$. Suppose $\mathcal{K}_? \neq \emptyset$. Then the group of roots of unity in the composite $\mathbf{L}$ of L for $L \in \mathcal{K}_?$ in $\overline{\mathbb{Q}}$ contains $\mu_{p^\infty}(K)$ as a subgroup of finite index.*

Exercise 3.12. *Prove the above lemma.*

By this lemma, 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 a given weight is finite.

3.2. **A rigidity lemma.** We start with a rigidity lemma:

Lemma 3.13. *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, $\Phi(\zeta^s - 1) = \Phi(\zeta - 1)^s \Leftrightarrow \Phi(t^s - 1) = \Phi(t-1)^s$ ($t = 1+T$), and the power series is the desired form as stated in a remark of Chai [C03] Remark 6.6.1 (iv) (see also [C08]). Here is another elementary proof supplied to me by Kiran Kedlaya (a proof following Chai can be found in [H11] §5).

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 $\Phi(T)=\sum_{n=0}^{j}a_nT^n+T^{j+1}f(T)$ with $f(T)\in W[[T]]$, we have

$$\sum_{n=0}^{j}a_nT^n\equiv 1+b_0T^{p^{h_0}}\equiv(1+T^{p^{h_0}})^{b_0}\equiv(1+T)^s \mod (\mathfrak{m}_W+(T^{j+1})).$$

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 $s=\sum_{k=0}^{\infty}b_kp^{h_k}\in\mathbb{Z}_p$, $\Phi(T)/(1+T)^s-1=\sum_{n=1}a_nT^n$ 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 act on power series through coefficients by $(\sum_n a_nT^n)^\phi=\sum_n a_n^\phi T^n$, 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 3.14. *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 $A_P(l)=\alpha_{l,P}=\zeta_0(\varepsilon_P(\gamma))^{\log_p(\alpha_1)/\log_p(\gamma)}\langle\alpha_1\rangle^{k(P)}$ 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. In this lecture, we give a proof assuming $\mathbb{I}=\Lambda=W[[T]]$, referring to [H11] of Proposition 5.2 for a proof dealing with the general case. Let $A=A(l)$. By Proposition 3.9 (and a remark after Lemma 3.11), we have only a finite number of Weil l-numbers of weight k in $\bigcup_{P\in\mathcal{A}}L_P$ up to multiplication by roots of unity in $\mu_{p^\infty}(K)$, 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 p-power order roots of unity, unless the automorphic representation generated by f_P is Steinberg at $l\neq p$. If f_{P_0} is Steinberg at $l\neq p$ for one arithmetic P_0, then l is a factor of N; so, this case is excluded by our assumption $l\nmid N$ (though this case can be also treated; see [H11] Proposition 5.2). The automorphic representation generated by f_P for arithmetic P has l-component in principal series if $l\nmid N$ or $k(P)>2$ (as Steinberg case for p is limited to $k(P)=1$, otherwise, as already explained, the $U(p)$ eigenvalue is $p^{(k(P)-1)/2}$ up to roots of unity or 0 which is not a p-adic unit, against ordinarity at p).

After a variable change $T \mapsto Y = \gamma^{-k}(1+T)-1$, we get $A(Y)|_{Y=0} = A(T)|_{T=\gamma^k-1}$. 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 $\Phi(Y) := \alpha^{-1}A(Y) = \alpha^{-1}A(\gamma^{-k}(1+T)-1) \in W[[Y]]$. The subset Ω of Ω_1 made up of $\zeta \in \Omega_1$ such that $\Phi(\zeta-1) \in \mu_{p^\infty}(K)$ is an infinite set. Then Φ satisfies the assumption of Lemma 3.13, 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 $A(T) = \zeta\alpha(\gamma^{-k}(1+T))^{s_1}$. Let $T = \zeta'\gamma^{k'}-1$ for $\zeta' \in \mu_{p^\infty}(K)$. Then $A(\zeta'\gamma^{k'}-1) = \zeta\alpha(\zeta'\gamma^{-k+k'})^{s_1}$, which is equal to a Weil l-number of weight k'. To get the expression of s as in the proposition, take $k' > 1$. Then

$$\alpha_1 := \frac{A(\gamma^{k'}-1)}{A(\gamma^{k'-1}-1)} = \frac{\zeta\alpha(\zeta'\gamma^{-k+k'})^{s_1}}{\zeta\alpha(\zeta'\gamma^{-k+k'-1})^{s_1}} = \gamma^{s_1},$$

which is an algebraic number α_1 independent of k'. Note that for $k' > 1$, α_1 is a ratio of Weil l-numbers of weight $k'-1$ and k', and hence α_1 is not a root of unity. Thus we have $s_1 = \frac{\log_p(\alpha_1)}{\log_p(\gamma)}$. We now equate

$$\zeta\zeta_\alpha\gamma^{\log_p(\alpha)/\log_p(\gamma)}(\gamma^{-k}(1+T))^{\log_p(\alpha_1)/\log_p(\gamma)} = \zeta_0(1+T)^{\log_p(\alpha_1)/\log_p(\gamma)},$$

where $\alpha = \zeta_\alpha\gamma^{\log_p(\alpha)/\log_p(\gamma)}$ for roots ζ_α and ζ_0 of unity. By putting $T = 0$, we get

$$\zeta\zeta_\alpha\gamma^{\log_p(\alpha)/\log_p(\gamma)-k(\log_p(\alpha_1)/\log_p(\gamma))} = \zeta_0,$$

which shows

$$\zeta_0 = \zeta\zeta_\alpha \quad \text{and} \quad ks_1 = \log_p(\alpha)/\log_p(\gamma).$$

We conclude $\alpha_1 = \sqrt[k]{\langle\alpha\rangle}$ for $\langle\alpha\rangle = \alpha\zeta_\alpha^{-1}$, which is a Weil l-number of weight 1. □

3.3. **Proof of Theorem 3.1.** Consider the W-algebra endomorphism $\sigma_s : (1+T) \mapsto (1+T)^s = \sum_{n=0}^\infty \binom{s}{n}T^n$ of Λ for $s \in \mathbb{Z}_p$.

Lemma 3.15. *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.

Exercise 3.16. *Prove* $\mathrm{Tr}(\rho^2) = \mathrm{Tr}(\rho^{sym\otimes 2}) - \det(\rho)$

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, as $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$-modules, we have $\mathbf{1} \hookrightarrow Ad(\rho)$. 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 which is impossible as $p > 2$). □

Here is a well known lemma called Steinitz's theorem:

Lemma 3.17. *Let Q be a field with a field automorphism σ and $\overline{Q}$ be an algebraic closure of Q. Then σ extends to an automorphism of $\overline{Q}$.*

Let Q be now the field of fractions of $\mathbb{I}$ and fix an algebraic closure $\overline{Q}$ of Q. We need one more fact from ring theory.

Lemma 3.18. *Suppose $\mathbb{I}$ is isomorphic to one variable power series ring $\Lambda_X := W[[X]]$. If $L \subset V$ be a Λ_X-submodule of finite type spanning V over Q, then the intersection $\widetilde{L}$ of all Λ_X-free submodules of V of rank equal to $\dim V$ is free Λ_X-module of rank equal to $\dim V$.*

We call $\widetilde{L}$ the *reflexive closure* of L (cf. [BCM] VII.4.2).

Proof of Theorem 3.1. For simplicity, we assume that $\mathbb{I} \cong \Lambda_X = W[[X]]$ (see [H11] §6 for the treatment in general). The Galois representation $\rho_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(Q)$ is continuous and hence has compact image. Then $\mathrm{Im}(\rho_{\mathbb{I}}) \cdot \mathbb{I}^2$ is a compact set covered by finitely many open subsets $\lambda_i \mathbb{I}^2$ with $\lambda_i \in Q^\times$ as the neighborhoods of 0 in $M_2(Q)$ is given by $\{\lambda \cdot \Lambda^2\}_{\lambda \in Q^\times}$. Thus $L = \sum_{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} \rho_{\mathbb{I}}(\sigma)\mathbb{I}^2$ is a $\mathbb{I}$-submodule of finite type of $V = Q^2$ spanning V over Q. Take the reflexive closure $\widetilde{L}$. For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\widetilde{\rho_{\mathbb{I}}(\sigma)L} = \rho_{\mathbb{I}}(\sigma)\widetilde{L}$ as $\widetilde{L}$ is uniquely determined by L; so, $\widetilde{L}$ is stable under the Galois action. By Lemma 3.18, $\widetilde{L}$ is free $\mathbb{I}$-module of rank 2; so, writing $\rho_{\mathbb{I}}$ in a matrix form, we may assume that $\rho_{\mathbb{I}}$ has values in $GL_2(\mathbb{I})$.

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 CM; so, let us suppose $[\mathcal{H}_{\mathcal{A}}(\mathbb{I}) : K] < \infty$. For each arithmetic P with $k(P) = k$, by Lemma 3.2, $[K(f_P) : K(a_P(p))] < d$ 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 3.14, 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 $P_0 \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ to see the order of ζ is bounded independent of l. Let α be a root of $\det(X - \rho_{P_0}(Frob_l)) = 0$ in $\overline{\mathbb{Q}}_p$. Then $[\mathbb{Q}(f_{P_0}, \alpha) : \mathbb{Q}(f_{P_0})] \leq 2$. Write $m = [\mathbb{Q}(f_{P_0}) : \mathbb{Q}]$, $\zeta = \zeta_p \zeta^{(p)}$ with $\zeta_p \in \mu_{p^\infty}$ and $\zeta^{(p)}$ of order prime to p. Write R for the integer ring of $\mathbb{Q}(f_{P_0}, \alpha)$; so, $2m \geq \dim_{\mathbb{F}_p} R/pR$. Since $(1+T)^s \equiv 1 \mod \mathfrak{m}_{\mathbb{I}}$, the order of $\zeta^{(p)}$ is bounded by p^{2m}. Note that $P_0((1+T)^a) = (1+T)^a \mod P_0$ is in a finite extension L of $\mathbb{Q}_p$ depending only on the denominator p^n of a. For example, if P_0 contains $(1+T) - \gamma^k$, $L \subset \mathbb{Q}_p[\gamma^a] = \mathbb{Q}_p[\sqrt[p^n]{(1+p)}] \subset \mathbb{Q}_p[\sqrt[p^B]{(1+p)}]$ for $\gamma = 1 + p$, where $B > 0$ is an integer such that ap^B

abd $a'p^B$ is in $\mathbb{Z}_p$ (which can be chosen independently of l) . We have $\zeta_p \in L[\zeta_p]$ whose degree is bounded by $2m[L:\mathbb{Q}_p]$; so, the order of ζ_p is also bounded independent of l. Replacing W by its finite extension, we may assume that all such roots of unity are in W.

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 $G = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$. In Lemma 3.15, take $A = \overline{Q}$ (so, $\sigma_2 \in \mathrm{Aut}(\Lambda)$ extends to an automorphism of $\overline{Q}$ by Lemma 3.17 and the lemma is applicable). Then $\rho^{ss}|_G$ is abelian, and hence $\mathbb{I}$ has CM.

We give here an outline of the proof of converse and referring to the research article [H11] for details. Suppose that $\mathcal{F} = \mathcal{F}_{\mathbb{I}}$ has CM; so, it has complex multiplication by an imaginary quadratic extension $M/\mathbb{Q}$ in $\overline{\mathbb{Q}}$ as explained in §1.2. We then find a continuous character $\Psi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \widetilde{\mathbb{I}}^\times$ with $\rho_{\mathbb{I}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \Psi$ for the normalization $\widetilde{\mathbb{I}}$ of $\mathbb{I}$. By Galois deformation theory, we show that $\Psi_P = \Psi \mod P$ for the arithmetic P of weight k is associated to a Hecke character λ_P of conductor at most Np^∞ such that $\Psi_P(Frob_{\mathfrak{l}}) = \lambda_P(\mathfrak{l})$ for primes $\mathfrak{l} \nmid Np$ and $\lambda_P((\alpha)) = \zeta\alpha^k$ up to roots of unity $\zeta \in \mu_{mp^\infty}$ for a bounded m. 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 $\mathbb{Q}(\mu_{p^\infty})(f_P) \subset \mathbb{Q}(\alpha_{l,P})_{k(P)=k,l:\text{non-inert}} \subset \mathbb{Q}(\mu_{p^\infty h})[\alpha_j^{1/h} | j = 1,\dots,h]$ which is a finite extension of $\mathbb{Q}[\mu_{p^\infty}]$ containing $\mathcal{H}_k(\mathbb{I})$.

Now we prove, 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 3.14. Thus we can still apply the above proof and conclude that $\mathcal{F}$ has complex multiplication. □

Exercise 3.19. (1) *For a finite extension F of $\mathbb{Q}$, show that there are only finitely many root of unity in F.*
(2) *For a finite extension F of $\mathbb{Q}_p$, show that there are only finitely many root of unity in F.*

3.4. **Vertical Version.** Let $\mathcal{F} = \mathcal{F}_{\mathbb{I}}$ be a cuspidal p-adic analytic family of p-ordinary Hecke eigen cusp forms of slope 0. Let $\mathbb{Q}_{V,r}(\mathcal{F})$ be the subfield of $\overline{\mathbb{Q}}$ generated by $a(n, f_P)$ for all n and all arithmetic $P \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ with $r(P) \leq r$. In the early 1990s, L. Clozel asked the author if (or when) the Hecke field $\mathbb{Q}_{V,r}(\mathcal{F})$ for a finite r is a finite extension of $\mathbb{Q}$. At the time, for a scarcity of examples, my answer was "probably" that it is finite if and only if the family contains a CM

theta series (i.e., a binary theta series) of weight $k(P) \geq 2$. We make the following "vertical" conjecture.

Conjecture 3.20. *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 $\mathcal{V}_{\mathcal{A}}^{(l)}(\mathbb{I})$ for the field generated by $\{\alpha_{l,P}, \beta_{l,P}\}$ for all $P \in \mathcal{A}$, where P runs over all points in $\mathcal{A}$. We give an outline of a proof in [H11] of

Theorem 3.21 (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. *$\Sigma_{\alpha_0} = \left\{\sigma : \mathbb{Q}(\alpha_0) \hookrightarrow \overline{\mathbb{Q}} \middle| |i_p(\alpha_0^\sigma)| = 1\right\}$ 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.

3.5. **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 3.22. *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. *$\Sigma_{\alpha_0} = \left\{\sigma : \mathbb{Q}(\alpha_0) \hookrightarrow \overline{\mathbb{Q}} \middle| |i_p(\alpha_0^\sigma)| = 1\right\}$ 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 $a(p, f_P) = \zeta(\varepsilon_P(\gamma))^{\log_p(\alpha)/\log_p(\gamma)}\langle\alpha\rangle^{k(P)}$ 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. In this lecture, to simply the argument, we only deal with the case where $M := \mathcal{V}_{\mathcal{A}}(\mathbb{I})$ is an imaginary quadratic field and $r = 0$ (see [H11] Proposition 7.2 for the general case). 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 $\Phi_\alpha(T) \in W[[T]]$ 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 $(1 + T - \gamma^{k(P)})$. Thus we find $A \equiv \Phi_\alpha \mod P_j$ for infinitely many distinct primes P_j; so, $A = \Phi_\alpha$, as desired. □

3.6. **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 3.22 is met. By Proposition 3.22, we find a Weil number α of weight 1 and a power series $\Phi_\alpha(T) \in W[[T]]$ 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, $a(p) = \Phi_\alpha \in W[[T]] \subset \mathbb{I}$. 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 easier (in the same manner as in the proof of Theorem 3.1; see [H11] §4 for more details). This finishes the proof of Theorem 3.21.

We could make the following conjecture:

Conjecture 3.23. *Let $\mathcal{A} \subset \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ be an infinite set of arithmetic points P with bounded level $r(P) \le r$. Suppose that $\mathbb{I}$ does not have complex multiplication. Then we have*

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

4. Constancy theorem

The adjoint p-adic L-function $L_p(s, Ad(f_P))$ has an exceptional zero at $s = 1$ coming from modifying Euler p-factor. Greenberg proposed Galois cohomological definition of an $\mathcal{L}$-invariant $\mathcal{L}(Ad(f_P))$, and we have the following derivative formula I proved in [H04b]:

$$\mathcal{L}(Ad(f_P)) = -2\log_p(\gamma)a(p)^{-1}t\frac{ta(p)}{dt}|_{t=\gamma^{k(P)}\varepsilon_P(\gamma)}.$$

Thus $P \to \mathcal{L}(Ad(f_P))$ is interpolated over $\mathrm{Spec}(\mathbb{I})$ as an analytic function.

Theorem 4.1. *The function $P \to \mathcal{L}(Ad(f_P))$ is constant if and only if $\rho_{\mathbb{I}}$ has CM.*

Proof. For simplicity, assume $\mathbb{I} = W[[T]]$. Then, $a(p)^{-1}t\frac{da(p)}{dt} = s \in W$. Thus $t\frac{da}{dt} = s \cdot a$ for $a(t) = a(p)(t)$ for $s \in W$. 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 $\Phi(t) := t^s$, we find $\Phi(t^z) = \Phi(t)^z$ for $z \in \mathbb{Z}_p$. Thus by the rigidity lemma and its proof, we conclude $s \in \mathbb{Z}_p$ and that for any $\zeta \in \mu_{p^\infty}$, $a(p, f_\zeta) = \alpha$ for a Weil p-number α 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 first theorem, we conclude that $\mathcal{F}$ is a CM family.

Conversely, if $\mathcal{F}$ is a CM family associated to a Galois character $\Psi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \mathbb{I}^\times$, from $a(p) = \Psi^c(Frob_{\mathfrak{p}}) = t^{\log_p(\overline{\mathfrak{p}})/\log_p(\gamma)}$ up to a root of unity, we conclude the constancy of the $\mathcal{L}$-invariant. □

4.1. **Recall of $\mathcal{L}$-invariant.** According to Mazur–Tate–Teitelbaum [MTT86], the $\mathcal{L}$–invariant times the archimedean L-value would 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 exceptional zero at $s = 1$, and

this case the conjecture is first proven by Greenberg-Stevens [GS93] and by others later: For $L_p'(1,E)=\frac{dL_p(s,E)}{ds}|_{s=1}$, we have

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

and the explcit value of $\mathcal{L}^{an}(E)$ conjectured by [MTT86] and proved by Greenberg-Stevens [GS93] is, for the Tate period $q\in p\mathbb{Z}_p$,

$$\mathcal{L}^{an}(E)=\mathcal{L}(E)=\frac{\log_p(q)}{\mathrm{ord}_p(q)} \text{ writing } E(\overline{\mathbb{Q}}_p)=\overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}.$$

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:

$$\mathcal{L}^{an}(E)=-2\log_p(\gamma)\frac{da(p)}{dT}\Big|_{T=\varepsilon_P(\gamma)\gamma^{k(P)}}.$$

Here is an analogous formula in [H04b]:

Theorem 4.2. *Let p be an odd prime. Then we have*

$$\mathcal{L}(Ad(\rho_P))=-2\log_p(\gamma)a_P(p)^{-1}\frac{da(p)}{dT}\Big|_{T=\varepsilon_P(\gamma)\gamma^{k(P)}}.$$

4.2. **Galois deformation.** A main ingredient of the proof of Theorem 4.2 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 $\widehat{\mathbb{I}}_P\cong\kappa(P)[[X]]$ $(X=(1+T)-\varepsilon_P(\gamma)\gamma^{k(P)})$ (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 the following result (e.g., [HMI] Corollary 3.77) for "most" cases:

Theorem 4.3. *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.

4.3. **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, $N = 1$). 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. 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 $F^-Ad(V)/F^+Ad(V) \cong \kappa$; so, the p-adic L-function of $Ad(V)$ has an exceptional zero at $s = 1$. Put

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

Write simply $H^1(?) = H^1(\mathfrak{G}^S, ?)$. Then we define

$$\mathrm{Sel}(Ad(V)) = \mathrm{Ker}(H^1(Ad(V)) \to \frac{H^1(D_p, A)}{U_p(A)}). \tag{4.1}$$

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 $\mathrm{Sel}^-(Ad(V)) \supset \mathrm{Sel}(Ad(V))$.

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 4.4. *We have* $\dim \mathrm{Sel}^-(Ad(V)) = 1$ *and*

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

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, $\dim_\kappa \mathrm{Sel}(Ad(V)) = \dim_\kappa \mathrm{Sel}(Ad(V)^*(1))$; so, the desired vanishing also follows for the dual. □

We write S for the set of ramified primes for V including p. We have the Poitou-Tate exact sequence:

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

Thus by (V), we have

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

4.4. **Greenberg's $\mathcal{L}$–invariant.** Greenberg defined in [G94] 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 $\mathcal{L}(Ad(V)) \in \kappa$.

4.5. **Proof of Theorem 4.2.** 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 $\delta_P^{-1}\boldsymbol{\delta}([u,\mathbb{Q}_p]) = t^{\log_p(u)/2\log_p(\gamma)}$ by our construction. Then to get the desired result is just a simple computation.

References

Books

[BCM] N. Bourbaki, *Algébre Commutative*, Hermann, Paris, 1961–1998.

[GME] H. Hida, *Geometric Modular Forms and Elliptic Curves*, World Scientific, Singapore, 2000.

[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.

[MFM] T. Miyake, *Modular Forms*, Springer, New York-Tokyo, 1989.

Articles

[C03] 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`)

[C08] C.-L. Chai, A rigidity result for p–divisible formal groups, preprint, Asian J. Math. **12** (2008), 193?-202

[D69] P. Deligne, Formes modulaires et représentations l–adiques, Sém. Bourbaki, exp. 335, 1969

[G94] R. Greenberg, Trivial zeros of p–adic L–functions, Contemporary Math. **165** (1994), 149–174

[GV05] E. Ghate and V. Vatsal, On the local behaviour of ordinary $\mathbb{I}$-adic representations, Ann. Inst. Fourier (Grenoble) **54** (2004), 2143–2162 (2005)

[GS93] R. Greenberg and G. Stevens, p-adic L–functions and p–adic periods of modular forms, Inventiones Math. **111** (1993), 407–447

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

[H10a] H. Hida, The Iwasawa μ–invariant of p–adic Hecke L–functions, Ann. of Math. **172** (2010), 41–137

[H10b] H. Hida, Vanishing of the μ-invariant of p-adic Hecke L-functions, to appear in Compositio Math (a preprint version posted in `www.math.ucla.edu/~hida`)

[H10c] H. Hida, Constancy of adjoint $\mathcal{L}$-invariant, (a preprint version posted in `www.math.ucla.edu/~hida`)

[H10d] H. Hida, Image of Λ-adic Galois representations modulo p, preprint, 2010, 23 pages (a preprint version posted in `www.math.ucla.edu/~hida`)

[H11] H. Hida, Hecke fields of analytic families of modular forms, J. Amer. Math. Soc. **24** (2011), 51-80 (a preprint version posted in `www.math.ucla.edu/~hida`)

[K78a] N. M. Katz, p-adic L-functions for CM fields, Inventiones Math. **49** (1978), 199–297.

[K78b] N. M. Katz, Serre–Tate local moduli, In "Surfaces Algébriques," Lecture Notes in Math. **868** (1978), 138–202

[L74] J. H. Loxton, On two problems of R. M. Robinson about sum of roots of unity, Acta Arithmetica **26** (1974), 159–174.

[MTT86] 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

[MT90] B. Mazur and J. Tilouine, Représentations galoisiennes, différentielles de Kähler et "conjectures principales", Publication IHES **71** (1990), 65–103

[Ri85] K. A. Ribet, On l-adic representations attached to modular forms. II. Glasgow Math. J. **27** (1985), 185–194

[Ru91] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Inventiones Math. **103** (1991), 25–68

[Ru94] K. Rubin, More"main conjectures" for imaginary quadratic fields. Elliptic curves and related topics, 23–28, CRM Proc. Lecture Notes, **4**, Amer. Math. Soc., Providence, RI, 1994.

[Sc90] A. J. Scholl, Motives for modular forms, Inventiones Math. **100** (1990), 419–430.

[Sh58] G. Shimura, Correspondances modulaires et les fonctions ζ de courbes algébriques. J. Math. Soc. Japan **10** (1958) 1–28

[T89] J. Tilouine, Sur la conjecture principale anticyclotomique, Duke Math. J. **59** (1989), 629–673