* Hecke fields and $\mathcal{L}$-invariant

Haruzo Hida
Department of Mathematics, UCLA,
Los Angeles, CA 90095-1555, U.S.A.

November 2010

*A talk at Kyushu university 11/29/2010.
The author is partially supported by the NSF grant: DMS 0753991 and DMS 0854949 and by Clay Mathematics institute as a senior scholar.

Each rational elliptic curve $E_{/\mathbb{Q}}$ is associated to a Hecke eigenform f_E of level $\Gamma_0(N)$ for a suitable positive integer N in the following way (Shimura/Taniyama conjecture):

- Look at $T_l E = \varprojlim_n E[l^n](\overline{\mathbb{Q}})$ (Tate module for a prime l), where $E[l^n](\overline{\mathbb{Q}}) = \{x \in E(\overline{\mathbb{Q}}) | l^n x = 0\}$;

- The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on it, and for the inertia group at another prime $p \neq l$,

$$T_l E^{I_p} = \{x \in T_l E | \sigma x = x \, \forall \sigma \in I_p\} \cong \begin{cases} 0 \\ \mathbb{Z}_l \\ \mathbb{Z}_l^2 \end{cases}$$

  depending on p with $\mathrm{rank}_{\mathbb{Z}_l} T_l E^{I_p} = 2$ for almost all p.

- The Frobenius element $Frob_p$ has its characteristic polynomial independent of l

$$\Phi_p(X) = \det(1 - Frob_p|_{T_l E^{I_p}} X) \in \mathbb{Z}[X].$$

- Make the H^1–part of Hasse–Weil L-function $L(s,E)$ by

$$L(s,E) = \prod_p \Phi_p(p^{-s})^{-1} = \sum_{n=1}^{\infty} a_n n^{-s}.$$

- Make a Fourier series convergent on $\mathfrak{H} = \{z \in \mathbb{C} | \operatorname{Im}(z) > 0\}$:

$$f(z) = \sum_{n=1}^{\infty} a_n \exp(2\pi i n z) \quad (\operatorname{Im}(z) > 0).$$

- Then $f(\frac{az+b}{cz+d}) = f(z)(cz+d)^2$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ with $N|c$ for a positive integer N called the level (weight 2 modular form).

This can be generalized to any system $\{\rho_{\mathfrak{l}} \circlearrowright V(\rho_{\mathfrak{l}}) \cong F_{\mathfrak{l}}^2\}_{\mathfrak{l}}$ of $\mathfrak{l}$-adic odd Galois representations, where $\mathfrak{l}$ runs over prime ideals of a number field F. Then

$$\prod_p \det(1-\rho_{\mathfrak{l}}(Frob_p)|_{V(\rho_{\mathfrak{l}})^{I_p}} p^{-s})^{-1} = \sum_{n=1}^{\infty} a_n(\rho) n^{-s}$$

gives rise to a modular form

$$f_\rho = \sum_{n=1}^{\infty} a_n(\rho) \exp(2\pi i n z)$$

which satisfies $f(\frac{az+b}{cz+d}) = \psi(d) f(z)(cz+d)^k$ as before for an integer $k > 0$ and a Dirichlet character ψ modulo the level N.

For a number field $K \subset \overline{\mathbb{Q}}$, the field

$$K(a_\rho(n)|n = 1, 2, \dots)$$

is called the Hecke field, which is one of the most **mysterious** series of number fields. One can simplify the question, fixing one prime p, and consider a simple extension $K(a_\rho(p))$ or for a family of systems of $\mathfrak{l}$-adic Galois representations $\mathcal{F} = \{\rho\}$, we could think of $K(a_\rho(p))_{\rho\in\mathcal{F}}$, and ask

how big this field is?

§1. Notation

To define the family $\mathcal{F}$ we study, we introduce some notation. Fix

- An odd prime $p > 2$;
- a positive integer N ($p \nmid N$);
- two field embeddings $\mathbb{C} \hookleftarrow \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

Consider the space of cusp form

$$S_{k+1,\psi} = S_{k+1}(\Gamma_0(Np^{r+1}), \psi) \quad (r \geq 0)$$

of weight "$k+1$" with Nebentypus ψ.

Let the rings

$$\mathbb{Z}[\psi] \subset \mathbb{C} \quad \text{and} \quad \mathbb{Z}_p[\psi] \subset \overline{\mathbb{Q}}_p$$

be generated by $\psi(n)$ ($n = 1, 2, \ldots$) over $\mathbb{Z}$ and $\mathbb{Z}_p$.

The Hecke algebra over $\mathbb{Z}$ is

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

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.

§2. Big Hecke algebra

The ordinary part $h^{ord}_{k+1,\psi} \subset h_{k+1,\psi}$ is the **maximal ring direct summand** on which $U(p)$ is invertible; so,

$$h^{ord} = e \cdot h \quad \text{for} \quad e = \lim_{n\to\infty} U(p)^{n!}.$$

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

- $\mathbf{h}$ is free of finite rank over $\mathbb{Z}_p[[T]]$ with $T(n) \in \mathbf{h}$ $(n = 1, 2, \ldots;\ T(p) = U(p))$
- Let $\gamma = 1 + p$. If $k \geq 1$ and $\varepsilon : \mathbb{Z}_p^\times \to \mu_{p^\infty}$ is a character,

$$\mathbf{h}/(1 + T - \psi(\gamma)\varepsilon(\gamma)\gamma^k)\mathbf{h} \cong h^{ord}_{k+1,\varepsilon\psi_k}$$

for $\psi_k := \psi_1\omega^{1-k}$, sending $T(n)$ to $T(n)$, where ω is the Teichmüller character.

§3. Galois representation

Each **irreducible component**

$$\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbf{h})$$

has a **Galois representation**

$$\rho_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(2)$$

with **coefficients** in $\mathbb{I}$ (or its quotient field) such that

$$\mathrm{Tr}(\rho_{\mathbb{I}}(Frob_l)) = a(l)$$

(for the image $a(l)$ in $\mathbb{I}$ of $T(l)$) for almost all primes ℓ. Usually $\rho_{\mathbb{I}}$ has values in $GL_2(\mathbb{I})$, and we suppose this for simplicity.

We regard $P \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ as an algebra homomorphism $P : \mathbb{I} \to \overline{\mathbb{Q}}_p$, and we put $\rho_P = P \circ \rho_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{Q}}_p)$.

§4. Analytic family

A point P of Spec$(\mathbb{I})(\overline{\mathbb{Q}}_p)$ is called

arithmetic

if $P(1+T-\varepsilon\psi_k(\gamma)\gamma^k)=0$ for $k \geq 1$ and $\varepsilon : \mathbb{Z}_p^\times \to \mu_{p^\infty}$.

If P is arithmetic, we have a Hecke eigenform $f_P \in S_{k+1}(\Gamma_0(Np^{r(P)}), \varepsilon\psi_k)$ such that

$$f_P|T(n) = a_P(n) f_P \quad (n = 1, 2, \dots)$$

for $a_P(n) := P(a(n)) = (a(n) \mod P) \in \overline{\mathbb{Q}}_p$.

We write $\varepsilon_P = \varepsilon$ and $k(P) = k$ for such a P.

Thus $\mathbb{I}$ gives rise to an **analytic family**

$$\mathcal{F}_{\mathbb{I}} = \{f_P | \text{arithemtic } P \in \text{Spec}(\mathbb{I})\}.$$

§5. CM component and CM family

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 $\rho_{\mathbb{I}}$ is CM.

If $\mathbb{I}$ is a CM component, it is known that for an imaginary quadratic field M in which p splits, there exists a Galois character $\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \mathbb{I}^{\times}$ such that $\rho_{\mathbb{I}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \varphi$.

If $\rho_P \cong \mathrm{Ind}_M^{\mathbb{Q}} \varphi_P$ for some arithmetic point P, $\mathbb{I}$ is a CM component.

§6. A theorem on Hecke fields

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 1 (H-theorem)**.** *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. Moreover*

$$\limsup_{P\in\mathcal{A}}[\mathbb{Q}(\mu_{p^\infty})(a_P(p)) : \mathbb{Q}(\mu_{p^\infty})] = \infty.$$

Assume that $[H_{\mathcal{A}}(\mathbb{I}) : \mathbb{Q}(\mu_{p^\infty})] < \infty$. We try to prove that $\mathbb{I}$ has CM. The converse is an easy application of **Galois deformation theory**.

§7. Number of eigenforms bounded

We start preparing to give a proof of the theorem. Put $K(f_P) = K[a_P(n); n = 1, 2, \ldots]$ inside $\overline{\mathbb{Q}}$.

Lemma 1 (Bounded degree)**.** *The degree*

$$[\mathbb{Q}(\mu_{p^\infty})(f_P) : \mathbb{Q}(\mu_{p^\infty})(a_P(p))]$$

for arithmetic P with fixed $k(P) \geq 1$ is **bounded** *(basically by* $\operatorname{rank}_{\mathbb{Z}_p[[T]]} \mathbf{h}$*) independently of P.*

For a prime l outside Np, let

$$A(l) = \text{a root of } \det(X - \rho_{\mathbb{I}}(Frob_l)) = 0.$$

Then $\alpha_{l,P} := P(A(l)) \in \overline{\mathbb{Q}}_p$ 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 lemma, if $[\mathbb{Q}(\mu_{p^\infty})(a_P(p)) : \mathbb{Q}(\mu_{p^\infty})] < B$ for B independent of $P \in \mathcal{A}$, $K_P = \mathbb{Q}(\mu_{p^\infty})(\alpha_{l,P})$ has **bounded degree** over $\mathbb{Q}(\mu_{p^\infty})$ independent of l and P for all $P \in \mathcal{A}$.

§8. Weil numbers

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 $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

The number of Weil l-numbers of a given weight k in $\mathbb{Q}(\mu_{p^\infty})$ is **finite** up to roots of unity, as we have only finitely many possibility of its prime factorization. Indeed, if l is either inert or ramified fully in $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$, weight k Weil l-number is (at most) $l^{k/2}$ up to roots of unity.

§9. Finiteness proposition

Two nonzero numbers a and b **equivalent** if a/b is a root of unity. Let $\mathcal{K}_d$ be the set of all extensions of $\mathbb{Q}[\mu_{p^\infty}]$ of **degree** $d < \infty$ inside $\overline{\mathbb{Q}}$ whose ramification at l is **tame**. Here is a slight improvement:

Proposition 1 (Finiteness Proposition)**.** *We have only* **finitely many** *Weil l-numbers of a given weight in the set-theoretic union* $\bigcup_{K \in \mathcal{K}_d} K$ **up to equivalence**.

The proof is an elementary but subtle analysis of prime decomposition of the Weil number. Tameness is assumed since in that case, there are only **finitely many** isomorphism classes of $K \otimes_{\mathbb{Q}} \mathbb{Q}_l$ for $K \in \mathcal{K}_d$, and one can consider the prime factorization in a fixed algebra $K \otimes_{\mathbb{Q}} \mathbb{Q}_l$ picking one isomorphism class.

§10. A rigidity lemma

Let W be a p-adic valuation ring finite flat over $\mathbb{Z}_p$ and $\Phi(T) \in W[[T]]$. Regard Φ as a function of $t = 1 + T$; so, $\Phi(1) = \Phi|_{T=0}$. We start with a lemma whose characteristic p version was studied by Chai:

Lemma 2 (Rigidity)**.** *Suppose that there is an infinite subset $\Omega \subset \mu_{p^\infty}(\overline{K})$ such that $\Phi(\Omega) \subset \mu_{p^\infty}$. Then there exist $\zeta_0 \in \mu_{p^\infty}$ and $s \in \mathbb{Z}_p$ such that $\zeta_0^{-1}\Phi(t) = t^s = \sum_{n=0}^{\infty} \binom{s}{n} T^n$.*

Note here that if

$$Z \subset \widehat{\mathbb{G}}_m \times \widehat{\mathbb{G}}_m = \mathrm{Spf}(W[t, \widehat{t^{-1}, t'}, t'^{-1}])$$

is a formal subtorus, it is defined by the equation $t = t'^s$ for $s \in \mathbb{Q}_p$. Thus we need to prove that the graph of the function $t \mapsto \Phi(t)$ in $\widehat{\mathbb{G}}_m \times \widehat{\mathbb{G}}_m$ is a **formal subtorus**. Fo simplicity, assume $\Phi(1) = 1$ (so $\zeta_0 = 1$) in the following proof.

§11. Proof of the rigidity lemma.

Step 1: Regard Φ as a morphism of formal schemes $\widehat{\mathbb{G}}_m \to \widehat{\mathbb{G}}_m$.

Step 2: For any σ in an open subgroup $1 + p^m\mathbb{Z}_p \subset \mathrm{Gal}(W[\mu_{p^\infty}]/W) \subset \mathbb{Z}_p^\times$, we have $\Phi(\zeta^z) = \Phi(\zeta^\sigma) = \sigma(\Phi(\zeta)) = \Phi(\zeta)^z$; so,

$$\Phi(t^z) = \Phi(t)^z$$

if $\zeta^\sigma = \zeta^z$ for the value $z \in 1 + p^m\mathbb{Z}_p$ of the **cyclotomic character** at σ.

Step 3: The graph Z of $t \mapsto \Phi(t)$ in $\widehat{\mathbb{G}}_m \times \widehat{\mathbb{G}}_m$ is therefore **stable** under $(t, t') \mapsto (t^z, t'^z)$ for $z = 1 + p^m\mathbb{Z}_p$.

Step 4: Pick a point $(t_0, t'_0 = \Phi(t_0))$ of infinite order in Z, then

$$(t_0^{1+p^m z}, {t'_0}^{1+p^m z}) = (t_0, t'_0)(t_0, t'_0)^{p^m z} \in Z$$

for all $z \in \mathbb{Z}_p$. Thus Z has to be a coset of a **formal subgroup** generated by $(t_0, t'_0)^{p^m}$. Since $(1, 1) \in Z$, Z is a formal torus, and we find $s \in \mathbb{Z}_p$ with $\Phi(t) = t^s$. $\square$

§12. Frobenius eigenvalues

Suppose $[H_{\mathcal{A}}(\mathbb{I}) : \mathbb{Q}(\mu_{p^\infty})] < \infty$. This implies $K_P = \mathbb{Q}(\mu_{p^\infty})(\alpha_{l,P})$ has bounded degree over $\mathbb{Q}(\mu_{p^\infty})$; so, for primes $l \gg 0$, l is **tamely** ramified in K_P (the tameness assumption in Finiteness Proposition).

Proposition 2 (Eigenvalue formula)**.** *There exists 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 $s = \frac{\log_p(\alpha_1)}{\log_p(\gamma)}$.

§13. Proof of eigenvalue formula

We give a sketch of a proof assuming $\mathbb{I} = W[[T]]$. By Finiteness proposition, we have only a **finite** number of Weil l-numbers of weight k in $\bigcup_{P \in \mathcal{A}} K_P$ 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 suitable variable change $T \mapsto Y = \gamma^{-k}(1+T) - 1$ and division by a Weil number, $A(Y)$ satisfies the assumption of the **rigidity lemma**. We have

$$A(Y) = \zeta\alpha(1+Y)^{s_1}$$

for $s_1 \in \mathbb{Z}_p$, and $A(T) = \zeta_0(1+T)^s$. From this, it is not difficult to determine s as stated in the proposition. $\square$

§14. Abelian image lemma

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 $s \in \mathbb{Z}_p$. 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.

Lemma 3 (Abelian image)**.** *Take a continuous representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to GL_2(A)$ 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 the **square map**: $\sigma \mapsto \rho^2(\sigma)$ is still a representation ρ^σ; so, it has to have an abelian image. Since any automorphism of the quotient field Q of $\mathbb{Z}_p[[T]]$ extends to its algebraic closure $\overline{Q} \supset \mathbb{I}$, we can apply the above lemma to $\rho_{\mathbb{I}}$.

§15. Proof of the theorem. Suppose $[H_{\mathcal{A}}(\mathbb{I}) : \mathbb{Q}(\mu_{p^\infty})] < \infty$.

Step 1: We have $[K_P : \mathbb{Q}(\mu_{p^\infty})]$ bounded independent of l; so, if $l \gg 0$, K_P is at most tamely ramified.

Step 2: By Eigenvalue formula, we have $\mathrm{Tr}(\rho(Frob_l)) = \zeta(1+T)^a + \zeta'(1+T)^{a'}$ for two roots of unity ζ, ζ' and $a, a' \in \mathbb{Q}_p$.

Step 3: Not too difficult to show that the order of ζ, ζ' is bounded independent of l.

Step 4: Let $\mathfrak{m}_N = \mathfrak{m}_{\mathbb{I}}^N + (T)$ and $\overline{\rho} = \rho_{\mathbb{I}} \bmod \mathfrak{m}_N$ for $N \gg 0$ and F be the splitting field of $\overline{\rho}$; so, taking $N \gg 0$, we may assume

$$\mathrm{Tr}(\rho(Frob_l^f)) = (1+T)^{fa} + (1+T)^{fa'}$$

for all $l \gg 0$ as long as $Frob_l^f \in \mathrm{Gal}(\overline{\mathbb{Q}}/F)$.

Step 5: This shows

$$\mathrm{Tr}(\sigma_s \circ \rho) = \mathrm{Tr}(\rho^s)$$

over $G = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$. Then by the above lemma, $\rho^{ss}|_G$ is abelian, and hence $\mathbb{I}$ is CM. $\square$

§16. p-Adic L-function

Recall of adjoint L-functions and $\mathcal{L}$-invariant to state an application.

We have one variable $L_p \in \mathbb{I}$ characterized by

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

and

$$L_p(P) := P(L_p) = \frac{L(1, Ad(f_P))}{\text{period}}$$

for all arithemtic P.

§17. Congruence criterion and $\mathcal{L}$-invariant

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

Spec$(\mathbb{I})\cap$Spec$(\mathbb{X})$ = Spec$(\mathbb{I}\otimes_{\mathbf{h}}\mathbb{X}) \cong$ Spec$(\frac{\mathbb{I}}{(L_p)})$

Adding the cyclotomic variable, because of the modifying Euler p-factor,

$L_p(s, Ad(\rho_{\mathbb{I}}))$ has **exceptional zero** at 1,

and for an analytic $\mathcal{L}$-**invariant** $0 \neq \mathcal{L}^{an}(Ad(\rho_{\mathbb{I}}))$

in $\mathbb{I}[\frac{1}{p}]$, we expect to have

$$L_p'(s, Ad(\rho_{\mathbb{I}}))|_{s=1} \stackrel{?}{=} \mathcal{L}^{an}(Ad(\rho_{\mathbb{I}}))L_p.$$

§18. An application

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 formula in IMRN **59** (2004) 3177–3189: for $c = -2\log_p(\gamma)$ and $a = a(p)$,

$$\mathcal{L}(Ad(f_P)) = c \cdot a^{-1} t \frac{da}{dt}\Big|_{t=\gamma^{k(P)}\varepsilon_P(\gamma)}.$$

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

Theorem 2 (Constancy)**.** $P \to \mathcal{L}(Ad(f_P))$ *is* **constant** *if and only if $\rho_{\mathbb{I}}$ has CM.*

By this, $P \mapsto \mathcal{L}(Ad(f_P))$ is non-constant for non CM component; so, **non-zero** except for finitely many P.

§19. Proof of the constancy theorem

For simplicity, assume $\mathbb{I} = W[[T]]$. Fix weight $k(P) \geq 1$. Suppose $\mathcal{L}(Ad(f_P))$ is constant.

Step 1: By assumption, $a^{-1}t\frac{da}{dt} = s \in W$ for $a(t) = a(p)(t)$. Thus $t\frac{da}{dt} = s \cdot a$.

Step 2: Putting $b(x) = \log_p \circ a(\exp_p(x))$ (for $x = \log_p(t)$), as $dx = \frac{dt}{t}$, by chain rule,

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

Step 3: b is a linear function of x:

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

Step 4:Taking $\Phi(t) := t^s$, we find $\Phi(t^z) = \Phi(t)^z$ for $z \in \mathbb{Z}_p$. By the rigidity lemma and its proof, we conclude $s \in \mathbb{Z}_p$.

Step 5: Thus $[H_{\mathcal{A}}(\mathbb{I}) : \mathbb{Q}(\mu_{p^\infty})] < \infty$. Then by the H-theorem, we conclude that $\mathcal{F}$ is a CM family. The converse is easy.