UCLA
UCLA Previously Published Works

Title
Greenberg's L-invariants of adjoint square Galois representations

Permalink
https://escholarship.org/uc/item/0814b8zj

Journal
International Mathematics Research Notices, 2004(59)

ISSN
1073-7928

Author
Hida, Haruzo

Publication Date
2004

Peer reviewed

eScholarship.org Powered by the California Digital Library
University of California

GREENBERG'S $\mathcal{L}$–INVARIANTS OF ADJOINT SQUARE GALOIS REPRESENTATIONS

HARUZO HIDA

Abstract. For a two-dimensional p-adic Galois representation V associated to a p–ordinary Hecke eigen cusp form f of weight $k \geq 2$, we identify the $\mathcal{L}$–invariant (of R. Greenberg) of the (three dimensional) adjoint square $Ad(V)$ of V with the derivative of the p–coefficient of the Λ–adic lift of f. By this result, for a given p-adic analytic family of ordinary Hecke eigenforms, the $\mathcal{L}$-invariant does not vanish for almost all members in the p-adic family (as expected).

1. Introduction

After the conjecture of Mazur-Tate-Teitelbaum, many number theorists have proposed diverse definitions of the $\mathcal{L}$–invariant which are expected to give the error term (or the difference) of the conjectural arithmetic part of the leading term of the Taylor expansion of a given p–adic motivic L–function at an exceptional zero from its archimedean counter-part. 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. Thus if E has *split* multiplicative reduction, $a_p = 1$, and $L_p(s,E)$ has zero at $s = 1$. This type of zero of a p–adic L–function resulted from the modification Euler p–factor is called an exceptional zero, and it is generally believed that if the archimedean L–values does not vanish, the order of the zero is the number e of such Euler p–factors; so, in this case, $e = 1$. Then $L_p'(1,E) = \frac{dL_p(s,E)}{ds}|_{s=1}$ is conjectured to be equal to the archimedean value $\frac{L_\infty(1,E)}{\text{period}}$ times an error factor $\mathcal{L}(E)$, the so-called $\mathcal{L}$–invariant:

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

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

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

The author is partially supported by the NSF grant: DMS 0244401.

Since E is modular, it is associated to an elliptic Hecke eigenform f_E of weight 2 with q–expansion $\sum_{n=1}^{\infty} a(n, f_E)q^n$. In particular, $a(p, f_E) = a_p = 1$ and $a(1, f_E) = 1$. We can lift f_E to a unique Λ–adic Hecke eigenform $\mathcal{F}$ for a finite flat extension Λ of $\mathbb{Z}_p[[x]]$ (étale around $x = 0$) so that f_E is a specialization of $\mathcal{F}$ at $x = 0$. Then one of the key ingredients of their proof is the following formula:

$$\mathcal{L}(E) = -2\log_p(\gamma)\frac{da(p, \mathcal{F})}{dx}\Big|_{x=0},$$

where γ is the generator of $\Gamma = 1 + p\mathbb{Z}_p$ corresponding to $1 + x$ under the identification: $\mathbb{Z}_p[[\Gamma]] = \mathbb{Z}_p[[x]]$.

Greenberg has generalized in [G] the conjectural formula of his $\mathcal{L}$–invariant to general V when V is p–ordinary. We write $\mathcal{L}(V)$ for the $\mathcal{L}$-invariant of Greenberg. Suppose that V is a modular ordinary two dimensional Galois representation associated to a p–ordinary elliptic Hecke eigenform f of weight $k \geq 2$ with "Neben" character having conductor prime to p. Thus V is a two dimensional Galois representation over a p–adic field K with integer ring W, and $a(p, f) \in W^{\times}$. Then for a suitable finite flat extension Λ of $W[[x]]$ isomorphic to the normalization of the irreducible component of the universal ordinary Hecke algebra carrying the Hecke eigenform f, we have a unique Λ–adic Hecke eigenform $\mathcal{F}$ lifting f so that its specialization at a point P_f of $\mathrm{Spf}(\Lambda)$ over (x) gives f (see [LFE] Theorem 7.3.3). Writing S for the set of primes ramifying for V including p and ∞, we write $\mathfrak{G}^S$ for the Galois group over $\mathbb{Q}$ of the maximal extension of $\mathbb{Q}$ unramified outside S. Then we have a Λ-adic ordinary Galois representation $\boldsymbol{\rho}^{ord}_{\mathcal{F}} : \mathfrak{G}^S \to GL_2(\Lambda)$ associated to $\mathcal{F}$ acting on $T_\Lambda = \Lambda^2$ (see [LFE] Theorem 7.5.1 and [MFG] 5.6.1). Assume $p > 2$. The Galois character $\det(\boldsymbol{\rho}^{ord}_{\mathcal{F}})^{-1}\det(\rho)$ has values in the p-profinite group $1 + \mathfrak{m}_\Lambda$ for the maximal ideal $\mathfrak{m}_\Lambda$ of Λ, and hence we have its unique square root ψ. Define a representation $\boldsymbol{\rho}_{\mathcal{F}} : \mathfrak{G}^S \to GL_2(\Lambda)$ with $\det(\boldsymbol{\rho}_{\mathcal{F}}) = \det(\rho)$ by $(\boldsymbol{\rho}^{ord}_{\mathcal{F}} \otimes \psi)(\sigma) = \psi(\sigma)\boldsymbol{\rho}^{ord}_{\mathcal{F}}(\sigma)$. Note that $\boldsymbol{\rho}_{\mathcal{F}} \equiv \boldsymbol{\rho}^{ord}_{\mathcal{F}} \mod P_f$.

We fix a W–lattice $T \subset V$ stable under the Galois action. The lattice T and $\boldsymbol{\rho}_{\mathcal{F}}$ is unique up to isomorphisms if $\overline{T} = T/\mathfrak{m}T$ is absolutely irreducible for the maximal ideal $\mathfrak{m}$ of W, and hence we may assume that $T_\Lambda/P_f T_\Lambda = T$ (a result of Carayol and Serre; e.g., [MFG] Proposition 2.13). Even if $\overline{T}$ is reducible, choosing a basis of T over W, the matrix representation $\rho_T : \mathfrak{G}^S \to GL_2(K)$ is isomorphic to $\rho := (\boldsymbol{\rho}_{\mathcal{F}} \mod P_f)$, because they are irreducible and have the same trace (e.g., [GME] Theorem 4.2.7). We find $\alpha_f \in GL_2(K)$ with $\alpha_f \rho_T \alpha_f^{-1} = \rho$ and $\alpha_f(T_\Lambda/P_f T_\Lambda) = T$. Taking $\alpha_\Lambda \in GL_2(\Lambda_{P_f})$ with $\alpha_\Lambda \mod P_f = \alpha_f$ and replacing T_Λ by $\alpha_\Lambda T_\Lambda$, we assume that $\rho = (\boldsymbol{\rho}_{\mathcal{F}} \mod P_f) = \rho_T$. Then we consider the deformation functor into sets from the category of local profinite W–algebras with residue field $W/\mathfrak{m}$ whose value at a local W–algebra A is given by the set of isomorphism classes of rank two free A–modules $\widetilde{T}$ with continuous $\mathfrak{G}^S$–action satisfying the following three properties:

(D1) $\widetilde{T}/\mathfrak{m}_A\widetilde{T} \cong \overline{T}$ as $\mathfrak{G}^S$–modules for $\overline{T} = T/\mathfrak{m}T$;

(D2) Writing $\iota : W \to A$ for the structure homomorphism of W–algebras, we have the identity of the determinant characters:

$$\iota \circ \det(\rho) = \det \widetilde{T};$$

(D3) Fix a decomposition group D_p of p in $\mathfrak{G}$. Then we have an exact sequence $0 \to F^+\widetilde{T} \to \widetilde{T} \to \widetilde{T}/F^+\widetilde{T} \to 0$ stable under D_p such that $\widetilde{T}/F^+\widetilde{T}$ is free of rank one over A and that $F^+\widetilde{T}/\mathfrak{m}_A F^+\widetilde{T} \cong F^+\overline{T}$ as D_p-modules.

The condition (D3) is the near ordinarity, and we call the character of D_p giving the action on $\widetilde{T}/F^+\widetilde{T}$ the *nearly ordinary character* of $\widetilde{T}$. A deformation $\widetilde{T}$ is ordinary if the nearly ordinary character of $\widetilde{T}$ is unramified. This functor may not be prorepresentable but almost always has a minimal versal hull R (unique up to non-canonical isomorphisms) with a versal deformation $\boldsymbol{\rho} : \mathfrak{G}^S \to GL_2(R)$ of $\overline{T}$. The nearly ordinary character $\boldsymbol{\delta}$ of $\boldsymbol{\rho}$ gives rise to a character of the inertia group I_p into $R^\times$. By local class field theory, the abelianization I_p^{ab} is canonically isomorphic to $\mathbb{Z}_p^\times$, and through this character $\boldsymbol{\delta}$, we endow R with an algebra structure over the Iwasawa algebra $W[[x]]$ (sending x to $\gamma - 1$). It is known that $\boldsymbol{\rho}_{\mathcal{F}}$ satisfies (D1-3) (e.g., [GME] Theorem 4.2.7 (2)), and the algebra structure over $W[[x]]$ of Λ is given in the same way by the nearly ordinary character $\boldsymbol{\delta}_{\mathcal{F}}$ of $\boldsymbol{\rho}_{\mathcal{F}}$.

We assume the existence of the minimal versal hull. Since $\boldsymbol{\rho}_{\mathcal{F}}$ satisfies (D1-3), we have a morphism $\pi : Spec(\Lambda) \to Spec(R)$ such that $\pi^*\boldsymbol{\rho} \cong \boldsymbol{\rho}_{\mathcal{F}}$. Since the action of D_p on F^+T ramifies (because of $k \geq 2$), we have $\pi \circ \boldsymbol{\delta} = \boldsymbol{\delta}_{\mathcal{F}}$. The Galois module T gives rise to a W-point $P = P_T$ of $Spec(R)$ such that $\pi(P_f) = P_T$ and $(\boldsymbol{\rho} \mod P_T) \cong \rho \cong (\boldsymbol{\rho}_{\mathcal{F}} \mod P_f)$. Since $\pi \circ \boldsymbol{\delta} = \boldsymbol{\delta}_{\mathcal{F}}$, we have $P_f \cap W[[x]] = (x)$. We prove

Theorem 1.1. *Let p be an odd prime, and assume that f has weight $k \geq 2$ and that the "Neben" character of f has conductor prime to p. Suppose that the versal nearly p–ordinary deformation ring R, after localization and completion at $P = P_T$, is isomorphic under π to the local completed ring Λ_{P_f} of Λ at P_f. Then we have*

$$\mathcal{L}(Ad(V)) = -2\log_p(\gamma)a(p,f)^{-1}\frac{da(p,\mathcal{F})}{dx}\Big|_{x=0}.$$

We write $\overline{\varepsilon}$ (resp. $\overline{\delta}$) for the character of D_p with values in $\mathbb{F} = W/\mathfrak{m}$ given by $F^+\overline{T}$ (resp. $\overline{T}/F^+\overline{T}$). The assumption of the theorem has been verified by Wiles and other mathematicians working in Galois deformation theory (see [W], [SW], [SW1] and [BCDT]), for example, if the following three conditions are satisfied:

1. $p > 2$;
2. $\overline{\varepsilon} \neq \overline{\delta}$ (the p–distinguishedness condition);
3. The cusp form f has square free prime-to–p level N and $\rho \mod \mathfrak{m}$ ramifies at each prime factor of N.

The above three conditions are listed for the reader's convenience, and as long as the condition (2) (which implies the existence of the minimal versal hull R) is satisfied, the assumption of the theorem is verified in almost all cases.

The above theorem combined with Theorem 6.3 (4) and Proposition 7.1 of [H00] (or Theorem 5.51 of [MFG]) confirms, for many modular adjoint square Galois representations, the conjectures of Greenberg (see [G]) predicting the non-vanishing of $\mathcal{L}(Ad(V))$. Indeed, in Proposition 7.1 of [H00], the derivative $\frac{da(p,\mathcal{F})}{dx}$ (possibly in the quotient field of Λ) before specializing at $x = 0$ is proven to be nonzero, and hence, it vanishes only at finitely many (unspecified) points in $\mathrm{Spf}(\Lambda)(W)$. Thus in the infinite family of Hecke eigenforms obtained as specializations of the Λ-adic form $\mathcal{F}$, the Hecke eigenforms have nonzero $\mathcal{L}$-invariant except for finitely many members of the family.

In our subsequent paper, we hope to prove a similar result also in the Hilbert modular case, which certainly involves more technicality. The author wishes to thank the referee of this paper for pointing him out a missing factor from an earlier version of the formula of $\mathcal{L}(Ad(V))$.

In the following sections, we shall start with a brief review of the definition by Greenberg of the Selmer group and the $\mathcal{L}$–invariant of the adjoint square of a two dimensional modular ordinary p–adic Galois representation. After the review, we shall give a proof of the theorem. Hereafter we suppose that $p > 2$.

2. Selmer Groups

We shall describe the definition due to Greenberg of his Selmer group associated to the adjoint square Galois representation. Let K be a finite extension of $\mathbb{Q}_p$ with p-adic integer ring W. Let $M/\mathbb{Q}$ be a subfield of $\overline{\mathbb{Q}}$. All Galois cohomology groups with coefficients in a finite Galois module are continuous cohomology groups as defined in [MFG] 4.3.3. We write $\mathfrak{p}$ for a prime of M over p and $\mathfrak{q}$ for general primes of M. Write $D_{\mathfrak{q}}$ for the decomposition group at $\mathfrak{q}$ in $\mathfrak{G}_M = \mathrm{Gal}(\overline{\mathbb{Q}}/M)$ and $I_{\mathfrak{q}}$ for the inertia subgroup of $D_{\mathfrak{q}}$. For a general K-vector space V with a continuous action of $\mathfrak{G} = \mathfrak{G}_{\mathbb{Q}}$ and a $\mathfrak{G}$-stable W-lattice T of V, we define $H^q(X,T) = \varprojlim_n H^q(X, T/p^nT)$, $H^q(X, V/T) = \varinjlim_n H^q(X, p^{-n}T/T)$ and $H^q(X, V) = H^q(X, T) \otimes_W K$ for $X = M$ and $M_{\mathfrak{q}}$. Here $H^q(M, ?) = H^q(\mathfrak{G}_M, ?)$ and $H^q(M_{\mathfrak{q}}, ?) = H^q(D_{\mathfrak{q}}, ?)$.

Assume now V to be a two dimensional vector space over K with a continuous action of $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ associated to a Hecke eigen cusp form f whose "Neben" character has conductor prime to p. Thus the Galois action is unramified at almost all primes. We let $\mathfrak{G}$ act on $\mathrm{End}_K(V)$ by conjugation and define $Ad(V) \subset \mathrm{End}_K(V)$ by the trace 0 subspace of dimension 3.

We assume given a filtration as in (D3):

$$\text{(ord)} \qquad V \supsetneq F^+V \supsetneq \{0\}$$

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

$$Ad(V) \supset F^-Ad(V) \supset F^+Ad(V) \supset \{0\}, \tag{2.1}$$

where

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

If we take a basis of V containing a generator of F^+V and we identify $\mathrm{End}_K(V)$ with $M_2(K)$ by this basis, $F^-Ad(V)$ (resp. $F^+Ad(V)$) is made up of upper triangular matrices with trace zero (resp. upper nilpotent matrices). Note that D_p acts trivially on $F^-Ad(V)/F^+Ad(V)$; so, $F^-Ad(V)/F^+Ad(V) \cong K$ as D_p-modules. In particular, the p-adic L-function of $Ad(V)$ has an exceptional zero at $s = 1$.

We denote by $\chi : \mathfrak{G} \to \mathbb{Z}_p^\times$ the cyclotomic character given by $\zeta^\sigma = \zeta^{\chi(\sigma)}$ for all $\zeta \in \mu_{p^\infty}$. Taking the dual $Ad(V)^*(1) = \mathrm{Hom}_K(Ad(V), K) \otimes \chi \cong Ad(V)(1)$, we define subspaces $F^-Ad(V)^*(1) = F^+Ad(V)^\perp(1) = F^-Ad(V)(1)$ and $F^+Ad(V)^*(1) = F^-Ad(V)^\perp(1) = F^+Ad(V)(1)$. Thus we have

$$Ad(V)^*(1) \supset F^-Ad(V)^*(1) \supset F^+Ad(V)^*(1) \supset \{0\}. \tag{2.2}$$

On $\frac{F^-Ad(V)^*(1)}{F^+Ad(V)^*(1)}$, D_p acts by χ, using the conventional notation, $\frac{F^-Ad(V)^*(1)}{F^+Ad(V)^*(1)} \cong K(1)$.

We define $Ad(T) = \mathrm{End}_W(T) \cap Ad(V)$ and $Ad(T)^*(1) = \mathrm{Hom}(Ad(T), W) \otimes \chi \subset Ad(V)^*(1)$. Taking intersection with $Ad(T)$ and $Ad(T)^*(1)$, we have three step filtrations of $Ad(T)$ and $Ad(T)^*(1)$ induced from the above filtrations. We put $Ad(V/T)^*(1) = Ad(V)^*(1)/Ad(T)^*(1)$.

For each prime $\mathfrak{q}$ of M, we put

$$U_{\mathfrak{q}}(Ad(V)) = \begin{cases} \mathrm{Ker}(\mathrm{Res} : H^1(M_{\mathfrak{q}}, Ad(V)) \to H^1(I_{\mathfrak{q}}, Ad(V))) & \text{if } \mathfrak{q} \nmid p, \\ \mathrm{Ker}(\mathrm{Res} : H^1(M_{\mathfrak{q}}, Ad(V)) \to H^1(I_{\mathfrak{q}}, \frac{Ad(V)}{F^+(Ad(V))})) & \text{if } \mathfrak{q} = \mathfrak{p}|p. \end{cases}$$

For $Ad(V/T) := Ad(V)/Ad(T)$, we define $U_{\mathfrak{q}}(Ad(V/T))$ by the image of $U_{\mathfrak{q}}(Ad(V))$ in the cohomology group $H^1(M_{\mathfrak{q}}, Ad(V/T))$. Then we define for $A = Ad(V)$ and $Ad(V/T)$

$$\mathrm{Sel}_M(A) = \mathrm{Ker}(H^1(M, A) \to \prod_{\mathfrak{q}} \frac{H^1(M_{\mathfrak{q}}, A)}{U_{\mathfrak{q}}(A)}). \tag{2.3}$$

The classical Selmer group of $Ad(V)$ is given by $\mathrm{Sel}_M(Ad(V/T))$ equipped with the discrete topology (which is denoted by $\mathrm{Sel}(Ad(T))_{/M}$ in [MFG] 5.2.1). Here we use the slightly different notation $\mathrm{Sel}_M(A)$, because A can be $Ad(V/T)$ and also $Ad(V)$. Write $\mathbb{Q}_\infty$ for the cyclotomic $\mathbb{Z}_p$–extension of $\mathbb{Q}$. The Selmer group $\mathrm{Sel}_{\mathbb{Q}_\infty}(Ad(V/T))$ is an Iwasawa module of co-finite type. Replacing $U_{\mathfrak{p}}(Ad(V))$ by the bigger

$$U^-_{\mathfrak{p}}(Ad(V)) = \mathrm{Ker}(\mathrm{Res} : H^1(M_{\mathfrak{q}}, Ad(V)) \to H^1(I_{\mathfrak{q}}, \frac{Ad(V)}{F^-(Ad(V))}))$$

for $\mathfrak{p}|p$ (and keeping $U_{\mathfrak{q}}(Ad(V))$ intact for $\mathfrak{q} \nmid p$), we can define a bigger "$-$" Selmer group $\mathrm{Sel}^-_M(A) \supset \mathrm{Sel}_M(A)$.

We also need balanced Selmer groups $\overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V))$ and $\overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V)^*(1))$ introduced in [G] (16) under the notation of $S_A(\mathbb{Q})$. We call this Selmer group balanced since $\overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V))$ and the dual $\overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V)^*(1))$ have equal dimensions (cf., [G] Proposition 2). We define $\overline{\mathrm{Sel}}_{\mathbb{Q}}(A)$ for $A = Ad(V)$ and $Ad(V/T)$ by slightly shrinking $U_p(Ad(V))$ to $\overline{U}_p(Ad(V)) \subset U_p(Ad(V))$ and keeping $U_q(Ad(V)) = \overline{U}_q(Ad(V))$ for $q \neq p$ intact. Then we define $\overline{U}_q(Ad(V)^*(1))$ by the orthogonal complement $U_q(Ad(V))^\perp$ under the Tate pairing for all q including p. Then $\overline{U}_q(Ad(V/T))$ and $\overline{U}_q(Ad(V/T)^*(1))$ are defined by the image of $\overline{U}_q(Ad(V))$ and $\overline{U}_q(Ad(V)^*(1))$ in $H^1(\mathbb{Q}_q, Ad(V/T))$ and $H^1(\mathbb{Q}_q, Ad(V/T)^*(1))$, respectively. The new Selmer group is defined by the same formula as in (2.3):

$$\overline{\mathrm{Sel}}_{\mathbb{Q}}(A) = \mathrm{Ker}(H^1(\mathbb{Q}, A) \to \prod_q \frac{H^1(\mathbb{Q}_q, A)}{\overline{U}_q(A)}) \tag{2.4}$$

for $A = Ad(V)$, $Ad(V/T)$, $Ad(V)^*(1)$ and $Ad(V/T)^*(1)$. Actually, the new Selmer group $\overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V))$ often coincides with our Selmer group defined by (2.3). Indeed, unless f is multiplicative at p, we simply set $\overline{U}_q(Ad(V)) = U_q(Ad(V))$ for all q; thus, $\overline{\mathrm{Sel}}_{\mathbb{Q}}(A) = \mathrm{Sel}_{\mathbb{Q}}(A)$ for $A = Ad(V)$ and $Ad(V/T)$ in this case. Here we call f *multiplicative* at p if f is of weight 2 and is associated to an abelian variety with multiplicative reduction at p (not necessarily split). Thus we only need to define $\overline{U}_p(Ad(V))$ if f is multiplicative. In this case, we simply put $\overline{U}_p(Ad(V)) = F^+H^1(\mathbb{Q}_p, Ad(V)) \subset U_p(Ad(V))$, which is the image of $H^1(\mathbb{Q}_p, F^+Ad(V))$ in $H^1(\mathbb{Q}_p, Ad(V))$.

The above definition coincides with the one given in [G], because as we already remarked, $F^+Ad(V)^*(1)$ (resp. $\frac{F^-Ad(V)}{F^+Ad(V)}$) is the smallest (resp. the largest) subspace of $F^-Ad(V)^*(1)$ (resp. $\frac{Ad(V)}{F^+Ad(V))}$) stable under D_p so that D_p acts on it by χ (resp. by the trivial character); so, $\frac{F^-Ad(V)^*(1)}{F^+Ad(V)^*(1)} \cong K(1)$ and $\frac{F^-Ad(V)}{F^+Ad(V)} \cong K$. Therefore the space $F^+Ad(V)^*(1)$ (resp. $F^-Ad(V)$) is the subspace written as $F^{11}Ad(V)^*(1)$ (resp. $F^{00}Ad(V)$) in [G].

We now verify the following condition in [G] necessary to define $\mathcal{L}(Ad(V))$:

Lemma 2.1. *Suppose that f satisfies the assumptions of* Theorem 1.1. *Then we have* $\mathrm{Sel}_{\mathbb{Q}}(Ad(V)) = 0$ *and*

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

Proof. Using the global Tate duality (e.g., [MFG] Theorem 4.50), Greenberg ([G] Proposition 2) has shown $\dim_K \overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V)) = \dim_K \overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V)^*(1))$. Since the Selmer group $\mathrm{Sel}_{\mathbb{Q}}(Ad(V/T))$ contains $\overline{\mathrm{Sel}}_{\mathbb{Q}}(V/T)$, we have

$$|\mathrm{Sel}_{\mathbb{Q}}(Ad(V/T))| < \infty \ (\Rightarrow |\overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V/T))| < \infty). \tag{V1}$$

If the deformation problem (D1-3) is representable and the universal ring R is isomorphic to an appropriate Hecke algebra, $R_k = R/PR$ for $P = P_f \cap W[[\Gamma]]$ is isomorphic to a suitable Hecke algebra of weight k and of finite level (possibly a multiple of N) by the control theorem of the universal ordinary Hecke algebra (cf., [MFG] Theorem 5.28, [H86] and [H88] Theorem II). Thus $R_k = R/PR$ is a W-module of finite type and its W-free quotient is reduced. Then by a standard argument (e.g., [MFG] Theorem 5.14), the Pontryagin dual of $\mathrm{Sel}_{\mathbb{Q}}(Ad(V/T))$ is isomorphic to the finite module $\Omega_{R_k/W} \otimes_{R_k} W$, where the tensor product is taken with respect to the algebra homomorphism $R_k \to W$ associated to ρ. This shows (V1) and the vanishing of $\mathrm{Sel}_{\mathbb{Q}}(Ad(V))$.

Now suppose that we are in the worst case where R only has a surjection onto a local ring of an appropriate Hecke algebra finite torsion-free over $W[[\Gamma]]$. Since Λ_{P_f} is generated by the trace of the Galois representation $\boldsymbol{\rho}_{\mathcal{F}}$ (the local étaleness of the Hecke algebra around $x = 0$), the assumed identity $\Lambda_{P_f} \cong R_{P_T}$ in the theorem tells us that $\boldsymbol{\rho} : \mathfrak{G} \to GL_2(R_{P_T})$ is universal among all continuous deformations over K of ρ into $GL_2(A)$ satisfying (P1-3) in Section 4. Here A runs over Artinian local K-algebras with residue field K (for a sketch of a proof of this fact, see the argument in Section 4 after (P1-3)). Since $R_k := R_{P_T}/P_T R_{P_T} \cong \Lambda_{P_f}/P_f\Lambda_{P_f} = K$ and $\Lambda_{P_f} = W[[\Gamma]]_{(x)}$, again the K-dual of $\mathrm{Sel}_{\mathbb{Q}}(Ad(V))$ is isomorphic to $\Omega_{R_k/K} \otimes_{R_k} K = \Omega_{K/K} = 0$. As already remarked, $\mathrm{Sel}_{\mathbb{Q}}(Ad(V)) = 0$ implies $\overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V)) = 0$, which in turn implies $\overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V)^*(1)) = 0$ by [G] Proposition 2. This finishes the proof. □

We write S for the set of ramified primes for V including p. We have the Poitou-Tate exact sequence (e.g., [MFG] Theorem 4.50 (5)):

$$0 \to \overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V)) \to H^1(\mathfrak{G}^S, Ad(V)) \to \prod_{q \in S} \frac{H^1(\mathbb{Q}_q, Ad(V))}{\overline{U}_q(Ad(V))} \to \overline{\mathrm{Sel}}_{\mathbb{Q}}(Ad(V)^*(1))^*,$$

where $\mathfrak{G}^S$ is the absolute Galois group of the maximal extension unramified outside $S \cup \{\infty\}$. Thus by (V), we have

$$H^1(\mathfrak{G}^S, Ad(V)) \cong \prod_{q \in S} \frac{H^1(\mathbb{Q}_q, Ad(V))}{\overline{U}_q(Ad(V))}. \tag{2.5}$$

3. Greenberg's $\mathcal{L}$–invariant

Greenberg defined in [G] his invariant $\mathcal{L}(Ad(V))$ in the following way. By the definition of $\overline{U}_p(Ad(V))$, the subspace $F^-H^1(\mathbb{Q}_p, Ad(V))/\overline{U}_p(Ad(V))$ inside the right-hand side of (2.5) is isomorphic to $F^-Ad(V)/F^+Ad(V) \cong K$ (see just below (21) in Section 2 of [G]). By (2.5), we have a unique subspace $\mathbb{T}$ of $H^1(\mathfrak{G}^S, Ad(V))$ projecting down isomorphically onto

$$\frac{F^-H^1(\mathbb{Q}_p, Ad(V))}{\overline{U}_p(Ad(V))} \hookrightarrow \prod_{q \in S} \frac{H^1(\mathbb{Q}_q, Ad(V))}{\overline{U}_q(Ad(V))}.$$

Then by the restriction, $\mathbb{T}$ gives rise to a subspace L of

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

isomorphic to $F^-Ad(V)/F^+Ad(V) \cong K$. Note that

$$\mathrm{Hom}(D_p^{ab}, \frac{F^-Ad(V)}{F^+Ad(V)}) \cong \left(\frac{F^-Ad(V)}{F^+Ad(V)}\right)^2 \cong K^2$$

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

$$\mathcal{L} : F^-Ad(V)/F^+Ad(V) \to F^-Ad(V)/F^+Ad(V),$$

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

The cocycle c as above becomes unramified at p after restriction to $\mathfrak{G}_{\mathbb{Q}_\infty}$ (because the p–ramification of c is consumed by $\mathbb{Q}_\infty/\mathbb{Q}$), it gives rise to an element c_∞ in $\mathrm{Sel}_{\mathbb{Q}_\infty}(Ad(V))$. The map $c \mapsto c_\infty$ is injective (under the triviality of $H^0(\mathfrak{G}_{\mathbb{Q}_\infty}, Ad(V))$) by the inflation-restriction sequence. Thus the image $\mathbb{T}_\infty \subset \mathrm{Sel}_{\mathbb{Q}_\infty}(Ad(V))$ gives rise to a zero of the characteristic power series of $\mathrm{Sel}_{\mathbb{Q}_\infty}(Ad(V/T))$ at the augmentation ideal of $W[[\Gamma]]$ (see [G] Proposition 1).

4. Proof of the theorem

We take a p–ordinary Hecke eigenform f of weight $k \geq 2$ as in the theorem and its two dimensional Galois representation V. We take a matrix form $\rho : \mathfrak{G} \to M_2(W)$ of the Galois representation T so that its restriction to D_p is given by $\rho(\sigma) = \begin{pmatrix} \epsilon(\sigma) & \beta(\sigma) \\ 0 & \delta(\sigma) \end{pmatrix}$. We now identify $Ad(T)$ with the following subspace of $M_2(W)$:

$$\left\{\xi \in M_2(W) = \mathrm{End}_W(T) \middle| \mathrm{Tr}(\xi) = 0\right\}.$$

Then $F^-Ad(T)$ is the subspace of $Ad(T)$ made up of upper triangular matrices, and $F^+Ad(T)$ is made up of upper nilpotent matrices on which D_p acts by the character $\epsilon\delta^{-1}$.

Recall the versal nearly ordinary deformation $\boldsymbol{\rho} : \mathfrak{G}^S \to GL_2(R)$ with $\det(\boldsymbol{\rho}) = \det(\rho)$ and the point $P = P_T \in \mathrm{Spf}(R)(W)$ carrying ρ. Recall the subspace $\mathbb{T}$ of $H^1(\mathfrak{G}^S, Ad(V))$ studied in the previous section. We know

1. $\dim_K \mathbb{T} = 1$,
2. $\mathbb{T}$ is made up of the classes of cocycles c which is upper triangular on D_p and unramified at the ℓ–inertia group for $\ell \in S$ different from p,
3. $\mathrm{Sel}_{\mathbb{Q}}(Ad(V)) = \{0\}$ (Lemma 2.1).

By (2), $\mathbb{T} \subset \mathrm{Sel}^-_{\mathbb{Q}}(Ad(V))$ which is defined just below (2.3). By (2.5), $\mathrm{Sel}^-_{\mathbb{Q}}(Ad(V)) = \mathbb{T} \oplus \mathrm{Sel}_{\mathbb{Q}}(Ad(V)) = \mathbb{T}$, because the image of $\mathbb{T}$ in $H^1(\mathbb{Q}_p, Ad(V))/U_p(Ad(V))$ is given by $U_p^-(Ad(V))/U_p(Ad(V))$. This fact can be also seen from [H00] Corollary 5.4 if we further assume that R is isomorphic to a local ring of the universal ordinary Hecke algebra.

First suppose that the deformation functor Φ of $\overline{T}$ defined by (D1-3) is representable by R. Then by Theorem 5.14 of [MFG], the K-dual $\mathrm{Sel}^-_{\mathbb{Q}}(Ad(V))^*$ of $\mathrm{Sel}^-_{\mathbb{Q}}(Ad(V))$ is canonically isomorphic to $\Omega^1_{R/W} \otimes_R R_P/PR_P$ where $P = P_T$ is the point of $\mathrm{Spf}(R)$ corresponding to ρ and R_P is the localization completion of R at P (so $R_P/PR_P = K$). Here $\Omega^1_{R/W}$ is the module of continuous differentials of R over W under the profinite topology of R. Thus $\mathbb{T} = \mathrm{Sel}^-_{\mathbb{Q}}(Ad(V))$ is isomorphic to the tangent space at P of R_P.

We now suppose the weaker assumption: $R_P = \Lambda_{P_f}$. Then as already remarked, R_P is topologically generated by trace of $\boldsymbol{\rho}_{\mathcal{F}}$, and hence $(R_P, \boldsymbol{\rho} : \mathfrak{G}^S \to GL_2(R_P))$ is the universal couple pro-representing the following localized functor Φ_P (see [HT] Section 2 for a general discussion of the "localized" deformation theory). The functor Φ_P associates to each local Artinian K-algebra A with residue field K the set of isomorphism classes of p-adically continuous defomations $\widetilde{\rho} : \mathfrak{G}^S \to GL_2(A)$ satisfying the following three conditions:

(P1) $\widetilde{\rho} \mod \mathfrak{m}_A \cong \rho$ for the maximal ideal $\mathfrak{m}_A$ of A;

(P2) Writing $\iota : K \to A$ for the structure homomorphism of K–algebras, we have the identity of the determinant characters:

$$\iota \circ \det(\rho) = \det \widetilde{\rho};$$

(P3) $\widetilde{\rho}|_{D_p} \cong \begin{pmatrix} \widetilde{\epsilon} & * \\ 0 & \widetilde{\delta} \end{pmatrix}$ with $\widetilde{\delta} \mod \mathfrak{m}_A = \delta$, writing $\rho|_{D_p} \cong \left(\begin{smallmatrix} \epsilon & * \\ 0 & \delta \end{smallmatrix}\right)$.

Indeed, if we have such $\widetilde{\rho} : \mathfrak{G}^S \to GL_2(A)$, moving $\widetilde{\rho}$ by conjugation in $GL_2(A)$ if necessary, we find by continuity a compact W-subalgebra $B \subset A$ such that $\widetilde{\rho}$ has image in $GL_2(B)$ and $\widetilde{\rho} \mod (\mathfrak{m}_A \cap B) \cong \rho$. This point can be also verified by using the technique of pseudo representation of Wiles (e.g., [MFG] 2.2.1). Then by the versality of R, we have a W-algebra homomorphism $\varphi : R \to B$ such that $\varphi \circ \boldsymbol{\rho} \cong \widetilde{\rho}$ in $GL_2(B)$. This morphism induces $\varphi_P : R_P \to A$ after localization. Since R_P is topologically generated by the traces of $\boldsymbol{\rho}$, the localized version φ_P is uniquely determined by $\widetilde{\rho}$, and hence $(R_P, \boldsymbol{\rho})$ prorepresents Φ_P. Then in the same manner as in the proof of Theorem 5.14 in [MFG], we have $\mathrm{Sel}^-_{\mathbb{Q}}(Ad(V))^* \cong \Omega_{R_P/K} \otimes_{R_P} K$, and hence once again, we obtain the isomorphisms of $\mathbb{T}$ onto $\mathrm{Sel}^-_{\mathbb{Q}}(Ad(V))$ and onto the tangent space of $\mathrm{Spf}(R_P)$ at P.

We only need to assume the existence of $\pi : R \to \Lambda$ which is an isomorphism at the level of the tangent spaces after localization at P. Since Λ_{P_f} is generated by the trace of $\boldsymbol{\rho}_{\mathcal{F}}$, the natural morphism $\pi : R_P \to \Lambda_{P_f}$ is surjective. We suppose that this surjection induces the isomorphism of the tangent space PR_P/P^2R_P of $\mathrm{Spf}(R_P)$

for the localization completion R_P of R at P onto the tangent space $(x)/(x)^2$ of $\mathrm{Spf}(K[[x]])$ at $x=0$. Since Λ_{P_f} is the one variable power series ring $K[[x]]$, the surjection $\pi: R_P \twoheadrightarrow \Lambda_{P_f}$ inducing the identification of the tangent space is actually an isomorphism $R_P \cong \Lambda_{P_f}$. Thus the assumption (weaker in appearance) of the tangential isomorphism is actually equivalent to having the isomorphism $R_P \cong \Lambda_{P_f}$. Then the tangent space at P of $\mathrm{Spf}(R_P)$ is one-dimensional over K generated by $\pi_* \frac{d}{dx}\big|_{x=0}$.

Here is how the isomorphism of $\mathbb{T}$ with the tangent space is computed, for example, in [MFG] 5.2.4: Each inhomogeneous cocycle c (representing an element of $\mathbb{T}$) gives rise to an infinitesimal nearly ordinary deformation $\widetilde{\rho}_c$ with $\det(\widetilde{\rho}) = \det\rho$:

$$\widetilde{\rho}_c : \mathfrak{G}^S \to GL_2(K[x]/(x^2))$$

given by $\widetilde{\rho}_c(\sigma) = \rho(\sigma) + c(\sigma)\rho(\sigma)x$. The tangent space at P of $\mathrm{Spf}(R)_{/W}$ is isomorphic to

$$\frac{\{\widetilde{\rho} \in \Phi(K[x]/(x^2)) | \widetilde{\rho} \mod (x) = \rho\}}{\sim} = \Phi_P(K[x]/(x)^2)$$

by a standard argument (which can be found in [MFG] 5.2.4). Here "$\sim$" is the conjugation under $1 + xM_2(K) \subset GL_2(K[x]/(x^2))$ and (as one can check easily) corresponds to the cohomologous relation in $\mathbb{T}$. Thus $c \mapsto \widetilde{\rho}_c$ induces the isomorphism from $\mathbb{T}$ to the tangent space of $\mathrm{Spf}(R_P)$ at P.

Taking an inhomogeneous cocycle $c : \mathfrak{G}^S \to Ad(V)$ representing a generator of $\mathbb{T}$, we write $c(\sigma) = \begin{pmatrix} -a(\sigma) & b(\sigma) \\ 0 & a(\sigma) \end{pmatrix}$ for $\sigma \in D_p$. If c restricted to D_p modulo upper nilpotent cocycles is unramified, it gives rise to a nontrivial element of $\mathrm{Sel}_{\mathbb{Q}}(Ad(V))$. By the vanishing of $\mathrm{Sel}_{\mathbb{Q}}(Ad(V))$ (Lemma 2.1), we find $a \neq 0$ on I_p. Then $\mathcal{L}(Ad(V)) = a([p,\mathbb{Q}_p]) \cdot \frac{\log_p(\gamma)}{a([\gamma,\mathbb{Q}_p])}$ for a generator γ of $1+p\mathbb{Z}_p$. We therefore need to compute this value.

Since $PR_P/P^2R_P \cong \mathbb{T}$ as already remarked, $\frac{d\boldsymbol{\rho}}{dx}$ gives rise to a generator of $\mathbb{T}$ by the universality of $(R_P, \boldsymbol{\rho} = \boldsymbol{\rho}_{\mathcal{F}})$; so, we have $c(\sigma)\rho(\sigma) = C \cdot \frac{d\boldsymbol{\rho}}{dx}(\sigma)$ with a constant $C \in K^\times$. Writing $\boldsymbol{\rho}(\sigma) = \begin{pmatrix} \boldsymbol{\epsilon}(\sigma) & \boldsymbol{\beta}(\sigma) \\ 0 & \boldsymbol{\delta}(\sigma) \end{pmatrix}$ for $\sigma \in D_p$, we have therefore

$$\begin{aligned} a([p,\mathbb{Q}_p])\delta([p,\mathbb{Q}_p]) &= C \cdot \frac{d\boldsymbol{\delta}([p,\mathbb{Q}_p])}{dx}\Big|_{x=0}, \\ a([\gamma,\mathbb{Q}_p])\delta([\gamma,\mathbb{Q}_p]) &= C \cdot \frac{d\boldsymbol{\delta}([\gamma,\mathbb{Q}_p])}{dx}\Big|_{x=0}. \end{aligned} \tag{4.1}$$

The factors $\delta([p,\mathbb{Q}_p])$ and $\delta([\gamma,\mathbb{Q}_p])$ on the left-hand side come from the left multiplication by $\rho(\sigma)$ in the identity: $c(\sigma)\rho(\sigma) = C \cdot \frac{d\boldsymbol{\rho}}{dx}(\sigma)$.

For the modular p–ordinary deformation $\boldsymbol{\rho}^{ord}_{\mathcal{F}}$, its determinant $\det(\boldsymbol{\rho}^{ord}_{\mathcal{F}})$ is the universal deformation on $\mathfrak{G}^S$ of $\det(\rho) \mod \mathfrak{m}$ (at least locally around P_f). Write the universal deformation of the trivial character of $\mathfrak{G}^{\{p\}}$ as $\gamma^s \mapsto (1+x)^s$. Thus the character $(1+x)^{-s/2}$ sends $\sigma \in \mathfrak{G}$ inducing $\chi^{-1}(\gamma^s)$ on $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ for a generator $\gamma \in 1+p\mathbb{Z}_p$ to $(1+x)^{-s/2}$. This shows $\boldsymbol{\rho} = \boldsymbol{\rho}_{\mathcal{F}} = \boldsymbol{\rho}^{ord}_{\mathcal{F}} \otimes (1+x)^{-s/2}$ after localization at P. Then the character $\boldsymbol{\delta}$ is given by $\boldsymbol{\delta}([\gamma^s,\mathbb{Q}_p]) = (1+x)^{-s/2}$ because the character $\boldsymbol{\delta}^{ord}$ at the lower right corner of $\boldsymbol{\rho}^{ord}_{\mathcal{F}}|_{D_p}$ is unramified. Then we have

$$\delta([\gamma,\mathbb{Q}_p]) = \boldsymbol{\delta}([\gamma,\mathbb{Q}_p])|_{x=0} = \left(\boldsymbol{\delta}^{ord}([\gamma,\mathbb{Q}_p])(1+x)^{-s/2}\right)\Big|_{x=0} = 1$$

by the unramifiedness of $\boldsymbol{\delta}^{ord}$, and

$$\frac{d\boldsymbol{\delta}([\gamma^s,\mathbb{Q}_p])}{dx}\Big|_{x=0} = -\frac{s}{2} \quad\text{and}\quad \frac{d\boldsymbol{\delta}([\gamma^s,\mathbb{Q}_p])}{dx}\Big|_{x=0}\log_p(\gamma^s)^{-1} = -\frac{1}{2\log_p(\gamma)}.$$

As for the value at $[p,\mathbb{Q}_p]$, we have $\boldsymbol{\delta}^{ord}([p,\mathbb{Q}_p]) = a(p,\mathcal{F})$ (e.g., [GME] Theorem 4.2.7 (3)). Since $\chi([p,\mathbb{Q}_p]) = 1$ and the character $(1+x)^{s/2}$ interpolates $\chi^{m(p-1)}$ for all integer m, $(1+x)^{s/2}$ has value 1 at $[p,\mathbb{Q}_p]$. We should not forget the factor $\delta([p,\mathbb{Q}_p])$ in the first equation of (4.1) which is equal to

$$\boldsymbol{\delta}^{ord}([p,\mathbb{Q}_p])|_{x=0} = a(p,\mathcal{F})|_{x=0} = a(p,f).$$

Thus we get the desired result from the definition of $\mathcal{L}(Ad(V))$. □

References

Books

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

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

[MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, 2000, Cambridge University Press

Articles

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves over **Q**: wild 3–adic exercises, J. AMS **14** (2001), 843–939

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

[G1] R. Greenberg, Iwasawa theory for p–adic representations, Adv. Studies in Pure Math. **17** (1989), 97–137

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

[H86] H. Hida, Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, Inventiones Math. **85** (1986), 545–613

[H88] H. Hida, On p-adic Hecke algebras for GL_2 over totally real fields, Ann. of Math. **128** (1988), 295–384

[H96] H. Hida, On the search of genuine p–adic modular L–functions for $GL(n)$, Mémoire SMF **67**, 1996

[H00] H. Hida, Adjoint Selmer groups as Iwasawa modules, Israel Journal of Math. **120** (2000), 361–427

[HT] H. Hida and J. Tilouine, On the anticyclotomic main conjecture for CM fields, Inventiones Math. **117** (1994), 89–147

[SW] C. Skinner and A. Wiles, Residually reducible representations and modular forms. Inst. Hautes Études Sci. Publ. Math. No. **89** (2000), 5–126

[SW1] C. Skinner and A. Wiles, Nearly ordinary deformations of irreducible residual representations, Ann. Fac. Sc. Toulouse Math. (6) **8** (2001)

[W] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. **141** (1995), 443–551

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