

MODULAR GALOIS REPRESENTATIONS OF “NEBEN” TYPE

HARUZO HIDA

1. INTRODUCTION

In 1995 in [W] Theorem 0.2, A. Wiles proved, under some mild conditions (and relying on a ring theoretic result on Hecke algebras in [TW]), that if a p -adic Galois representation is congruent modulo p to that of an elliptic cusp form, then the representation itself is associated to a cusp form. After that, I have been thinking of characterizing *residually dihedral* Galois representations, because a 2-dim induced Galois representation is always modular. In this context, this paper is a continuation of the investigation done in [H98] and [HM97]. We have shown in [H98] (downloadable at www.math.ucla.edu/hida) that for modular Galois representations of weight $k \geq 2$ with real quadratic Neben type, the (odd) prime p giving residually dihedral representation is always a factor of $N(\varepsilon^{k-1} - 1)$ for the positive fundamental unit ε of the quadratic extension, generalizing a result of Shimura in 1972 for weight 2. A simple application of this fact to the base-change problem was discussed in [HM97]. At the same time, I made a conjecture describing the universal p -ordinary deformation ring of a dihedral representation, which has been basically solved now by Cho-Vatsal [CV] (downloadable at www.math.ubc.ca/vatsal). However the knowledge of the deformation ring does not give us an immediate method of constructing residually dihedral Galois representations. Here we would like to present a simple and (very elementary) constructive method, which actually gives all residually dihedral representations. As an obvious application of our result, we can show automatically the modularity of many non- \mathbb{Q} -rational elliptic \mathbb{Q} -curves, \mathbb{Q} -HBAV or rank two \mathbb{Q} -motives, although we only discuss some examples of elliptic \mathbb{Q} -curves in details in this paper (see Section 5). Some more background materials of this type of approach to the modularity problems of motives will be included in my forthcoming book [H00]. Also one of my students: Ami Fischman is now trying to use the idea here to make the result in [HM97] more systematic. Hereafter in this paper the prime p is assumed to be odd.

2. TAYLOR-WILES THEOREM

Let Σ be a finite set of primes including the fixed odd prime p and \mathbb{Q}^Σ be the maximal extension unramified outside Σ and ∞ . Let $\mathfrak{G} = \text{Gal}(\mathbb{Q}^\Sigma/\mathbb{Q})$. We pick an absolutely irreducible *odd* representation $\bar{\rho} : \mathfrak{G} \rightarrow GL_2(\mathbb{F})$ for a finite field \mathbb{F} of characteristic p . All Galois representations are supposed to be *continuous*, and all valuation rings will be finite flat over \mathbb{Z}_p .

We consider the following conditions:

A summary of Sections 5.1.1 and 5.2.1-2 from my book: “Geometric Modular Forms and Elliptic Curves” from World Scientific, 2000.

- (Ordinarity) $\bar{\rho}|_{D_p} \cong \begin{pmatrix} \bar{\varepsilon} & * \\ 0 & \bar{\delta} \end{pmatrix}$ with $\bar{\delta}$ unramified and $\bar{\delta} \neq \bar{\varepsilon}$ on the decomposition group D_p at p ;
(Flatness) $\bar{\rho}$ restricted to the decomposition group at p is isomorphic to a Galois module associated to a locally free group scheme over \mathbb{Z}_p of rank $|\mathbb{F}|^2$;
(Irreducibility) $\bar{\rho}$ restricted to $\text{Gal}(\mathbb{Q}^\Sigma/\mathbb{Q}(\mu_p))$ remains absolutely irreducible;
(Modularity) $\bar{\rho}$ is associated to an elliptic cusp form.

We now quote a theorem from [W] Theorem 0.2 and [D]:

Theorem 2.1 (Wiles-Taylor-Diamond). *Suppose modularity and irreducibility and either ordinarity or flatness of $\bar{\rho}$. Let $\rho : \mathfrak{G}_\Sigma \rightarrow GL_2(O)$ be a Galois representation for a DVR O such that*

1. $\rho \equiv \bar{\rho} \pmod{\mathfrak{m}_O}$;
2. $\det \rho = \nu_p^{k-1}$ up to finite order characters for $k \geq 2$, where ν_p is the p -adic cyclotomic character;
3. $\rho|_{D_p} \cong \begin{pmatrix} \varepsilon & * \\ 0 & \delta \end{pmatrix}$ for an unramified character $\delta \equiv \bar{\delta} \pmod{\mathfrak{m}_O}$ when $\bar{\rho}$ is ordinary;
4. When $\bar{\rho}$ is flat, $k = 2$ and $\det \rho|_{I_p} = \nu_p|_{I_p}$ and ρ is associated to a p -divisible group over \mathbb{Z}_p in the sense of Tate.

Then there exist a positive integer N and a Hecke eigenform $f \in S_k(\Gamma_1(N))$ such that $\rho \cong \rho_f$.

The above theorem was proven in [W] as Theorem 0.2 under an additional condition on auxiliary ramification outside p , which was later removed by Diamond in [D]. Wiles proved the result assuming the complete intersection property of a certain Hecke algebra in the minimal ramification case, which was in turn proved in [TW]. The flatness condition is now eased by Conrad-Diamond-Taylor to potential flatness over an extension of \mathbb{Z}_p with ramification index $\leq p - 1$. Also there is a generalization of the above theorem to Hilbert modular forms by K. Fujiwara.

3. RESIDUALLY DIHEDRAL NON-DIHEDRAL REPRESENTATIONS

We always write A for a DVR. Let F be a quadratic extension of \mathbb{Q} , and fix a finite set S of rational primes including p . We look into a little smaller $G = \text{Gal}(F^S/\mathbb{Q})$ and $H = \text{Gal}(F^S/F)$. Here F^S/F is the maximal extension of F unramified outside S and ∞ . First we explain how to create a Galois representation $\rho_G : G \rightarrow GL_2(B)$ (for a canonical $B \supset A$) residually induced from a Galois representation $\rho = \rho_H : H \rightarrow GL_2(A)$.

Put $V = A^2$, and let H act on V via ρ_H . If ρ_H is absolutely irreducible as a representation with coefficients in the field of fractions K of A , we may assume $V = A[H]v$ for $\exists v \in V$ without changing its isomorphism class over K (replacing V by $A[H]v$ if necessary). We fix an element $\delta \in G$ which induces a non-trivial automorphism on F . We assume that ρ_H satisfies the following two conditions:

- (I0) $V = V(\rho_H)$ is cyclic over $A[H]$;
- (I1) ρ_H is absolutely irreducible over the quotient field of A ;
- (I2) We have an A -linear endomorphism $T : V \rightarrow V$ such that $T(hx) = \delta h \delta^{-1} T(x)$ and $\det T \neq 0$.

The existence of T assures us the existence of an extension ρ_G of ρ_H . Here is how to create an universal extension ρ_G . Consider the induced module: $W = A[G] \otimes_{A[H]} V$, which is free

of rank 4 over A . Define an A -linear endomorphism $\tilde{T} : W \rightarrow W$ by $\tilde{T}(\delta^i \otimes v) = \delta^{i-1} \otimes T(v)$ for $i \in \mathbb{Z}/2\mathbb{Z}$. By

$$\tilde{T}(h\delta^i \otimes v) = \delta^{i-1} \otimes T(\delta^{-i} h \delta^i v) = \delta^{i-1} \otimes \delta^{1-i} h \delta^{i-1} T(v) = h \delta^{i-1} \otimes T(v) = h \tilde{T}(\delta^i \otimes v),$$

\tilde{T} commutes with $A[H]$ and obviously commutes with δ and hence commutes with $A[G]$. Thus $B = \text{End}_{A[G]}(W)$ is bigger than A .

Dividing T by a suitable element in A , we may assume that $\bar{T} = (T \bmod \mathfrak{m}_A)$ for the maximal ideal \mathfrak{m}_A of A does not vanish. Then by definition, $\rho_H(\delta^{-2})T^2$ commutes with ρ_H and hence is a scalar t by Schur's lemma. The elements $t \in A$ is uniquely determined in $O = (A - \{0\})/(A^\times)^2$, and we call the class $Ob(\rho_H) \in O$ the obstruction class of ρ_H . Then it is easy to see:

Proposition 3.1. *Suppose (I0-2). We have*

1. $B \cong A[\sqrt{t}] = A[X]/(X^2 - t)$;
2. W is free of rank 2 over B ;
3. If $Ob(\rho_H) \in \mathfrak{m}_A$, then B is a local ring; so, write $\rho_G : G \rightarrow GL_2(B)$ for the representation realized on W ;
4. If $Ob(\rho_H) \in \mathfrak{m}_A$ and $\bar{\rho} = (\rho_G \bmod \mathfrak{m}_B)$ is absolutely irreducible, then there exists a character $\xi : H \rightarrow (B/\mathfrak{m}_B)^\times$ such that $\bar{\rho} \cong \text{Ind}_H^G \xi$.

Proof. All assertions can be easily proven. We first prove (1-3).

Let B' be the subalgebra of B generated over A by \tilde{T} . Since $\tilde{T}^2 = t = \rho_H(\delta^{-2})T^2$, we see $B' \cong A[\sqrt{t}]$. If either t is not square in A or $t \in \mathfrak{m}_A$, by our construction, B' is a local ring and $W/\mathfrak{m}_{B'}W$ is two dimensional over the residue field of B' . Then Nakayama's lemma shows that W is free of rank 2 over B' , and hence $B = B'$. When t is a square unit in A , obviously $B \cong A \oplus A$, and the assertion (1-3) again follows.

The assertion (4) follows from the fact that $\bar{T} \not\equiv 0 \pmod{\mathfrak{m}_A}$ but $\det \bar{T} = 0$. Thus we have an exact sequence of H -modules: $0 \rightarrow \text{Ker}(\bar{T}) \rightarrow V/\mathfrak{m}_A V \rightarrow \text{Im}(\bar{T}) \rightarrow 0$; so, $\bar{\rho}_H$ is reducible with semi-simplification isomorphic to $\xi \oplus \xi^\delta$ ($\xi^\delta(h) = \xi(\delta h \delta^{-1})$) by (I2). Mackey's criterion of irreducibility of induced representations now tells us that $\xi^\delta \neq \xi$ and $\bar{\rho} \cong \text{Ind}_H^G \xi$, because $\bar{\rho}$ is supposed to be absolutely irreducible. \square

The ring B has an involution $\sigma : \circlearrowleft B$ such that $\rho_G \otimes \chi \cong \sigma \circ \rho_G$ and $\sigma(\sqrt{t}) = -\sqrt{t}$ ($\chi : G/H \cong \{\pm 1\}$).

There is a converse of the above proposition: Start with a Galois representation $\varphi : G \rightarrow GL_2(O)$ for a DVR O with irreducible $\bar{\varphi} = (\varphi \bmod \mathfrak{m}_O) \cong \text{Ind}_H^G \xi$; so, $\bar{\varphi}(\delta)$ cannot be in the center. We assume that $\varphi_H = \varphi|_H$ is absolutely irreducible. We may assume (and will assume) that O is the normalization of the subring generated by $\text{Tr}(\varphi)$ over \mathbb{Z}_p because of the absolute irreducibility of $\bar{\varphi}$ (see [N] and [H99] II.2.1-2). Since, for $\chi : G/H \cong \{\pm 1\}$,

$$\phi \cong \text{Ind}_H^G \eta \exists \eta \iff \phi \otimes \chi \cong \phi,$$

we can divide our consideration into two cases:

- (a) There exists an involution σ of O such that $\sigma \circ \varphi \cong \varphi \otimes \chi$;
- (b) No such involution.

In Case (b), we may regard $\Phi \cong \varphi \oplus (\varphi \otimes \chi)$ as representations into $GL_2(B')$ for the subring $B' \subset O \oplus O$ generated over O by $\text{Tr}(\Phi(g))$ for all $g \in G$, because we can find such Φ in the isomorphism class of $\varphi \oplus (\varphi \otimes \chi)$ by means of pseudo-representations of Wiles (see [H99] II.2.1-2 for generality of pseudo-representations). Since φ is residually induced, B'

is a local ring. Then we define $\sigma \in \text{Aut}(B')$ by $\sigma(x, y) = (y, x)$. In Case (a), we write B' for O and Φ for φ . Then we have

Proposition 3.2. *Let $A_0 = H^0(\langle \sigma \rangle, B')$. Then there exist a DVR A unramified over A_0 and $\rho_H : H \rightarrow GL_2(A)$ such that*

1. $\text{Tr} \rho_H = \text{Tr} \varphi_H$;
2. $\text{Ob}(\rho_H) \in \mathfrak{m}_A$;
3. *We have an isomorphism $\iota : B \hookrightarrow A \otimes_{A_0} B'$ such that $\iota \circ \rho_G \cong \varphi$ or Φ according as we are in Case (a) or (b),*

where ρ_G is the representation constructed in the previous proposition.

Proof. Since $\text{Tr}(\Phi \otimes \chi) = \text{Tr}(\sigma \circ \Phi)$, we have $\Phi \otimes \chi \cong \sigma \circ \Phi$ over B' again by the result of Carayol. Thus we have an automorphism $\mathcal{T} : V(\Phi) \rightarrow V(\Phi)$ for the representation space $V(\Phi)$ of Φ such that $\mathcal{T}\Phi(g) = \chi(g)\sigma(\Phi(g))\mathcal{T}$ for all $g \in G$. The automorphism \mathcal{T} is uniquely determined up to scalar (cf. [H99] Lemma II.1.12). If \mathcal{T} is scalar, then $\Phi = \chi \otimes (\sigma \circ \Phi)$. Since we have $\text{Tr}(\Phi) \equiv \text{Tr}(\sigma \circ \Phi) \pmod{\mathfrak{m}_{B'}}$, σ induces the identity map on $B'/\mathfrak{m}_{B'}$. Thus $\Phi(g) \equiv \chi(g)\Phi(g) \pmod{\mathfrak{m}_{B'}}$ for all $g \in G$, which is impossible. Thus \mathcal{T} is non-scalar.

Let $\overline{\mathcal{T}} = \mathcal{T} \pmod{\mathfrak{m}_{B'}}$. Since σ is trivial modulo $\mathfrak{m}_{B'}$, $\overline{\mathcal{T}}^2$ has to be a scalar, because $\overline{\rho}$ is absolutely irreducible (by Schur's lemma: [H99] Lemma II.1.5). Similarly $\sigma(\mathcal{T})\mathcal{T}$ commutes with Φ and hence is a scalar $u \in B'^{\times}$. Thus \mathcal{T} commutes with $\sigma(\mathcal{T})^{-1}$ and hence commutes with $\sigma(\mathcal{T})$. In particular, u is in the subring A_0 of B' fixed by σ . By our construction, A_0 is a DVR and is the normalization of the subring generated (over \mathbb{Z}_p) by traces over H of the representation Φ . Note that $\overline{\rho} \otimes \chi \cong \overline{\rho}$; so, σ is the identity on the residue field of B' . In Case (a), O is a ramified quadratic extension of A_0 , and in Case (b), $A_0 = O$.

If u is not a square in A_0^{\times} , we define $A = A_0[\sqrt{u}]$, otherwise, we rewrite $A = A_0$. Since $p > 2$, A is a discrete valuation ring unramified over A_0 . Then we write B for $B'[\sqrt{u}]$. We extend σ to a unique automorphism of B fixing A . Then changing \mathcal{T} by $\zeta\mathcal{T}$ for $\zeta \in A$ with $\zeta^2 = u^{-1}$, we may assume that $\sigma(\mathcal{T})\mathcal{T} = 1$. Let K be the quotient field of A . Then $K[\mathcal{T}]$ is a semi-simple quadratic extension of K . By the Hilbert theorem 90, applied to $K[\mathcal{T}]$, we find $\mathcal{S} \in K[\mathcal{T}]$ such that $\mathcal{T} = \sigma(\mathcal{S})^{-1}\mathcal{S}$. Then $\rho' = \mathcal{S}\Phi\mathcal{S}^{-1}$ satisfies $\rho'(g) = \chi(g)\sigma(\rho'(g))$ for all $g \in G$. If G is a compact group and φ is continuous, the image of Φ has to be in a maximal compact subgroup, which is a conjugate of $GL_2(A)$. So further conjugating $\rho'|_H$ by an element in $GL_2(K)$, we find $\rho : H \rightarrow GL_2(A)$ such that

1. ρ has values in $GL_2(A)$;
2. $V(\rho)$ is generated by a single element over $A[H]$;
3. ρ is isomorphic to $\varphi|_H$ over the quotient field of O .

The third point follows from the trace identity of ρ and $\varphi|_H$. The point (2) is achieved by replacing $V(\rho)$ by $A[H]v$ for $v \neq 0$ in $V(\rho)$. By (3) and the assumption (I1), ρ is absolutely irreducible over K , and hence, $A[H]v$ is free of rank two over A .

Out of this choice of ρ , we go back to the process as in the proof of Proposition 3.1: Let $W = A[G] \otimes_{A[H]} V(\rho)$. Supposing that the ring $B = \text{End}_{A[G]}(W)$ is isomorphic to $A \oplus A$, we would like to show $\overline{\rho} \otimes \chi \not\cong \overline{\rho}$. This actually leads to a contradiction as we will see after proving the non-congruence. By our choice of ρ , $V(\rho) = A[H]v$ for $v \in V(\rho)$. Thus $W = A[G]v$. Therefore, for $\overline{W} = W \otimes_A \mathbb{F}$ with $\mathbb{F} = A/\mathfrak{m}_A$, we have $A[G]\overline{v} = \overline{W}$ for $\overline{v} = (v \pmod{\mathfrak{m}_A W})$. Thus we conclude that $\mathbb{F}[\overline{G}]\overline{v} = \overline{W}$, where $\overline{G} = G/\text{Ker}(\overline{\rho}) \cong \text{Im}(\overline{\rho})$. It is

known (e.g. [H99] II.1.5) that

$$\mathbb{F}[\overline{G}] \cong \bigoplus_{\pi \in \widehat{\overline{G}}} R(\pi),$$

where $\widehat{\overline{G}}$ is the set of irreducible representations of the finite group \overline{G} , and $R(\pi)$ modulo its nilradical is a simple algebra isomorphic to $\text{Im}(\pi)$. Since $\overline{W} \cong V(\overline{\rho}) \oplus V(\overline{\rho} \otimes \chi)$ is semi-simple by our assumption, the fact: $\overline{W} = \mathbb{F}[\overline{G}]_{\overline{\rho}}$ tells us that the nilradical of $\mathbb{F}[\overline{G}]$ kills \overline{W} , and \overline{W} is a surjective image of a single component $R(\pi)$ if $\overline{\rho} \cong \overline{\rho} \otimes \chi$. In this case, $\text{End}_{\mathbb{F}[\overline{G}]}(\overline{W}) = M_2(\mathbb{F})$, which does not have two distinct idempotents commuting each other. Since we have two distinct commuting idempotents in $\text{End}_{A[G]}(\overline{W})$, we conclude the non-congruence: $\overline{\rho} \otimes \chi \not\cong \overline{\rho}$. This is a contradiction against our assumption of residual dihedralness and residual irreducibility, because the congruence is a characterization of induced representations (see [H99] Lemma II.1.14). Thus B has to be a local ring, and hence $Ob(\rho) \in \mathfrak{m}_A$.

We have now rediscovered the ring B , which is either isomorphic to B' or $B' \otimes_{A_0} A$. The resulting representations ρ_G and Φ are isomorphic each other by the result of Carayol, because they have equal trace and absolutely irreducible reduction modulo the maximal ideal (cf. [H99] Proposition II.1.13). \square

4. MODULARITY PROBLEMS

We start with an irreducible Galois representation $\rho_H : H \rightarrow GL_2(A)$ satisfying the following three conditions in addition to (I1-2):

- (I3) We have $Ob(\rho_H) \in \mathfrak{m}_A$;
- (I4) $\overline{\rho}_G = \rho_G \pmod{\mathfrak{m}_B}$ is absolutely irreducible;
- (I5) $\det \rho_G(c) = -1$ for complex conjugation c .

Combining the two propositions with Theorem 2.1, we get

Theorem 4.1. *Suppose the five conditions (I1-5) and that the representation ρ_G is either p -ordinary with $\det \rho_G = \nu_p^{k-1}$ up to finite order characters for $k \geq 2$ or flat with $\det \rho|_{I_p} = \nu_p|_{I_p}$. Then for any extension $\varphi : G \rightarrow GL_2(O)$ of ρ_H for a DVR O over A , if $\overline{\varphi} = (\varphi \pmod{\mathfrak{m}_O})$ is absolutely irreducible on $\text{Gal}(F^S/\mathbb{Q}(\mu_p))$, then there exist an integer $N > 0$ and a Hecke eigenform $f : S_k(\Gamma_1(N))$ such that $\varphi \cong \rho_f$.*

The integer N of course can be taken to be the conductor of the compatible system of Galois representations attached to f as above.

An immediate corollary of this theorem is:

Corollary 4.2. *Let $\varphi = \{\varphi_l\}_l$ be a compatible system of 2 dimensional Galois representations of H with coefficients in a number field E . Here we assume that E is a minimal possible choice. If one of the members φ_p satisfies the five conditions (I1-5) and the assumptions of Theorem 4.1, then the system can be extended to a compatible system Φ of two dimensional Galois representations in exactly two ways, one is Φ and the other is $\Phi \otimes \chi$, and E is either a CM field or a totally real field.*

When φ is associated to an abelian variety, the conclusion of the corollary follows from the solution of the Tate conjecture by Faltings [F]. However the result is new for 2-dimensional compatible systems associated to general motives.

We now describe a sufficient condition that $\bar{\rho} = \text{Ind}_H^G \xi$ in (I4) remains irreducible over $K = \text{Gal}(F^S/\mathbb{Q}(\mu_p))$. By Frobenius reciprocity law (cf. [H99] II.1.6), reducibility of $\bar{\rho}$ on K is equivalent to the reducibility of $\bar{\rho}|_{H'}$ for $H' = \text{Gal}(F^S/\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}))$, where $\kappa = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ is the unique quadratic extension in $\mathbb{Q}(\mu_p)$. This happens only when $\bar{\rho}(H')$ modulo center is abelian.

Since the image of $\bar{\rho}$ modulo center is a dihedral group of order $2n$ for the order n of $\xi^{-1}\xi^\delta$, we study when a dihedral group D_{2n} of order $2n$ has an abelian normal subgroup of index 2. A dihedral group D_{2n} is abelian only when $n \leq 2$. A dihedral group of order $2n$ with $n \geq 3$ has a unique normal cyclic subgroup C_n of order n . We see easily that the maximal abelian quotient D_{2n}^{ab} of D_{2n} is either isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$ according as n is odd or even. Therefore when $n \geq 3$ is odd, the cyclic subgroup C_n is the unique subgroup of index 2.

Now we suppose that n is even. Since $D_{2n}^{ab} \cong (\mathbb{Z}/2\mathbb{Z})^2$, there are 3 normal subgroups X of index 2. If $X \neq C_n$, choose $d \in X - C_n$. Then $d^2 = 1$ and $dcd^{-1} = c^{-1}$ for $c \in C_n$. Thus $X \cong D_n$, which is non-abelian if $n > 4$. Thus we have an abelian normal subgroup of index two in D_{2n} if and only if $n = 2$ and 4.

Suppose that $n = 2m$ is even. The conjugation action of D_{2n}/C_n on C_n fixes element by element the unique subgroup C_n of order 2. Thus for any character ξ of C_n of order n , $\xi^{-1}\xi^\delta$ for $\delta \in D_{2n} - C_n$ has order m . Thus if $m \geq 4$, we still see that the restriction of $\text{Ind}_{C_n}^{D_{2n}} \xi$ to any subgroup of index 2 is irreducible. This settles the case where the order of $\xi^{-1}\xi^\delta$ is equal to 4. We thus conclude

Proposition 4.3. *Let the notation be as in (I4) and p be an odd prime. Suppose that $F \not\subseteq \mathbb{Q}(\mu_p)$ and that $\bar{\rho} = \text{Ind}_H^G \xi$ is absolutely irreducible. Then if either the order of $\xi^{-1}\xi^\delta$ is larger than 2 or there exists $\sigma \in \text{Ker}(\bar{\rho})$ acting non-trivially on κ , $\bar{\rho}$ remains absolutely irreducible over $\mathbb{Q}(\mu_p)$.*

5. ELLIPTIC \mathbb{Q} -CURVES

An elliptic curve E defined over a number field is called a \mathbb{Q} -curve if for any $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have an isogeny $\mu_\sigma : E \rightarrow E^\sigma$. By a result of Elkies, all elliptic \mathbb{Q} -curves have a model over a $(2, 2, \dots, 2)$ -extension of \mathbb{Q} . Here we treat the case where E itself has a model over a quadratic extension F/\mathbb{Q} . Presumably an inductive argument should give a similar result to more general cases. The following construction of an example of φ as in Theorem 4.1 is a version of an argument of Shimura in [S] Sections 9-10:

Corollary 5.1. *Let E be an elliptic curve defined over F . Suppose that $\text{End}(E/\overline{\mathbb{Q}}) = \mathbb{Z}$ and that we have an isogeny $\theta : E \rightarrow E^\delta$ defined over $\overline{\mathbb{Q}}$ with the following property for a prime $5 \leq p \nmid D$:*

$$p \mid \deg(\theta) \text{ and the } p\text{-primary part of } \text{Ker}(\theta) \text{ is cyclic.}$$

If E has a semi-stable reduction at p over F , then there exists a positive integer N such that E shows up as a factor over a finite abelian extension L of F of the jacobian of the modular curve $X_1(N)$. When θ is defined over F , L can be taken to be F itself.

We are going to prove that the Tate module $T_p(E)$ is reducible modulo p , giving rise to two characters $\xi, \xi' : H \rightarrow \mathbb{F}_p^\times$ and satisfies the assumptions of Theorem 4.1. It will be clear from the following proof that if either $p \equiv 1 \pmod{4}$ or $\xi^{-1}\xi'$ ramifies at a prime $q \neq p$, we do not need to assume any condition on reduction of E modulo p to show the assertion of the corollary.

Proof. We first assume that θ is defined over F . We need to check the five conditions: (I1-5) and the assumptions of Theorem 4.1 for $V(\varphi) = T_p(E)$. If this is done, we have by Theorem 4.1 a non-trivial $\mathbb{Z}_p[H]$ -linear homomorphism from the p -divisible group $J_1(N)[p^\infty]$ into $E[p^\infty]$; so, again by a theorem of Faltings already quoted, we have a surjection $J_1(N) \rightarrow E$ defined over F .

Since $\text{End}(E/\overline{\mathbb{Q}}) = \mathbb{Z}$, by the theorem of Faltings as above, the representation φ is absolutely irreducible over F (I1).

Since $\theta^\delta \circ \theta$ is an endomorphism of E , it is equal to an integer $d \neq 0$.

Now assume that p divides $\deg(\theta)$ and that $p \geq 5$. Here the set S is the union of $\{p\}$ and the set of rational primes where E has bad reduction. We may identify $E^\delta[p^\infty]$ with $E[p^\infty]$ by $x \mapsto \delta x$. Thus we have a natural identification of $V(\varphi^\delta)$ and $V(\varphi)$. Writing this identification as $i : V(\varphi) \cong V(\varphi^\delta)$, we have $i(h(x)) = \delta h \delta^{-1} i(x)$. Then the isogeny θ induces $T = i \circ \theta : V(\varphi) \rightarrow V(\varphi)$ such that $T(hx) = \delta h \delta^{-1} T(x)$ (I2).

Since θ is cyclic at p , $\text{Coker}(T)$ is isomorphic to the p -Sylow part of the group $\text{Ker}(\theta)$ which is cyclic, and hence $\text{Coker}(T)$ is non-trivial by our choice of p . Writing d_p for the p -primary part of d , we find that $\text{Ob}(\varphi_H) = d_p \in p\mathbb{Z}_p$ (I3).

Let ξ be the character of H through which H acts on $\text{Ker}(\theta) \otimes_{\mathbb{Z}} \mathbb{F}_p$. Then by definition, the action of H on $\text{Ker}(\theta^\delta) \otimes_{\mathbb{Z}} \mathbb{F}_p$ gives rise to $\xi^\delta(h) = \xi(\delta h \delta^{-1})$.

If $x \in E[d_p]$, then $\theta^\delta \circ \theta(x) = d_p x = 0$. Thus $\theta(x) \in \text{Ker}(\theta^\delta)$. By counting the order, we find that $\theta(E[d_p]) = \text{Ker}(\theta^\delta) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Thus we have an exact sequence of H -modules:

$$0 \rightarrow V(\xi) \rightarrow E[p] \xrightarrow{\theta} V(\xi^\delta) \rightarrow 0.$$

Since $\xi \xi^\delta = \omega_p$ for the mod p Teichmüller character ω_p of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and since $\omega_p|_H$ has order $p-1$ if $p \nmid D$ or $(p-1)/2$ when $p|D$, if $p \geq 5$ (under our assumption: $p \nmid D$), the order of ξ is larger than 2.

For the moment, suppose that F is real. Then for complex conjugation c , we have $\det \varphi(c) = -1$, and hence, $\xi \xi^\delta(c) = -1$. This shows that $\xi(c) \neq \xi^\delta(c)$ if p is odd.

We now give an argument proving $\xi^\delta \neq \xi$ valid both imaginary and real F . Since $\xi \xi^\delta = \omega_p$, if $\xi = \xi^\delta$, we have $\omega_p = \xi^2$. Restrict these characters to the inertia group at I_p . By local class field theory, we may regard these characters as characters of O_p^\times for a prime factor $\mathfrak{p}|p$ in F . Here O is the integer ring of F . Since ξ has values in \mathbb{F}_p^\times , ξ factors through $(O/\mathfrak{p})^\times$. If $O/\mathfrak{p} \cong \mathbb{F}_p$ and $p \nmid D$, the identity $\xi^2 = \omega_p$ is impossible, because ω_p has order $p-1$ (if $p \nmid D$). If $O/\mathfrak{p} \cong \mathbb{F}_{p^2}$, then $\xi^2 = \omega_p$ implies ξ has order $2(p-1)$, which is impossible since ξ has values in \mathbb{F}_p^\times . Thus $\xi \neq \xi^\delta$ on $(O/\mathfrak{p})^\times$ again in this case. However $\xi \neq \xi^\delta$ on $(O/\mathfrak{p})^\times$ implies that ξ has values in \mathbb{F}_{p^2} not in \mathbb{F}_p ; so, this case actually never happens. Thus we conclude that the prime p has to split in F .

Thus if ξ is unramified at one of the prime factors \mathfrak{p} of p (\Leftarrow semi-stable reduction of E at p), we are in the p -ordinary case, and $\xi^{-1} \xi^\delta$ has order at least $p-1 \geq 4$. Even if ξ and ξ^δ both ramify at $\mathfrak{p}|p$, we choose a Dirichlet character ϕ such that $\phi|_{I_p} = \xi|_{I_p}$. Then $\varphi \otimes \phi^{-1}$ is p -ordinary. Suppose that $\xi \xi^{-\delta}$ is of order 2, then $\xi^4 = (\xi \xi^\delta)^2 (\xi \xi^{-\delta})^2 = \omega_p^2$, which is impossible if $p \equiv 1 \pmod{4}$, and still $\xi \xi^{-\delta}$ has order > 2 in this case. Thus φ satisfies (I4) and also the irreducibility condition over $\text{Gal}(F^S/\mathbb{Q}(\mu_p))$ (a condition of Theorem 4.1) if either E has semi-stable reduction at p or $p \equiv 1 \pmod{4}$ or $\xi \xi^{-\delta}$ ramifies at a prime different from p (see Proposition 4.3).

The condition $\det(\rho(c)) = -1$ (I5) is automatic in the elliptic curve case by the self-dual pairing $\langle \cdot, \cdot \rangle$ on $E[p]$. When ξ is unramified at one of prime factor \mathfrak{p} of p , we directly find $f \in S_2(\Gamma_1(N))$ by Theorem 4.1 such that $\rho_f \cong \varphi$ over H . When ξ and ξ^δ both ramify at

$\mathfrak{p}|p$, we find $g \in S_2(\Gamma_1(N'))$ such that $\rho_g \cong \phi \otimes \phi^{-1}$ over H . Then the automorphic twist $f = g \otimes \phi$ is associated to E .

We now assume that θ is not defined over F . Choose a nowhere vanishing differential $\omega \in H^0(E, \Omega_{E/F})$ (always possible). Then $\theta^* \omega^\delta = c\omega$ for $c \in \overline{\mathbb{Q}}$. For $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/F)$, $(\theta^\sigma)^* \omega^\delta = c^\sigma \omega$. Then $\theta^{-1} \circ \theta^\sigma = \frac{n}{m}$ for mutually prime integers m and n , because $\text{End}(E/\overline{\mathbb{Q}}) = \mathbb{Z}$. Thus $n^2 \deg(\theta) = m^2 \deg(\theta^\sigma)$; so, $m = \pm n$ by the fact: $\deg(\theta) = \deg(\theta^\sigma)$. Thus $\theta^\sigma = \pm \theta$, and hence $c^\sigma = \pm c$. Therefore, θ is defined over $F(c)$, which is at most a quadratic extension of F .

We have $(\theta \circ \theta^\delta)^* \omega^\delta = cc^\delta \omega^\delta$. By $\text{End}(E/\overline{\mathbb{Q}}) = \mathbb{Z}$, $\theta \circ \theta^\delta$ is an integer in $\text{End}_{\overline{\mathbb{Q}}}(E^\delta)$; hence, $cc^\delta \in \mathbb{Z}$ for any extension of δ to $\overline{\mathbb{Q}}$. Thus $\text{Gal}(F(c)/\mathbb{Q})$ is either isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ or $(\mathbb{Z}/2\mathbb{Z})$.

By our assumption now, we have $F(c) \neq F$. Consider $T : T_p(E) \cong T_p(E^\delta)$ defined by $T(x) = \delta(\theta(x))$. Then $T(hx) = \varepsilon(h)\delta h\delta^{-1}T(x)$ for $h \in H$, where $\varepsilon(h) = (c^h/c)$.

If we can find a finite order character $\eta : \text{Gal}(\overline{\mathbb{Q}}/F) \rightarrow \overline{\mathbb{Q}}^\times$ such that $\varepsilon = \eta^{\delta-1}$, then for $\phi = \phi \otimes \eta$, we find $T\phi = \phi^\delta T$. Thus once we find such η , the twist ϕ satisfies (I2).

We now show that η with $\varepsilon = \eta^{\delta-1}$ always exists. Let X be a number field. By class field theory, any continuous character of $\text{Gal}(\overline{\mathbb{Q}}/X)$ can be regarded as a continuous idele character: $C_X = X_{\mathbb{A}}^\times / X^\times \rightarrow \mathbb{T}$, where

$$\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}.$$

A given continuous character of C_X is of finite order if and only if it is trivial on the identity component of the infinite part F_∞^\times of $F_{\mathbb{A}}^\times$ (cf. [H99] Proposition II.1.2). By Artin reciprocity, any finite order character of C_X can be viewed as a Galois character of $\text{Gal}(\overline{\mathbb{Q}}/X)$ canonically. Looking at the exact sequence:

$$1 \rightarrow F^\times \rightarrow F_{\mathbb{A}}^\times \rightarrow C_F \rightarrow 1,$$

by Hilbert's theorem 90 applied to F^\times and $\text{Gal}(F/\mathbb{Q})$, we find

$$H^0(\text{Gal}(F/\mathbb{Q}), C_F) = C_{\mathbb{Q}}.$$

Thus the kernel of $\delta - 1 : x \mapsto x^{\delta-1}$ is given by $C_{\mathbb{Q}}$. A character $\psi : C_F \rightarrow \mathbb{T}$ is of the form $\psi = \eta^{\delta-1}$ if and only if ψ is trivial on $C_{\mathbb{Q}}$. Since $\text{Gal}(F(c)/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, we can write $F(c) = F[\sqrt{m}]$ for $m \in \mathbb{Z}$. Thus $\varepsilon = \mu \circ N_{F/\mathbb{Q}}$ for the quadratic character μ associated to $\mathbb{Q}[\sqrt{m}]/\mathbb{Q}$. This shows that $\varepsilon(x) = \mu(x x^\delta) = \mu(x^2) = 1$ for $x \in C_{\mathbb{Q}}$. Thus we can write $\varepsilon = \eta^{\delta-1}$ for a character $\eta : C_F \rightarrow \mathbb{T}$. To show that η can be chosen to be of finite order, we need to show that η restricted to the identity component of F_∞^\times can be chosen to be trivial.

Suppose that F is imaginary, and write $\eta_\infty(z) = |z|^s z^m$ ($z \in \mathbb{C}^\times$) for $m \in \mathbb{Z}$ and $s \in \mathbb{C}$. Since $\eta_\infty^{\delta-1} = 1$, we have $m = 0$. Thus multiplying η by $|\cdot|_{\mathbb{A}}^{-s/2}$, we may assume that η is of finite order.

Suppose that F is real. Then we have $\eta_\infty(x, x') = |x|^s (x/|x|)^u |x'|^t (x'/|x'|)^v$ for $(x, x') \in (\mathbb{R}^\times)^2$ ($s, t \in \sqrt{-1}\mathbb{R}$ and $u, v \in \mathbb{Z}/2\mathbb{Z}$). By $\eta^{\delta-1}(x, x') = \varepsilon_\infty(x, x') = (x/|x|)^w (x'/|x'|)^w$ for $w \in \mathbb{Z}/2\mathbb{Z}$. This shows that $s = t$ and $u + v = w$. Thus multiplying η again by $|\cdot|_{\mathbb{A}}^{-s}$, we may assume that η is of finite order. Thus we have basically shown the following facts:

- (E1) There exists a finite order continuous character η of $\text{Gal}(\overline{\mathbb{Q}}/F)$ such that $T_p(E) \otimes \eta$ satisfies (I2).
- (E2) We can choose η unramified outside a given finite set of primes which are unramified over F in the minimal field $M = F(c)$ of definition of $\theta : E \rightarrow E^\delta$.

We will leave to the reader to give the detail of the proof of (EI2), since we do not use it in the sequel.

By our construction, $T_p(E) \otimes \eta$ satisfies (I1-5) except possibly for (I4). We now prove (I4) for $T_p(E) \otimes \eta$. Note that we have an exact sequence of H -modules:

$$0 \rightarrow V(\xi) \rightarrow E[p] \rightarrow V(\varepsilon\xi^\delta) \rightarrow 0.$$

Thus $\varepsilon\xi\xi^\delta = \omega_p$. If $\xi\eta = (\xi\eta)^\delta$, then $\xi^{1-\delta} = \eta^{\delta-1} = \varepsilon$. This shows $\xi^2 = \omega_p$, which is impossible if $p \nmid D$ as we have already seen. We also conclude that p splits in F under this circumstance. Thus $\xi\eta \neq (\xi\eta)^\delta$. Since p splits in F , we can always find a Dirichlet character ϕ such that $\phi|_{I_{\mathfrak{p}}} = \eta|_{I_{\mathfrak{p}}}$ for the inertia group $I_{\mathfrak{p}}$ at \mathfrak{p} . Then replacing η by $\eta(\phi \circ N_{F/\mathbb{Q}})^{-1}$, we may assume that η is unramified at \mathfrak{p} . Then we know that the order of $\eta\xi|_{I_{\mathfrak{p}}}$ and $(\eta\xi)(\eta\xi)^{-\delta} = \varepsilon\xi\xi^{-\delta}$ are greater than 2 as before. Thus the extension of $\varphi \otimes \eta$ to G is residually irreducible over $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p))$ by Proposition 4.3.

Thus we have a cusp form $f \in S_2(\Gamma_1(N))$ such that $T_p(E) \otimes \eta \cong V(\rho_f)$ as H -modules. The abelian variety A_f associated to f in Shimura's sense has a factor isogenous to E over the field L such that $\eta : \text{Gal}(L/F) \cong \text{Im}(\eta)$. By definition $L \supset F(c)$. \square

Here is some remark on the above result:

1. If one could ease the irreducibility condition of $\overline{\rho}$ over $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p))$ in Theorem 2.1 to the absolutely irreducibility over $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, one can remove the semi-stability assumption at p for E from the above corollary and ease the assumption on p to $3 \leq p \nmid D$.
2. The base-change lift \widehat{f} of f as above to $GL(2)_{/F}$ (established by Jacquet [J]; see also [L]) is a cohomological cusp form. We write g for \widehat{f} if $F = F(c)$. When $F \neq F(c)$, we twist back $\widehat{f} \otimes \eta^{-1}$ and write it as g , which is the automorphic twist of \widehat{f} by the finite order Hecke character η . The above proof shows that the cusp form g is associated to $T_p(E)$ restricted to H . This shows the existence of a cusp form g on $GL_2(F_{\mathbb{A}})$ associated to $E_{/F}$.

Here is how to find a lot of examples of Elliptic \mathbb{Q} -curves as in the above corollary. Pairs (E, C) of an elliptic curve and a cyclic subgroup of order p is classified by the modular curve $X_0(p)$. For each point $y \in X_0(p)(\overline{\mathbb{Q}})$ represented by (E, C) , $\mathbb{Q}(y)$ is characterized as the field of moduli of the pair (E, C) defined over $\overline{\mathbb{Q}}$: $\mathbb{Q}(y)$ is the fixed field of

$$G(E, C) = \{ \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid (E^\sigma, C^\sigma) \cong (E, C) \text{ over } \overline{\mathbb{Q}} \},$$

Take a point y with $\mathbb{Q}(y) = F$. As is well known, we can choose a model of E defined over F . For this model, we have the following two possibilities:

1. (E, C) is defined over F ;
2. C is defined over a $(2, 2)$ -extension of \mathbb{Q} containing F .

These two cases are covered by Corollary 5.1 if $5 \leq p \nmid D$ and $\text{End}(E/\overline{\mathbb{Q}}) = \mathbb{Z}$. Thus the main point is to find $y \in X_0(p)$ quadratic over \mathbb{Q} . The functorial correspondence $(E, C) \mapsto (E/C, E[p]/C)$ induces an involution τ of $X_0(p)$. We make a quotient curve $X^*(p) = X_0(p)/\langle \tau \rangle$. If $x \in X^*(p)(\mathbb{Q})$ and $y \in X_0(p)$ is over x , $\mathbb{Q}(y)$ is either \mathbb{Q} or a quadratic extension F .

Here is a list of primes $p \geq 5$ for which $X^*(p) \cong \mathbf{P}^1_{/\mathbb{Q}}$:

$$p = 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71.$$

By a work of Mazur ([M1] and [M2]) if $p \geq 11$ in the above list, there are no non-CM non-cuspidal rational points of $X_0(p)$ (actually there is at most one non-cuspidal \mathbb{Q} -rational point in these cases). Thus all points on $X_0(p)$ over infinitely many (non-CM) \mathbb{Q} -rational points of $X^*(p)$ yield examples of type (1) or (2).

Even if the genus of $X_0(p)$ is 0, by Hilbert's irreducibility theorem, for infinitely many $x \in X^*(\mathbb{Q})$, we find $\mathbb{Q}(y)$ quadratic over \mathbb{Q} (for $y \in X_0(p)$ over x) as explicitly seen by Shimura in [S] for $p = 5$.

Here are some concluding remarks:

1. We could have stated the result for \mathbb{Q} -HBAV (or possibly rank 2 \mathbb{Q} -motives) in place of elliptic \mathbb{Q} -curves. In the case of \mathbb{Q} -HBAV, we need to start with \mathbb{Q} -HBAV A defined over a quadratic field F/\mathbb{Q} with an isogeny $\theta: A \rightarrow A^\delta$ and assume the HBAV-version of the assumption of the corollary and that A has semi-stable reduction at p (this last assumption could presumably be removed). Then A is a factor of $J_1(N)$ for a suitable N over an abelian extension L/F .
2. Almost all modular compatible systems of quadratic Neben types (up to character twists) satisfies the conditions (I1-5) and the assumptions of Theorem 4.1 for an odd prime p . In particular, when weight is two, every geometric factor of modular jacobian is a \mathbb{Q} -HBAV or its quaternionic analog. In the case of higher weight, modular compatible system is obtained from motivic analogs of \mathbb{Q} -HBAV, which we call "rank 2 \mathbb{Q} -motive".
3. If f is a Hecke eigenform with quadratic Neben type, its field of Hecke eigenvalues is a CM field $\mathbb{Q}(f)$ over a totally real field $\mathbb{Q}_+(f)$, as long as f does not have complex multiplication ($\iff \rho_f$ is non-dihedral). In this case, the relative different of $\mathbb{Q}(f)$ over $\mathbb{Q}_+(f)$ is spanned by $Ob(\rho_f|_H)$. Strictly speaking, we should have said that the relative different of the order of $\mathbb{Q}_p(f)$ generated by Hecke eigenvalues over the integer ring of the closure of $\mathbb{Q}_+(f)$ in $\mathbb{Q}_p(f)$ is spanned by $Ob(\rho_f|_H)$, where $\mathbb{Q}_p(f)$ is the subfield of $\overline{\mathbb{Q}}_p$ generated over \mathbb{Q}_p by $\text{Tr}(\rho_f)$. For a given f , there always exists a prime p for which the relative different is non-trivial. Therefore we could say that almost all f with quadratic Neben type can be included into the frame of our theory. We said "almost all", because we still have some problem if the prime p is small, like, 2 and 3, or dividing D .
4. The above arguments can be basically carried out for Hilbert modular forms in place of elliptic modular forms using Fujiwara's generalization of Theorem 2.1 to Hilbert modular case (cf. [HM97]).

REFERENCES

- [CV] Sheena Cho and Vinayak Vatsal, Deformation rings for induced representations, preprint, 1999
- [D] F. Diamond, On deformation rings and Hecke rings, *Ann. of Math.* **144** (1996), 137–166
- [F] G. Faltings, Endlichkeitssätze für abelsche varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366 (English translation in "Arithmetic Geometry" edited by G. Cornell and J. H. Silverman, Springer, 1986)
- [H98] H. Hida, Global quadratic units and Hecke algebras, *Documenta Math.* **3** (1998), 273–284
- [H99] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge University Press, Cambridge, England, 1999
- [H00] H. Hida, *Geometric Modular Forms and Elliptic Curves*, to be published by World Scientific Publishing Company, Singapore
- [HM97] H. Hida and Y. Maeda, Non-abelian base change for totally real fields, Olga Taussky Todd memorial issue, *Pacific Journal of Math.* (1997), 189–217
- [J] H. Jacquet, *Automorphic forms on $GL(2)$, II*, Lecture notes in Math. **278**, Springer, 1972

- [L] R. P. Langlands, *Base change for $GL(2)$* , Annals of Math. Studies **96**, Princeton University Press, 1980
- [M1] B. Mazur, Modular curves and the Eisenstein ideal, Publ. Math. I.H.E.S. **47** (1977), 33–186
- [M2] B. Mazur, Rational isogenies of prime degree, Invent. Math. **44** (1978), 129–162
- [N] L. Nyssen, Pseudo-représentations, Math. Ann. **306** (1996), 257–283
- [S] G. Shimura, Class fields over real quadratic fields and Hecke operators, Ann of Math. **95** (1972), 130–190
- [TW] R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke modules, Ann. of Math. **142** (1995), 553–572
- [W] A. Wiles, Modular elliptic curves and Fermat’s last theorem, Ann. of Math. **142** (1995), 443–551