On icosahedral Artin representations II

Richard Taylor [1]
Department of Mathematics,
Harvard University,
Cambridge,
MA 02138,
U.S.A.

April 4, 2000

[1] Partially supported by NSF Grant DMS-9702885

Introduction

This paper is a sequel to [BDST]. In that paper we proved the Artin conjecture for certain odd icosahedral representations of $\mathrm{Gal}(\mathbb{Q}^{ac}/\mathbb{Q})$ by proving that they were modular. In this paper we will prove a variant of this result with different local hypotheses. Neither set of hypotheses is strictly weaker/stronger than the other. The key innovation in this paper is to work with the prime 5 rather than the prime 2. To do this we have to prove Serre's conjecture for many continuous representations $\overline{\rho} : \mathrm{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \to GL_2(\mathbb{F}_5^{ac})$ which have projective image A_5. (Note that such representations do not have cyclotomic determinant.) The key to doing this is to combine base change arguments with a beautiful method of Ramakrishna (see [R]) and with an extension to totally real fields of results of Wiles and of the author and Wiles ([W],[TW]). (Such a generalisation can be found in [SW2], however we make no use of the main innovation of [SW2]. There are two key ingredients in the result we do use. One is due independently to Diamond [Dia] and Fujiwara [F], the other is due to Skinner and Wiles [SW1]. Results along the lines of the one we use have been previously announced by Fujiwara.) We no longer have to make appeal to the main results of [SBT] and [Dic], but we do still make essential use of [BT].

More precisely an example of our main result is the following.

Theorem A *Let $\rho : \mathbb{G}_{\mathbb{Q}} \to GL_2(\mathbb{C})$ be an irreducible continuous representation with $\det \rho(c) = -1$ (where c denotes a complex conjugation). Suppose moreover that if the projective image of ρ is isomorphic to A_5 then the projective image of the inertia group at 3 has odd order and the projective image of the decomposition group at 5 is unramified of order 2. Then ρ is modular and its Artin L-function, $L(\rho, s)$, is entire.*

This paper is organised as follows. In the first section we prove a slight extension of one of the main results of [R]. We emphasise that the method is entirely Ramakrishna's, we simply make some minor technical improvements. In the second section we apply this result to prove our main theorems.

Notation

If K is a perfect field we will let K^{ac} denote its algebraic closure and G_K denote its absolute Galois group $\mathrm{Gal}(K^{ac}/K)$. If moreover p is a prime number different from the characteristic of K then we will let $\epsilon_p : G_K \to \mathbb{Z}_p^\times$ denote the p-adic cyclotomic character and ω_p the Teichmuller lift of $\epsilon_p \bmod p$. If V is a $\mathbb{Z}_p[G_K]$ module we will write $V(n)$ for $V \otimes_{\mathbb{Z}_l} \mathbb{Z}_l(\epsilon_p^n)$. If K is a local field we will let W_K denote the Weil group of K. If K is a number field and x is a finite place of K we will write G_x for a decomposition group above x, I_x for the inertia subgroup of G_x and Frob_x for an arithmetic Frobenius element in G_x/I_x. We will also let $\mathcal{O}_K$ denote the integers of K and $k(x)$ denote the residue field of $\mathcal{O}_K$ at x. We will let c denote complex conjugation on $\mathbb{C}$.

We will write μ_N for the group scheme of N^{th} roots of unity. We will write $W(k)$ for the Witt vectors of k. We will write $\mathrm{ad}^0\rho$ for the trace zero submodule of the adjoint $\mathrm{Hom}(\rho,\rho)$ of ρ.

Suppose that E/K is an elliptic curve. If m is a positive integer prime to the characteristic of K we will write $\overline{\rho}_{E,m}$ for the representation of G_K on $E[m](K^{ac})$. If l is rational prime coprime to the characteristic of K, we will write T_lE for the l-adic Tate module of E, V_lE for $T_lE \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\rho_{E,l}$ for the representation of G_K on V_lE.

Suppose that F is a totally real number field and that π is an algebraic cuspidal automorphic representation of $GL_2(\mathbb{A}_F)$ with field of definition (or coefficients) $M \subset \mathbb{C}$. In some cases, including the cases that π_∞ is regular and the case π_∞ is weight $(1,...,1)$, then it is known that M is a CM number field and that for each prime λ of $\mathcal{O}_M$ there is a continuous irreducible representation

$$\rho_{\pi,\lambda} : G_F \to GL_2(M_\lambda)$$

canonically associated to π. (See [Ta] for details.) We may always conjugate $\rho_{\pi,\lambda}$ so that it is valued in $GL_2(\mathcal{O}_{M,\lambda})$ and then reduce it to get a continuous representation $G_F \to GL_2(\mathcal{O}_M/\lambda)$. If for one such choice of conjugate the resulting representation is irreducible then it is independent of the choice of conjugate and we will denote it $\overline{\rho}_{\pi,\lambda}$.

1 Generalisation of a result of Ramakrishna.

In this section we give a slight generalisation of a result of Ramakrishna [R]. We stress that both the result and the arguments we use are essentially his.

In this section we will let l denote an odd rational prime, ϵ denote ϵ_l and ω denote ω_l. We will also let k denote a finite extension of $\mathbb{F}_l$ and $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(k)$ a continuous representation such that $\overline{\rho}(G_{\mathbb{Q}})$ is insoluble. Define a positive integer n as follows. If $\overline{\rho}|_{G_l}$ is absolutely reducible set $n = 1$. Otherwise choose $1 \leq n \leq l-1$ such that

$$\overline{\rho}|_{I_l} \sim \psi^{n+(l+1)m} \oplus \psi^{nl+(l+1)m}$$

(over k^{ac}) where ψ is a fundamental character of level 2 (see [S]).

Let S denote a finite set of rational primes which contains l and all primes where $\overline{\rho}$ is ramified. We will let G_S denote the Galois group of the maximal extension of $\mathbb{Q}$ which is unramified outside S. Thus $\overline{\rho}$ factors through G_S. By a *deformation* of $\overline{\rho}$ (resp. $\overline{\rho}|_{G_v}$) we shall mean a complete noetherian local ring $(R, \mathfrak{m})$ with residue field k and a continuous representation $\rho : G_S \to GL_2(R)$ (resp. $\rho : G_v \to GL_2(R)$) such that $(\rho \bmod \mathfrak{m}) = \overline{\rho}$ and $\epsilon^{-n} \det \rho$ has finite order prime to l. In the global case we will write *S-deformation* if we wish to emphasise the choice of set S.

Now suppose that for each $v \in S$ we are given a pair $(\mathcal{C}_v, L_v)$ where $\mathcal{C}_v$ is a collection of deformations of $\overline{\rho}|_{G_v}$ and L_v is a subspace of $H^1(G_v, \mathrm{ad}^0\overline{\rho})$ satisfying the following properties.

P1. $(k, \overline{\rho}|_{G_v}) \in \mathcal{C}_v$.

P2. $\mathcal{C}_v$ is closed under conjugation by elements of $1 + M_2(\mathfrak{m})$.

P3. If $(R, \rho) \in \mathcal{C}_v$ and $f : R \to S$ is a morphism of complete local noetherian rings which induces an isomorphism on residue fields then $(S, f \circ \rho) \in \mathcal{C}_v$.

P4. Suppose that (R_1, ρ_1) and $(R_2, \rho_2) \in \mathcal{C}_v$, that I_1 (resp. I_2) is an ideal of R_1 (resp. R_2) and that $\phi : R_1/I_1 \xrightarrow{\sim} R_2/I_2$ is an isomorphism such that $\alpha(\rho_1 \bmod I_1) = \rho_2 \bmod I_2$. Let R_3 be the subring of $R_1 \oplus R_2$ consisting of pairs with the same image in $R_1/I_1 \xrightarrow{\sim} R_2/I_2$. Then $(R_3, \rho_1 \oplus \rho_2) \in \mathcal{C}_v$.

P5. If (R, ρ) is a deformation of $\overline{\rho}|_{G_v}$ and if $\{I_i\}$ is a nested sequence of ideals in R with intersection (0) such that each $(R/I_i, \rho) \in \mathcal{C}_v$ then $(R, \rho) \in \mathcal{C}_v$.

P6. Suppose $(R, \mathfrak{m})$ is a complete noetherian local ring with residue field k and suppose that I is an ideal of R with $\mathfrak{m}I = (0)$. If $(R/I, \rho) \in \mathcal{C}_v$ then there is a deformation $\widetilde{\rho}$ of $\overline{\rho}|_{G_v}$ to R such that $(R, \widetilde{\rho}) \in \mathcal{C}_v$ and $(\widetilde{\rho} \bmod I) = \rho$.

P7. Suppose that $((R, \mathfrak{m}), \rho_1)$ and $((R, \mathfrak{m}), \rho_2)$ are deformations of $\overline{\rho}$ with $((R, \mathfrak{m}), \rho_1) \in \mathcal{C}_v$, and that I is an ideal of R with $\mathfrak{m}I = (0)$ and $(\rho_1 \bmod I) = (\rho_2 \bmod I)$. Thus $\sigma \mapsto \rho_2(\sigma)\rho_1(\sigma)^{-1} - 1$ defines an element of $H^1(G_v, \mathrm{ad}^0\overline{\rho}) \otimes_k I$ which we shall denote $[\rho_2 - \rho_1]$. Then $[\rho_2 - \rho_1] \in L_v \otimes_k I$ if and only if $(R, \rho_2) \in \mathcal{C}_v$.

Let us next give some examples of such pairs $(\mathcal{C}_v, L_v)$.

E1. Suppose that $v \neq l$ and that $l \nmid \#\overline{\rho}(I_v)$. Take $\mathcal{C}_v$ to be the class of lifts ρ of $\overline{\rho}|_{G_v}$ which factor through $G_v/(I_v \cap \ker \overline{\rho})$ and take L_v to be $H^1(G_v/I_v, (\mathrm{ad}^0\overline{\rho})^{I_v})$. Note that

- $H^2(G_v/(I_v \cap \ker \overline{\rho}), \mathrm{ad}^0\overline{\rho}) \cong H^2(G_v/I_v, (\mathrm{ad}^0\overline{\rho})^{I_v}) = (0)$,
- $H^1(G_v/(I_v \cap \ker \overline{\rho}), \mathrm{ad}^0\overline{\rho}) = L_v \subset H^1(G_v, \mathrm{ad}^0\overline{\rho})$
- and $\dim L_v = \dim H^0(G_v, \mathrm{ad}^0\overline{\rho})$.

E2. Suppose that $v = 2$, $l = 3$ and that $(\mathrm{ad}^0\overline{\rho})(G_v) \cong A_4$. Take $\mathcal{C}_v$ to be the class of lifts ρ of $\overline{\rho}|_{G_v}$ which factor through $G_v/(I_v \cap \ker \overline{\rho})$ and take L_v to be $H^1(G_v/I_v, (\mathrm{ad}^0\overline{\rho})^{I_v})$. Note that

- $H^i(\overline{\rho}(I_v), \mathrm{ad}^0\overline{\rho}) = (0)$ for all $i \geq 0$,
- $H^2(G_v/(I_v \cap \ker \overline{\rho}), \mathrm{ad}^0\overline{\rho}) = (0)$,
- $H^1(G_v/(I_v \cap \ker \overline{\rho}), \mathrm{ad}^0\overline{\rho}) = (0) = L_v \subset H^1(G_v, \mathrm{ad}^0\overline{\rho})$
- and $\dim L_v = \dim H^0(G_v, \mathrm{ad}^0\overline{\rho}) = 0$.

E3. Suppose that with respect to some basis e_1, e_2 of k^2 the restriction $\overline{\rho}|_{G_v}$ has the form

$$\begin{pmatrix} \epsilon\overline{\chi} & * \\ 0 & \overline{\chi} \end{pmatrix}$$

and that either $v \not\equiv 1 \bmod l$ or $l | \#\overline{\rho}(G_v)$. Take $\mathcal{C}_v$ to be the class of deformations ρ of $\overline{\rho}|_{G_v}$ of the form

$$\begin{pmatrix} \epsilon\chi & * \\ 0 & \chi \end{pmatrix}$$

where χ lifts $\overline{\chi}$ and take L_v to be the image of

$$H^1(G_v, \mathrm{Hom}\,(ke_2, ke_1)) \longrightarrow H^1(G_v, (\mathrm{ad}^0\overline{\rho})).$$

If I and R are as in the statement of property P6 then

$$H^0(G_v, R^\vee) \longrightarrow H^0(G_v, I^\vee)$$

is surjective, so that

$$H^2(G_v, I(1)) \longrightarrow H^2(G_v, R(1))$$

is injective and

$$H^1(G_v, R(1)) \longrightarrow H^1(G_v, (R/I)(1))$$

is surjective. Thus $\mathcal{C}_v$ has property P6. Note also that

$$\begin{aligned}
& \dim L_v \\
= \; & \dim H^1(G_v, \mathrm{Hom}\,(ke_2, ke_1)) - \dim H^0(G_v, (\mathrm{ad}\,^0\overline{\rho})/\mathrm{Hom}\,(ke_2, ke_1)) \\
& + \dim H^0(G_v, \mathrm{ad}\,^0\overline{\rho}) - \dim H^0(G_v, \mathrm{Hom}\,(ke_2, ke_1)) \\
= \; & \delta_{vl} + 1 + \dim H^0(G_v, \mathrm{Hom}\,(ke_2, ke_1)) - 1 + H^0(G_v, \mathrm{ad}\,^0\overline{\rho}) \\
& - H^0(G_v, \mathrm{Hom}\,(ke_2, ke_1)) \\
= \; & \delta_{vl} + \dim H^0(G_v, \mathrm{ad}\,^0\overline{\rho}),
\end{aligned}$$

where $\delta_{vl} = 1$ if $v = l$ and 0 otherwise.

E4. Suppose $v = l$ and that with respect to some basis e_1, e_2 of k^2 $\overline{\rho}|_{G_l}$ has the form

$$\begin{pmatrix} \epsilon\overline{\chi}_1 & * \\ 0 & \overline{\chi}_2 \end{pmatrix}.$$

Suppose also that $\overline{\chi}_1 \neq \overline{\chi}_2$ and that if $\epsilon\overline{\chi}_1 = \overline{\chi}_2$ then $\overline{\rho}_{G_l}$ is wildly ramified. Take $\mathcal{C}_v$ to consist of all deformations of the form

$$\begin{pmatrix} \epsilon\chi_1 & * \\ 0 & \chi_2 \end{pmatrix},$$

where χ_1 and χ_2 are tamely ramified and χ_2 lifts $\overline{\chi}_2$. Also take L_v to be the image in $H^1(G_v, (\mathrm{ad}\,^0\overline{\rho}))$ of the kernel of the natural map

$$\begin{array}{c} H^1(G_v, \mathrm{Hom}\,(ke_2, ke_1) \oplus ((\mathrm{Hom}\,(ke_1, ke_1) \oplus \mathrm{Hom}\,(ke_2, ke_2)) \cap \mathrm{ad}\,^0\overline{\rho})) \\ \downarrow \\ H^1(I_v, ((\mathrm{Hom}\,(ke_1, ke_1) \oplus \mathrm{Hom}\,(ke_2, ke_2)) \cap \mathrm{ad}\,^0\overline{\rho})). \end{array}$$

If I and R are as in the statement of property P6 then

$$H^0(G_v, I^\vee(\chi_2/\chi_1) = (0),$$

so that $H^2(G_v, I(\epsilon\chi_1/\chi_2)) = (0)$ and

$$H^1(G_v, R(\epsilon\chi_1/\chi_2)) \longrightarrow H^1(G_v, (R/I)(\epsilon\chi_1/\chi_2))$$

is surjective. Thus $\mathcal{C}_l$ has property P6. One can also check that (see for instance tables 2 and 3 in [R])

$$\dim L_l = 1 + \dim H^0(G_l, \mathrm{ad}\,^0\overline{\rho}).$$

E5. Suppose that $v = l$ and that for some $1 \leq n \leq l-1$ we have

$$\overline{\rho}|_{I_l} \sim \psi^{n+(l+1)m} \oplus \psi^{nl+(l+1)m}$$

where ψ is a fundamental character of level 2. Take $\mathcal{C}_l$ to be the collection of lifts $\rho : G_l \to GL_2(R)$ such that $\rho \otimes \omega^{-n}$ is crystalline (in the sense that it is the inverse limit of crystalline representations over Artinian quotients of R). A calculation using the theory of Fontaine and Lafaille shows that $\mathcal{C}_l$ has property P6 and that there is a suitable L_l with $\dim L_l = 1$. (This calculation basicly goes back to Ramakrishna's thesis, see for instance the paragraph before proposition 2 of [R].)

Recall that the trace gives a perfect pairing $\mathrm{ad}^0\overline{\rho} \times \mathrm{ad}^0\overline{\rho} \to k$. By Tate local duality this induces a perfect pairing

$$H^1(G_v, \mathrm{ad}^0\overline{\rho}) \times H^1(G_v, (\mathrm{ad}^0\overline{\rho})(1)) \longrightarrow k.$$

We will let $L_v^\perp$ denote the annihilator of L_v under this pairing. We will let $H^1_{\{L_v\}}(G_S, \mathrm{ad}^0\overline{\rho})$ denote the preimage under the restriction map

$$H^1(G_S, \mathrm{ad}^0\overline{\rho}) \longrightarrow \bigoplus_{v\in S} H^1(G_v, \mathrm{ad}^0\overline{\rho})$$

of $\bigoplus_{v\in S} L_v$. Similarly we will let $H^1_{\{L_v^\perp\}}(G_S, (\mathrm{ad}^0\overline{\rho})(1))$ denote the preimage under the restriction map

$$H^1(G_S, (\mathrm{ad}^0\overline{\rho})(1)) \longrightarrow \bigoplus_{v\in S} H^1(G_v, (\mathrm{ad}^0\overline{\rho})(1))$$

of $\bigoplus_{v\in S} L_v^\perp$. Ramakrishna's first observes the following.

Lemma 1.1 *Keep the above notation and assumptions. If*

$$H^1_{\{L_v^\perp\}}(G_S, (\mathrm{ad}^0\overline{\rho})(1)) = (0)$$

then we can find an S-deformation $(W(k), \rho)$ of $\overline{\rho}$ such that for all $v \in S$ the restriction $(W(k), \rho|_{G_v}) \in \mathcal{C}_v$.

Proof: The Poitou-Tate exact sequence gives us an exact sequence

$$\begin{array}{ccccc} H^1(G_s, \mathrm{ad}^0\overline{\rho}) & \longrightarrow & \bigoplus_{v\in S} H^1(G_v, \mathrm{ad}^0\overline{\rho})/L_v & \longrightarrow & H^1_{\{L_v^\perp\}}(G_S, (\mathrm{ad}^0\overline{\rho})(1))^\vee \\ & & & & \downarrow \\ & & \bigoplus_{v\in S} H^2(G_v, \mathrm{ad}^0\overline{\rho}) & \longleftarrow & H^2(G_S, \mathrm{ad}^0\overline{\rho}) \end{array}$$

(see for instance the proof of theorem 2.18 of [DDT]). Thus we see that

$$H^1(G_S, \mathrm{ad}^0\overline{\rho}) \twoheadrightarrow \bigoplus_{v\in S} H^1(G_v, \mathrm{ad}^0\overline{\rho})/L_v$$

and

$$H^2(G_S, \mathrm{ad}^0\overline{\rho}) \hookrightarrow \bigoplus_{v\in S} H^2(G_v, \mathrm{ad}^0\overline{\rho}).$$

Now we recursively look for S-deformations $(W(k)/l^m, \rho_m)$ of $\overline{\rho}$ such that for all $v \in S$ we have $(W(k)/l^m, \rho_m|_{G_v}) \in \mathcal{C}_v$. For $m = 1$ there is nothing to prove. In general, for all $v \in S$ we can lift $\rho_{m-1}|_{G_v}$ to a continuous homomorphism $\rho_v : G_v \to GL_2(W(k)/l^m)$. By injectivity of the restriction map on H^2's this means that we can lift ρ_{m-1} to a continuous homomorphism $\rho : G_S \to GL_2(W(k)/l^m)$. By surjectivity of the map on H^1's we may find a class $\phi \in H^1(G_S, \mathrm{ad}^0\overline{\rho})$ mapping to

$$([\rho|_{G_v} - \rho_v])_{v\in S} \in \bigoplus_{v\in S} H^1(G_v, \mathrm{ad}^0\overline{\rho})/L_v.$$

Thus we may find a second lifting ρ_m of ρ_{m-1} to $W(k)/l^m$ such that for all $v \in S$ we have $(W(k)/l^m, \rho_m|_{G_v}) \in \mathcal{C}_v$. The lemma follows. $\square$

In fact under these conditions essentially the same argument shows that the universal S-deformation of $\overline{\rho}$ of type $\mathcal{C}_v$ for all $v \in S$ is a power series ring over $W(k)$ in $\dim H^1_{\{L_v\}}(G_S, \mathrm{ad}^0\overline{\rho})$ variables.

Ramakrishna's main innovation is the following result which gives conditions under which the hypotheses of the last lemma can be achieved.

Lemma 1.2 *Let $\overline{\rho}$, S, $\{(\mathcal{C}_v, L_v)\}$ be as above and suppose that*

$$\sum_{v\in S} \dim L_v \geq \sum_{v\in S\cup\{\infty\}} \dim H^0(G_v, \mathrm{ad}^0\overline{\rho}).$$

Then we can find a finite set of rational primes $T \supset S$ and data $(\mathcal{C}_v, L_v)$ for $v \in T - S$ satisfying the above conditions P1-P7 and such that

$$H^1_{\{L_v^\perp\}}(G_T, (\mathrm{ad}^0\overline{\rho})(1)) = (0).$$

Proof: Suppose first that $l = 5$ and $\mathrm{ad}^0\overline{\rho}(G_{\mathbb{Q}}) \cong A_5$, because in this case we will require a little extra argument. Choose $w \notin S$ such that $w \equiv 1 \bmod 5$ and $\mathrm{ad}^0\overline{\rho}(\mathrm{Frob}_w)$ has order 5. Adding w to S with the pair $(\mathcal{C}_w, L_w)$ as in example E3, we see that in this case we may assume that

$$H^1_{\{L_v\}}(G_S, \mathrm{ad}^0(\overline{\rho})) \cap H^1(\mathrm{ad}^{\overline{\rho}}(G_{\mathbb{Q}}), \mathrm{ad}^{\overline{\rho}}) = (0).$$

(For if ϕ lies in this intersection and is non-zero then ϕ restricts to a non-zero element of $H^1(G_w/I_w, \mathrm{ad}^0\overline{\rho})$, while

$$H^1(G_w/I_w, \mathrm{ad}^0\overline{\rho}) \cap L_w = (0).)$$

Now return to the general case. Suppose that

$$0 \neq \phi \in H^1_{\{L_v^\perp\}}(G_S, (\mathrm{ad}^0\overline{\rho})(1)).$$

We will show below that we can find a prime $w \notin S$ and $(\mathcal{C}_w, L_w)$ satisfying properties P1-P7 and such that

- $\dim L_w = \dim H^1(G_w/I_w, \mathrm{ad}^0\overline{\rho})$,
- $H^1_{\{L_v\}}(G_s, \mathrm{ad}^0\overline{\rho}) \twoheadrightarrow H^1(G_w/I_w, \mathrm{ad}^0\overline{\rho})$
- and ϕ does not map to zero in $H^1(G_w, (\mathrm{ad}^0\overline{\rho})(1))/L_w^\perp$.

Suppose for a moment that we have done this. We have an injection

$$H^1_{\{L_v^\perp\}}(G_S, (\mathrm{ad}^0\overline{\rho})(1)) \hookrightarrow H^1_{\{L_v^\perp\}\cup\{H^1(G_w,(\mathrm{ad}^0\overline{\rho})(1))\}}(G_{S\cup\{w\}}, (\mathrm{ad}^0\overline{\rho})(1))$$

and a formula of Wiles (see for instance theorem 2.18 of [DDT]) tells us that

$$\begin{array}{l} \#H^1_{\{L_v^\perp\}\cup\{H^1(G_w,(\mathrm{ad}^0\overline{\rho})(1))\}}(G_{S\cup\{w\}}, (\mathrm{ad}^0\overline{\rho})(1)) = \\ \#H^1_{\{L_v^\perp\}}(G_S, (\mathrm{ad}^0\overline{\rho})(1))\#\mathrm{coker}\,(H^1_{\{L_v\}}(G_S, \mathrm{ad}^0\overline{\rho}) \to H^1(G_w/I_w, \mathrm{ad}^0\overline{\rho})). \end{array}$$

Thus in our case

$$H^1_{\{L_v^\perp\}}(G_S, (\mathrm{ad}^0\overline{\rho})(1)) = H^1_{\{L_v^\perp\}\cup\{H^1(G_w,(\mathrm{ad}^0\overline{\rho})(1))\}}(G_{S\cup\{w\}}, (\mathrm{ad}^0\overline{\rho})(1))$$

and so we get a left exact sequence

$$\begin{array}{ccccc} (0) & \longrightarrow & H^1_{\{L_v^\perp\}}(G_{S\cup\{w\}}, (\mathrm{ad}^0\overline{\rho})(1)) & \longrightarrow & H^1_{\{L_v^\perp\}}(G_S, (\mathrm{ad}^0\overline{\rho})(1)) \\ & & & & \downarrow \\ & & & & H^1(G_w, (\mathrm{ad}^0\overline{\rho})(1))/L_w^\perp. \end{array}$$

Thus

$$\phi \notin H^1_{\{L_v^\perp\}}(G_{S\cup\{w\}}, (\mathrm{ad}^0\overline{\rho})(1)) \subset H^1_{\{L_v^\perp\}}(G_S, (\mathrm{ad}^0\overline{\rho})(1))$$

and arguing recursively the lemma will follow.

We now turn to the proof of the existence of a prime $w \notin S$ and a pair $(\mathcal{C}_w, L_w)$ with the above properties. In fact it suffices to show that if $0 \neq \phi \in H^1_{\{L_v^\perp\}}(G_S, (\mathrm{ad}^0\overline{\rho})(1))$ and $0 \neq \psi \in H^1_{\{L_v\}}(G_S, (\mathrm{ad}^0\overline{\rho})(1))$, then we can find a prime $w \notin S$ and $(\mathcal{C}_w, L_w)$ satisfying properties P1-P7 and such that

- $\dim H^1(G_w/I_w, \mathrm{ad}^0\overline{\rho}) = \dim L_w = 1$,
- ψ does not map to zero in $H^1(G_w/I_w, \mathrm{ad}^0\overline{\rho})$
- and ϕ does not map to zero in $H^1(G_w, (\mathrm{ad}^0\overline{\rho})(1))/L_w^\perp$.

(To see this note that by the assumption of the lemma and by Wiles' formula (see for instance theorem 2.18 of [DDT]) we have

$$\dim H^1_{\{L_v\}}(G_s, \mathrm{ad}^0\overline{\rho}) \geq \dim H^1_{\{L_v^\perp\}}(G_s, (\mathrm{ad}^0\overline{\rho})(1)),$$

so that if $H^1_{\{L_v^\perp\}}(G_s, (\mathrm{ad}^0\overline{\rho})(1)) \neq (0)$ then we can find

$$0 \neq \psi \in H^1_{\{L_v\}}(G_S, (\mathrm{ad}^0\overline{\rho})(1)).)$$

Let $K/\mathbb{Q}$ be the field generated by a primitive l^{th} root of unity and by the fixed field of $\ker(\mathrm{ad}^0\overline{\rho})$. Note that

- $H^1(\mathrm{Gal}\,(K/\mathbb{Q}), \mathrm{ad}^0\overline{\rho}) = (0)$,
- $H^1(\mathrm{Gal}\,(K/\mathbb{Q}), (\mathrm{ad}^0\overline{\rho})(1)) = (0)$
- and there is an element $\sigma \in \mathrm{Gal}\,(K/\mathbb{Q})$ such that $\mathrm{ad}^0\overline{\rho}(\sigma)$ has an eigenvalue $\epsilon(\sigma) \not\equiv 1 \bmod l$.

(This is a straightforward exercise using the following facts.

- $\mathrm{ad}^0\overline{\rho}(G_\mathbb{Q}) \cong A_5$, $PSL_2(\mathbb{F}_{l^r})$ or $PGL_2(\mathbb{F}_{l^r})$ for some $r \in \mathbb{Z}_{>0}$.
- If l is an odd prime, $r \in \mathbb{Z}_{>0}$ and $l^r \neq 5$ then $H^1(PSL_2(\mathbb{F}_{l^r}), \mathrm{ad}^0) = (0)$.
- $H^1(PGL_2(\mathbb{F}_5), \mathrm{ad}^0) = (0)$.
- In the case $l = 5$ and $\mathrm{ad}^0\overline{\rho}(G_\mathbb{Q}) \cong A_5$, we have seen that we may assume that
$$H^1_{\{L_v\}}(G_S, \mathrm{ad}^0(\overline{\rho})) \cap H^1(\mathrm{ad}^{\overline{\rho}}(G_\mathbb{Q}), \mathrm{ad}^{\overline{\rho}}) = (0).)$$

Let $\widetilde{\sigma}$ be a lift of σ to $G_\mathbb{Q}$. Then $\overline{\rho}(\widetilde{\sigma})$ has two distinct eigenevalues $\alpha, \beta \in k$ with $\alpha/\beta = \epsilon(\sigma)$. Let e_α and e_β denote corresponding eigenvectors. We get a decomposition

$$\begin{aligned}\mathrm{ad}^0\overline{\rho} &= \mathrm{Hom}\,(ke_\beta, ke_\alpha) \oplus \\ &\quad ((\mathrm{Hom}\,(ke_\alpha, ke_\alpha) \oplus \mathrm{Hom}\,(ke_\beta, ke_\beta)) \cap \mathrm{ad}^0\overline{\rho}) \oplus \mathrm{Hom}\,(ke_\alpha, ke_\beta).\end{aligned}$$

Let ϕ and ψ be cohomology classes as above. We will use the same symbols to denote some choice of cocycles representing these cohomology classes. The restrictions of ϕ and ψ are non-zero homomorphisms $\phi : G_K \to (\mathrm{ad}^0\overline{\rho})(1)$ and $\psi : G_K \to \mathrm{ad}^0\overline{\rho}$. Let K_ϕ and K_ψ denote the fixed field of their kernels. Because $\mathrm{ad}^0\overline{\rho}$ is absolutely irreducible and not isomorphic to its twist by ϵ we see that K_ψ and K_ϕ are disjoint over K. Moreover the images $\psi(G_K)$ and $\phi(G_K)$ are not contained in any proper subspaces of $\mathrm{ad}^0\overline{\rho}$ and $(\mathrm{ad}^0\overline{\rho})(1)$, respectively. Thus we can find a $\tau \in \mathrm{Gal}\,(K_\phi K_\psi/K)$ such that

$$\begin{aligned}&\phi(\tau\widetilde{\sigma}) = \phi(\tau) + \phi(\widetilde{\sigma}) \notin \\ &\mathrm{Hom}\,(ke_\beta, ke_\alpha)(1) \oplus ((\mathrm{Hom}\,(ke_\alpha, ke_\alpha) \oplus \mathrm{Hom}\,(ke_\beta, ke_\beta)) \cap \mathrm{ad}^0\overline{\rho})(1)\end{aligned}$$

and

$$\psi(\tau\widetilde{\sigma}) = \psi(\tau) + \psi(\widetilde{\sigma}) \notin \mathrm{Hom}\,(ke_\beta, ke_\alpha) \oplus \mathrm{Hom}\,(ke_\alpha, ke_\beta).$$

Now choose a prime $w \notin S$ which is unramified in $K_\phi K_\psi/\mathbb{Q}$ and such that $\mathrm{Frob}_w = \tau\widetilde{\sigma}$. Take $\mathcal{C}_w$ as in example E3 so that $L_w = H^1(G_w, \mathrm{Hom}\,(ke_\beta, ke_\alpha))$. It follows easily that $(w, \mathcal{C}_w, L_w)$ has the desired properties. $\Box$

Theorem 1.3 *Let k be a finite extension of $\mathbb{F}_l$ and $\overline{\rho} : G_\mathbb{Q} \to GL_2(k)$ a continuous representation such that $\det \overline{\rho}(c) = -1$ and $\overline{\rho}(G_\mathbb{Q})$ is insoluble.*

Suppose first that

$$\overline{\rho}|_{G_l} \sim \begin{pmatrix} \epsilon\overline{\chi}_1 & * \\ 0 & \overline{\chi}_2 \end{pmatrix}$$

and that if $\epsilon\overline{\chi}_1 = \overline{\chi}_2$ then $\overline{\rho}|_{G_l}$ is wildly ramified. Then there is a continuous representation $\rho : G_\mathbb{Q} \to GL_2(W(k))$ such that

- $(\rho \bmod l) = \overline{\rho}$,
- $\rho|_{G_l} \sim \begin{pmatrix} \epsilon\chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$ *with χ_i a tamely ramified lift of $\overline{\chi}_i$ for $i = 1, 2$*
- *and for some prime $p \neq l$ we have $\rho|_{G_p} \sim \begin{pmatrix} \epsilon\chi & * \\ 0 & \chi \end{pmatrix}$ for some character χ.*

Now suppose that for some $1 \leq n \leq l - 1$ we have

$$\overline{\rho}|_{I_l} \sim \psi^{n+(l+1)m} \oplus \psi^{nl+(l+1)m}$$

where ψ is a fundamental character of level 2, then there is a continuous representation $\rho : G_\mathbb{Q} \to GL_2(W(k))$ such that

- $(\rho \bmod l) = \overline{\rho}$,
- $(\rho \otimes \omega^{-m})|_{G_l}$ *is crytsalline with Hodge-Tate numbers* 0 *and* n
- *and for some prime* $p \neq l$ *we have* $\rho|_{G_p} \sim \begin{pmatrix} \epsilon\chi & * \\ 0 & \chi \end{pmatrix}$ *for some character* χ.

2 Icosahedral Galois representations

We begin with some elementary lemmas on number fields. They are presumably well known, but it is easier to prove them than find a reference.

Lemma 2.1 *Let* K *be a number field (finite extension of* $\mathbb{Q}$*) and* S *a finite set of places of* K*. We will let* $K_S^\times$ *denote the subgroup of* $K^\times$ *consisting of elements which are units at all finite places* $v \notin S$ *and positive at all real places* $v \notin S$*. Then for any positive integer* n *we can find an open subgroup* $U \subset \prod_{v \notin S,\, v \not| \infty} \mathcal{O}_{K,v}^\times$ *such that*

$$K_S^\times \cap U \subset (K_S^\times)^n.$$

Proof: We may suppose that S contains all infinite places and that $\sqrt{-1} \in K$ (as $K^\times \subset K(\sqrt{-1})^\times$). We may also suppose that n is a prime power, say $n = p^r$. Thus if ζ denotes a primitive n^{th} root of unity then $\mathrm{Gal}\,(K(\zeta)/K)$ is cyclic. Because $K_S^\times$ is finitely generated, it suffices to prove that if $a \in K^\times$ and for all $y \notin S$ we have $a \in (K_y^\times)^n$ then $a \in (K^\times)^n$. Thus suppose $a \in K^\times$ and for all $y \notin S$ we have $a \in (K_y^\times)^n$. Then all but finitely many places split completely in $K(\sqrt[n]{a}, \zeta)/K(\zeta)$ so that $K(\zeta)$ contains every n^{th} root of a. We may choose $y \notin S$ which is unramified in $K(\zeta)$ and such that Frob_y generates the cyclic group $\mathrm{Gal}\,(K(\zeta)/K)$. We conclude that K contains an n^{th} root of a, as desired. $\square$

Lemma 2.2 *Let* K *be a number field and* S *a finite set of places of* K*. For each* $v \in S$ *let* L_v *be a finite Galois extension of* K_v*. Then we can find a finite, soluble, Galois extension* M *of* K*, such that for each place* w *of* M *above a place* $v \in S$ *we have* $L_v \cong M_w$ *as* K_v*-algebras.*

Proof: We need only find a finite extension M/K such that M embeds in a soluble Galois extension of K and such that for each place w of M above a place $v \in S$ we have $L_v \cong M_w$ as K_v-algebras. (Then replace M by its normal closure over K.) We may also suppose that S contains all infinite places of K. Then, by a simple induction argument, we may reduce to the case that each L_v/K_v is an abelian Galois extension. Thus suppose that L_v/K_v corresponds by class field theory to an open finite index subgroup $W_v \subset K_v^\times$. Set $W = \prod_{v \in S} W_v$ and choose an open subgroup $U \subset \prod_{v \notin S} \mathcal{O}_{K,v}^\times$ such that

$$K_S^\times \cap U \subset K_S^\times \cap W.$$

Finally take M to be the abelian extension of K corresponding to

$$K^\times (K_\infty^\times)^0 W U.$$

□

Lemma 2.3 *Suppose that $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_5^{ac})$ is a continuous representation which satisfies the following conditions.*

- $\det \overline{\rho}(c) = -1$.
- *$\overline{\rho}$ has projective image A_5.*
- *The projective image of I_3 has odd order.*
- *The projective image of G_5 has order 2 and the corresponding map $\mathbb{Q}_5^\times \to \{\pm 1\}$ sends 5 to -1.*

Then there is a finite, soluble, totally real extension $F/\mathbb{Q}$ and an elliptic curve E/F satisfying the following conditions.

- *$F \supset \mathbb{Q}(\sqrt{5})$ and $\sqrt{5}$ splits completely in F.*
- *$\overline{\rho}_{E,5}$ is equivalent to a twist of $\overline{\rho}|_{G_F}$ by some character.*
- *$\overline{\rho}_{E,3} : G_F \twoheadrightarrow GL_2(\mathbb{F}_3)$.*
- *E has good ordinary reduction at 3 and potentially good ordinary reduction at 5.*
- *For all primes v of F above 3 we have*

$$\overline{\rho}_{E,3}|_{G_{F_v}} \sim \begin{pmatrix} \chi_{1,v} & * \\ 0 & \chi_{2,v} \end{pmatrix}$$

  with $\chi_{1,v} \neq \chi_{2,v}$.

Proof: The obstruction to lifting the continuous homomorphism

$$G_{\mathbb{Q}(\sqrt{5})} \xrightarrow{\overline{\rho}} A_5 \cong PSL_2(\mathbb{F}_5)$$

to a continuous homomorphism $G_{\mathbb{Q}(\sqrt{5})} \to SL_2(\mathbb{F}_5)$ lies in

$$H^2(G_{\mathbb{Q}(\sqrt{5})}, \{\pm 1\}) \hookrightarrow \bigoplus_v H^2(G_{\mathbb{Q}(\sqrt{5})_v}, \{\pm 1\}).$$

Also the local component at (3) is trivial as 3 is inert in $\mathbb{Q}(\sqrt{5})$. Thus we can find a totally real, biquadratic field F_1

- such that F_1 contains $\mathbb{Q}(\sqrt{5})$ and both (3) and $(\sqrt{5})$ splits in F_1,
- and such that the image of this obstruction vanishes at all finite places of F_1.

As $\det \overline{\rho}(c) = -1$ the image of this obstruction is non-trivial at all infinite places of F_1. Similarly the obstruction to lifting the mod 5 cyclotomic character

$$G_{\mathbb{Q}(\sqrt{5})} \longrightarrow \{\pm 1\} \subset \mathbb{F}_5^\times$$

to a character $G_{\mathbb{Q}(\sqrt{5})} \to \mu_4$ with square the mod 5 cyclotomic character lies in

$$H^2(G_{\mathbb{Q}(\sqrt{5})}, \{\pm 1\}) \hookrightarrow \bigoplus_v H^2(G_{\mathbb{Q}(\sqrt{5})_v}, \{\pm 1\})$$

and has trivial image at all finite places and non-trivial image at infinity. Thus the sum of the two obstructions vanishes in $H^2(G_{F_1}, \{\pm 1\})$ and so we can lift

$$G_{F_1} \xrightarrow{\overline{\rho}} A_5 \cong PSL_2(\mathbb{F}_5)$$

to a continuous representation

$$\widetilde{\rho} : G_{F_1} \longrightarrow GL_2(\mathbb{F}_5)$$

with $\det \widetilde{\rho} = \epsilon_5$.

Choose a finite, soluble, totally real extension F_2/F_1 such that $(\sqrt{5})$ splits completely in F_2, such that $\widetilde{\rho}$ is trivial on the decomposition group of every prime of F_2 above 3, but such that the ramification index of any prime above 3 in F_2 is odd. Finally let F be the Galois closure of $F_2/\mathbb{Q}$.

Let $X_{\widetilde{\rho}}/F$ be the twist of X_5 defined in section 1 of [SBT]. By lemma 1.1 of [SBT] we see that $X_{\widetilde{\rho}}$ is isomorphic over F to a Zariski open subset of the projective line. Also let $Y_{\widetilde{\rho}}/X_{\widetilde{\rho}}$ be the cover defined in the proof of theorem 1.2 of [SBT]. Thus $Y_{\widetilde{\rho}}$ is geometrically irreducible and $Y_{\widetilde{\rho}}/X_{\widetilde{\rho}}$ has degree 24.

Suppose that v is a prime of F above 3. Then $\epsilon_5(\mathrm{Frob}_v) \equiv 1 \bmod 5$ so that the residue field of v contains $\mathbb{F}_{81}$. Thus the elliptic curve $y^2 = x^3 + x^2 - x - 1$ defines an element of $X_{\widetilde{\rho}}(F_v)$ with good ordinary reduction at v. The same will be true of any point of $X_{\widetilde{\rho}}(F_v)$ sufficiently close to this one in the 3-adic topology. Let $\mathcal{U}_v \subset X_{\widetilde{\rho}}(F_v)$ be a non-empty open set (for the 3-adic topology) consisting of points corresponding to elliptic curves with good ordinary reduction.

Suppose now that v is a prime of F above 5. We claim that we can find a non-empty open subset (for the 5-adic topology) $\mathcal{U}_v \subset X_{\widetilde{\rho}}(F_v)$ consisting of points corresponding to elliptic curves with good ordinary reduction. It suffices to find one such point (and then take $\mathcal{U}_v$ to be a sufficiently small open neighbourhood of that point). Note that up to twist by quadratic characters

$$\widetilde{\rho}|_{G_{F_v}} \sim \chi\delta \oplus \chi$$

where δ is a quadratic character corresponding to a character of $\mathbb{Q}_5(\sqrt{5})^\times$ taking $\sqrt{5}$ to -1, and χ is a tamely ramified character of order 4 corresponding to a character of $\mathbb{Q}_5(\sqrt{5})^\times$ taking $\sqrt{5}$ to 2. Moreover if δ is ramified then we may take χ unramified, while if δ is unramified the restriction of χ to inertia also has order 4. In the first case the elliptic curve $y^2 = x^3 + x$ provides a point in $X_{\widetilde{\rho}}(F_v)$. This elliptic curve has CM by $\mathbb{Z}[\sqrt{-1}]$ over F_v and a suitable quartic twist provides a point on $X_{\widetilde{\rho}}(F_v)$ in the second case.

By Ekedahl's version of the Hilbert irreducibility theorem [E] we may find a point $P \in X_{\widetilde{\rho}}(F)$ which lies in $\mathcal{U}_v$ for all $v|15$ and such that any point of $Y_{\widetilde{\rho}}$ above F cuts out an extension of F of degree 24. Let E/F be the elliptic curve corresponding to P. $\Box$

Theorem 2.4 *Let $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_5^{ac})$ be a continuous representation which satisfied the following conditions.*

- $\det \overline{\rho}(c) = -1$.
- *$\overline{\rho}$ has projective image A_5.*
- *The projective image of I_3 has odd order.*
- *The projective image of G_5 has order 2 and the corresponding map $\mathbb{Q}_5^\times \to \{\pm 1\}$ sends 5 to a non-trivial element.*

Then $\overline{\rho}$ is modular.

Proof: Choose F and E as in the previous lemma. By the Langlands-Tunnell theorem there is a cuspidal automorphic representation π''' of $GL_2(\mathbb{A}_F)$ and a place μ of the field of coefficients of π''' above 3 such that the following conditions are satisfied.

- For each infinite place v the component π'''_v is lowest discrete series.
- $\overline{\rho}_{\pi''',\mu} \sim \overline{\rho}_{E,3}$.
- For any place v of F above 3 we have
$$\rho_{\pi''',\mu}|_{G_v} \sim \begin{pmatrix} \chi_{1,v}\epsilon_3 & * \\ 0 & \chi_{2,v} \end{pmatrix},$$
where $\chi_{1,v}$ and $\chi_{2,v}$ are finitely tamely ramified, and $\chi_{1,v}\epsilon_3 \not\equiv \chi_{2,v} \bmod \mu$.

(See [L] and [Tu], as well as [RT] for the method for arranging the conditions on $\overline{\rho}_{\pi''',v}$ for v infinite.)

Applying theorem 5.1 of [SW2] to the 3-adic Tate module of E, we see that there is a cuspidal automorphic representation π'' of $GL_2(\mathbb{A}_F)$ satisfying the following conditions.

- For each infinite place v the component π''_v of π'' is lowest discrete series.
- π'' has field of coefficients $\mathbb{Q}$.
- For every rational prime l, the representation $\rho_{\pi'',l} \sim \rho_{E,l}$.

Twisting π'' we see that there is a cuspidal automorphic representation π' of $GL_2(\mathbb{A}_F)$ and a place λ' of the field of coefficients of π' above 5 such that the following conditions are satisfied.

- For each infinite place v the component π'_v is lowest discrete series.
- There is an embedding of the residue field of λ' in $\mathbb{F}_5^{ac}$ such that $\overline{\rho}_{\pi',\lambda'} \sim \overline{\rho}$.
- For any place v of F above 5 we have
$$\rho_{\pi',\lambda'}|_{G_v} \sim \begin{pmatrix} \chi_{1,v}\epsilon_5 & * \\ 0 & \chi_{2,v} \end{pmatrix},$$
where $\chi_{1,v}$ and $\chi_{2,v}$ are finitely tamely ramified.

Note that by our assumptions on $\overline{\rho}$, $\chi_{1,v}\epsilon_5 \not\equiv \chi_{2,v} \bmod \lambda'$.

We will next explain how to descend (in a $\bmod l$ sense) π' to $\mathbb{Q}$ while maintaining $\rho_{\pi',\lambda'} \sim \overline{\rho}$. We learned this argument from C.Khare.

By theorem 1.3 we may choose a continuous representation $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_5^{ac})$ satisfying the following conditions.

- ρ is a lift of $\overline{\rho}$.
- $\rho|_{G_5} \sim \begin{pmatrix} \chi_1\epsilon_5 & * \\ 0 & \chi_2 \end{pmatrix}$ where χ_1 and χ_2 are finitely tamely ramified.

The existence of π' above and theorem 5.1 of [SW2] tell us that there is a cuspidal automorphic representation π of $GL_2(\mathbb{A}_F)$ and a place λ of the field of coefficients of π above 5 such that the following conditions are satisfied.

- For each infinite place v the component π_v is lowest discrete series.
- There is an embedding of the λ-adic completion of the field of coefficients of π into $\mathbb{Q}_5^{ac}$ such that $\rho_{\pi,\lambda} \sim \rho|_{G_F}$.

Let $F = F_1 \supset F_2 \supset ... \supset F_n = \mathbb{Q}$ with F_i/F_{i+1} Galois and cyclic of prime degree for all i. We will show by induction on i that there is a cuspidal automorphic representation π_i of $GL_2(\mathbb{A}_{F_i})$ and a place λ_i of the field of coefficients of π_i above 5 such that the following conditions are satisfied.

- For each infinite place v the component $\pi_{i,v}$ is lowest discrete series.
- There is an embedding of the λ_i-adic completion of the field of coefficients of π_i into $\mathbb{Q}_5^{ac}$ such that $\rho_{\pi_i,\lambda_i} \sim \rho|_{G_{F_i}}$.

We have treated the case $i = 1$ above. Suppose we have treated the case of i. Let σ be a generator of $\mathrm{Gal}\,(F_i/F_{i+1})$. Then we see that $\pi_i^\sigma = \pi_i$ and so, by Langlands base change theorem [L], π_i descends to a cuspidal automorphic representation π'_{i+1} of $GL_2(\mathbb{A}_{F_{i+1}})$ with $\pi'_{i+1,v}$ lowest discrete series for each infinite place v of F'_{i+1}. Then there is an embedding of the field of coefficients of π'_{i+1} into $\mathbb{Q}_5^{ac}$, which gives rise to a place λ'_{i+1}, such that $\rho_{\pi'_{i+1},\lambda'_{i+1}}|_{G_{F_i}} \sim \rho|_{G_{F_i}}$. As $\rho|_{G_{F_i}}$ is irreducible we see that $\rho_{\pi'_{i+1},\lambda'_{i+1}}$ is the twist of $\rho|_{G_{F_{i+1}}}$ by a character of $\mathrm{Gal}\,(F_i/F_{i+1})$. Thus replacing π'_{i+1} by a twist the claim follows for $i+1$. The case $i = n$ of the claim implies the theorem. $\square$

Corollary 2.5 *Let $\rho : \mathbb{G}_{\mathbb{Q}} \to GL_2(\mathbb{C})$ be a continuous representation satisfying the following conditions.*

- $\det \rho(c) = -1$.
- *ρ has projective image A_5.*
- *The projective image of I_3 has odd order.*
- *The projective image of G_5 has order 2 and the corresponding map $\mathbb{Q}_5^\times \to \{\pm 1\}$ sends 5 to -1.*

Then ρ is modular.

Proof: This follows from the previous theorem and the main theorem of [Buz]. (In the case that the projective representation associated to $\overline{\rho}$ is unramified at 5, one may appeal instead to the main theorem of [BT].) $\Box$

We will finish by giving some concrete examples where this corollary can be applied. We list quintic polynomials whose splitting fields are A_5 extensions of $\mathbb{Q}$. In each case this A_5 extension can be lifted to a Galois representation ρ satisfying the conditions of the above corollary. None of these examples satisfy the conditions of the main theorem of [BDST]. They are all taken from the tables in [Buh].

$$\begin{array}{l} x^5 + 2x^4 + 6x^3 + 8x^2 + 10x + 8 \\ x^5 + 6x^4 + x^3 + 4x^2 - 24x + 32 \\ x^5 - 2x^3 + 2x^2 + 5x + 6 \\ x^5 + 5x^4 + 8x^3 - 20x^2 - 21x - 5. \end{array}$$

Corrigendum to [Ta].

I would like to thank Fred Diamond for pointing out an error in [Ta]. More precisely, with the definition of the inner product given on page 271 of [Ta], the calculation of the adjoint of a Hecke operator is in general wrong. This may be corrected as follows.

- Change the definition of $\langle f, g \rangle$ on page 271 to read
$$\langle f, g \rangle = \sum_{[x] \in X(U)} [D^\times \cap xUx^{-1} : F^\times \cap U]^{-1} \langle f(x), g(x) \rangle (\mathbf{N}\nu x)^\mu.$$
- Make the corresponding changes to the calculation on page 271 of the adjoint of $[UxU']$. The final formula remains unchanged.
- At the start of line 4 on page 274 of [Ta] and the following sentence. "Note that $[D^\times \cap t_j u_l U u_l^{-1} t_j^{-1} : F^\times \cap U] | [D^\times \cap t_j U_0 t_j^{-1} : F^\times \cap U_0]$ and so there are only finitely many possibilities (independent of $U \subset U_0$) for $[D^\times \cap t_j u_l U u_l^{-1} t_j^{-1} : F^\times \cap U]$."

References

[BDST] K.Buzzard, M.Dickinson, N.Shepherd-Barron and R.Taylor, *On icosahedral Artin representations*, preprint.

[BT] K.Buzzard and R.Taylor, *Companion forms and weight one forms*, Annals of Math. 149 (1999), 905-919.

[Buh] J.Buhler, *Icosahedral Galois representations*, LNM 654, Springer 1978.

[Buz] K.Buzzard, *Analaytic continuation of overconvergent eigenforms*, in preparation.

[DDT] H.Darmon, F.Diamond and R.Taylor, *Fermat's last theorem*, Current Developments in Mathematics 1 (1995), 1-154.

[Dia] F.Diamond, *The Taylor-Wiles construction and multiplicity one*, Invent. Math. 128 (1997), 379-391.

[Dic] M.Dickinson, *On the modularity of certain* 2*-adic Galois representations*, preprint.

[E] T.Ekedahl, *An effective version of Hilbert's irreducibility theorem*, in "Séminaire de Théorie des Nombres, Paris 1988-1989", Progress in Mathematics 91, Birkhäuser 1990.

[F] K.Fujiwara, *Deformation rings and Hecke algebras in the totally real case*, preprint.

[L] R.Langlands, *Base change for $GL(2)$*, PUP 1980.

[R] R.Ramakrishna, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur*, preprint.

[RT] J.Rogawski and J.Tunnell, *On Artin L-functions associated to Hilbert modular forms*, Invent. Math. 74 (1983), 1-42.

[S] J.-P.Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987), 179-230.

[SBT] N.Shepherd-Barron and R.Taylor, *Mod 2 and mod 5 icosahedral representations*, JAMS 10 (1997), 281-332.

[SW1] C.Skinner and A.Wiles, *Base change and a problem of Serre*, preprint.

[SW2] C.Skinner and A.Wiles, *Nearly ordinary deformations of irreducible residual representations*, preprint.

[Ta] R.Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. 98 (1989), 265-280.

[Tu] J.Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. AMS 5 (1981), 173-175.

[TW] R.Taylor and A.Wiles, *Ring theoretic properties of certain Hecke algebras*, Ann. of Math. 141 (1995), 553-572.

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