CHARACTERIZATION OF ABELIAN COMPONENTS OF THE 'BIG' HECKE ALGEBRA

HARUZO HIDA

Fix an odd prime p, a positive integer N prime to p and field embeddings $\mathbb{C} \hookleftarrow \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Consider $S_{k+1}(\Gamma_0(Np^r),\psi)$ $(p \nmid N, r \geq 1)$. 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 $\mathbb{Z}$ is $H = \mathbb{Z}[\psi][T(n)|n = 1, 2, \cdots] \subset \mathrm{End}(S_{k+1}(\Gamma_0(Np^r),\psi))$. We put $H_{k+1,\psi} = H \otimes_{\mathbb{Z}[\psi]} \mathbb{Z}_p[\psi]$. Sometimes our $T(p)$ is written as $U(p)$ as the level is divisible by p. The ordinary part $h_{k+1,\psi} \subset H_{k+1,\psi}$ 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 $\mathbf{h} = \mathbf{h}_{\psi_1}$ such that

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

Each irreducible component $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbf{h})$ has a 2-dimensional Galois representation $\rho_{\mathbb{I}}$ (of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) with coefficients in $\mathbb{I}$ (or its quotient field) such that

$$\mathrm{Tr}(\rho_{\mathbb{I}}(Frob_l)) = a(l) \ \ \text{(for the image } a(l) \text{ in } \mathbb{I} \text{ of } T(l))$$

for almost all primes ℓ. If a prime divisor P of $\mathrm{Spec}(\mathbb{I})$ contains $(1 + T - \varepsilon\psi_k(\gamma)\gamma^k)$ with $k \geq 1$, we therefore have a Hecke eigenform $f_P \in S_{k+1}(\Gamma_0(Np^{r(P)}), \varepsilon\psi_k)$ such that its eigenvalue for $T(n)$ is given by $a_P(n) := (a(n) \mod P) \in \overline{\mathbb{Q}}_p$ for all n. Such a P is called arithmetic, and we write $\varepsilon_P = \varepsilon$ and $k(P) = k$ for such a P. Thus $\mathbb{I}$ gives rise to an analytic family $\mathcal{F}_{\mathbb{I}} = \{f_P | \text{arithemtic } P \in \mathrm{Spec}(\mathbb{I})\}$. 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. One expects to have a two variable p-adic L-function $L_p(s, \rho_{\mathbb{I}}^{\otimes n})$ for each symmetric power interpolating $L(s, f_P^{\otimes n})$. In particular, we have $L_p(s, Ad(\rho_{\mathbb{I}}))$. We have $L_p := L_p(1, Ad(\rho_{\mathbb{I}})) = L_p(1, \rho_{\mathbb{I}}^{\otimes 2} \otimes \det(\rho_{\mathbb{I}})^{-1}) \in \mathbb{I}$ and

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

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

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

Adding the cyclotomic variable, because of the modifying Euler p-factor, $L_p(s, Ad(\rho_{\mathbb{I}}))$ has an exceptional zero at $s = 1$, and for an $\mathcal{L}$-invariant $0 \neq \mathcal{L}(Ad(\rho_{\mathbb{I}})) \in \mathbb{I}$, we have $L_p'(s, Ad(\rho_{\mathbb{I}})) = \mathcal{L}(Ad(\rho_{\mathbb{I}}))L_p$.

Date: October 22, 2009.

A talk at BC-MIT Number Theory Seminar on October 20, 2009. The author is partially supported by the NSF grant: DMS 0753991 and DMS 0854949.

1. IS CHARACTERIZING ABELIAN COMPONENTS IMPORTANT?

Here is a list of such characterizations (possibly conjectural)

- $\mathbb{I}$ 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 $\Psi : G_M = \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \mathbb{I}^\times$ of conductor $\mathfrak{c}\mathfrak{p}^\infty$ for an ideal $\mathfrak{c}$ prime to p such that $\rho_{\mathbb{I}} = \mathrm{Ind}_M^{\mathbb{Q}} \Psi$. Thus sometimes, 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 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 $\Leftrightarrow$ $\rho_{\mathbb{I}}$ modulo an arithmetic prime is abelian.
- (Almost known) $\mathbb{I}$ 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 split factors).
- (Almost known) $\mathcal{L}(Ad(\rho_{\mathbb{I}}))$ is constant in $\overline{\mathbb{Q}}_p$ if and only if $\mathbb{I}$ is abelian.
- (?) $L_p(s, Ad(f_P))$ (for an arithmetic P) has exceptional zero at $s = 1$ and its $\mathcal{L}$-invariant $\mathcal{L}(Ad(f_P))$ (in the style of Mazur–Tate-Teitelbaum). 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 $(\mathfrak{p}/\overline{\mathfrak{p}})^h = (\alpha)$, $\log_p(\mathfrak{p}/\overline{\mathfrak{p}}) = \frac{1}{h}\log_p(\alpha)$.
- (Known under a mild condition) 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 $\le Np^r$ for a fixed $r \ge 0$. Then $\mathbb{I}$ is abelian $\Leftrightarrow$ $[\mathcal{V}_r(\mathbb{I}) : \mathbb{Q}] < \infty$. This was a conjectural statement of L. Clozel asked to me in the early 1990s.
- (A theorem to be discussed) Fix $k \ge 1$ 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 $\Leftrightarrow$ $[\mathcal{H}_k(\mathbb{I}) : \mathbb{Q}(\mu_{p^\infty})] < \infty$. The implication: $\Rightarrow$ is easy.

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

2. A THEOREM

Here is what we can prove:

Theorem 2.1. *Pick an infinite set $\mathcal{A}$ of arithmetic points P with fixed weight $k(P) = k \ge 1$. Write $\mathcal{H}_{\mathcal{A}}(\mathbb{I}) \subset \overline{\mathbb{Q}}$ for the field generated over $\mathbb{Q}(\mu_{p^\infty})$ by $\{a_P(p)\}_{P\in\mathcal{A}}$. 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.*

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 $K(f_P) = K[a_P(n); n = 1, 2, \dots] \subset \overline{\mathbb{Q}}$. We add a lemma:

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

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 $P \in \mathcal{A}$.

3. 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

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

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 3.1. *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.*

4. A key result

We start with a lemma of Chai:

Lemma 4.1. *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.

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 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 $\mathrm{Aut}(\widehat{\mathbb{G}}_m) = \mathbb{Z}_p^\times \supset \Gamma$, if σ is induced by $t \mapsto t^z$ ($z \in \Gamma$), $\Phi(t)^z - \Phi(t^z)$ has infinite common zeros in Ω. Thus $\Phi(t^z) = \Phi(t)^z$ for all $z \in \Gamma$. The graph Γ_Φ of $t \mapsto \Phi(t)$ in $\widehat{\mathbb{G}}_m \times \widehat{\mathbb{G}}_m$ is therefore stable under the diagonal action of $\mathbb{Z}_p^\times$. By a lemma of Chai, such a formal subscheme is a formal subtorus; so, $\Phi(t) = t^s$ for some $s \in \mathbb{Z}_p$ as desired. □

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

Proposition 4.2. *Suppose $[\mathcal{H}_{\mathcal{A}}(\mathbb{I}) : \mathbb{Q}(\mu_{p^\infty})] < \infty$. 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 $0 \leq n \in \mathbb{Z}$ 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 3.1, 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 4.1, 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. □

5. 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 5.1. *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.*

Proof. Suppose that ρ is absolutely irreducible over Q, and try to get absurdity. We have the identity $\mathrm{Tr}(\rho^\sigma) = \mathrm{Tr}(\rho^2) = \mathrm{Tr}(\rho^{\otimes 2}) - \det(\rho)$ for the symmetric second tensor representation $\rho^{\otimes 2}$ of ρ. Over Q, by absolute irreducibility, we have the identity of semi-simplification: $(\rho^{\otimes 2})^{ss} \cong \rho^\sigma \oplus \det(\rho)$. 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 2.1. 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 2.2, $[K(f_P) : K(a_P(p))] < d$ 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 4.2, 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 abelian. □

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