POTENTIAL MODULARITY AND APPLICATIONS

ANDREW SNOWDEN

Contents

1. Introduction

In our seminar we have been working towards a modularity lifting theorem. Recall that such a theorem allows one (under suitable hypotheses) to deduce the modularity of a p-adic Galois representation from that of the corresponding mod p representation. This is a wonderful theorem, but it is not immediately apparent how it can be applied: when does one know that the residual representation is modular?

One example where residual modularity is known is the following: a theorem of Langlands and Tunnel states that any Galois representation (of any number field) into $\mathrm{GL}_2(\mathbf{F}_3)$ is modular. Their result is specific to $\mathbf{F}_3$ and does not apply to representations valued in other finite fields (except perhaps $\mathbf{F}_2$?): the key point is that $\mathrm{GL}_2(\mathbf{F}_3)$ is solvable. Modularity lifting thus allows one to conclude (under appropriate hypotheses) that representations into $\mathrm{GL}_2(\mathbf{Z}_3)$ are modular. Wiles' original application of modularity lifting to elliptic curves used this line of reasoning.

For finite fields other than $\mathbf{F}_3$ (and maybe $\mathbf{F}_2$) there is no analogue of the Langlands–Tunnel theorem: the finite groups $\mathrm{GL}_2(\mathbf{F}_q)$ are typically not solvable. However, Taylor [Tay], [Tay2] partially found a way around this problem: he observed, using a result of Moret-Bailly, that any odd residual representation of a totally real field F becomes modular after passing to a finite extension of F; that is, odd residual representations of F are *potentially modular*. Using modularity lifting, one can conclude that many p-adic are potentially modular as well. Typically, one cannot deduce modularity from potential modularity. Nonetheless, many of the nice properties of modular p-adic representations can be established for potentially modular representations as well: they satisfy the Weil bounds, their L-functions admit meromorphic continuation and satisfy a functional equation, they often can be realized in the Tate module of an abelian variety and they fit into compatible systems. We prove the final of these results.

As if these consequences of potential modularity were not impressive enough, Khare and Wintenberger [KW] went even farther: they proved that every irreducible odd residual representation of $G_{\mathbf{Q}}$ is modular, a result first conjectured by Serre. To do this, they first showed — using potential modularity — that any mod p representation admits a nice p-adic lift. This lift (by one of the corollaries of potential modularity) fits into a compatible system. To prove the modularity of the original mod p representation, it suffices (by modularity lifting, and basic properties of compatible systems) to prove the modularity of the reduction of any of the ℓ-adic representations in the system. This permits the possibility of an inductive argument, which turns out to be quite subtle but possible. The base cases of the induction had been previously proved by Serre and Tate; these results are specific to $\mathbf{Q}$ and is one reason that this sort of result has not been extended to other fields.

Date: March 27, 2010.

As indicated, the results presented here are mainly due to Taylor, Khare and Wintenberger, building on the modularity lifting theorems of Wiles and Kisin (though many other people contributed along the way). I learned most of these arguments by writing a paper [Sno] that extends them a small amount. Some of these notes are taken directly from that paper.

2. Review of compatible systems

In this section we provide a brief review of compatible systems and some of their most basic properties.

2.1. **Compatible systems with rational coefficients.** Let F be a number field. An *n-dimensional compatible system of G_F with coefficients in* $\mathbf{Q}$ is a family $\{\rho_\ell\}$ indexed by the set of rational prime numbers ℓ (or possibly some subset thereof) where $\rho_\ell : G_F \to \mathrm{GL}_n(\mathbf{Q}_\ell)$ is a continuous representation, such that the following conditions hold:

- There exists a finite set S of places of F such that each ρ_ℓ is unramified outside $S \cup S_\ell$. Here S_ℓ denotes the set of places of F above ℓ.
- For each place v of F not in S there exists a polynomial $p_v \in \mathbf{Q}[t]$ such that: for any prime ℓ and any place $v \notin S \cup S_\ell$ the characteristic polynomial of $\rho_\ell(\mathrm{Frob}_v)$ is p_v.

In words: the ρ_ℓ have uniform ramification properties and the characteristic polynomial of Frob_v is independent of ℓ.

Example 1. Let f be a Hilbert modular form over F whose Hecke eigenvalues are rational numbers. For each rational prime ℓ we have a Galios representation $\rho_\ell : G_F \to \mathrm{GL}_2(\mathbf{Q}_\ell)$. The collection of these Galois representations forms a compatible system. The set S can be taken to be the set of primes dividing the level of f, while p_v can be taken to be $t^2 - a_v t + a_{v,v}$ where a_v and $a_{v,v}$ are the T_v and $T_{v,v}$ eigenvalues of f.

Example 2. Let E be an elliptic curve over F. Let ρ_ℓ be the representation of G_F on the ℓth Tate module of E (tensored with $\mathbf{Q}_\ell$). Then the collection of these Galois representations forms a two-dimensional compatible system. The set S can be taken to be the set of places of F where E has bad reduction. We have $p_v(t) = t^2 - a_v t + \mathbf{N}\, v$, where $\mathbf{N}\, v + 1 - a_v$ is the number of points of the reduction of E at v with coefficients in the residue field of v. Of course, one can replace E with a higher dimensional abelian variety.

Example 3. Let X be a smooth projective variety over a number field F. Let ρ_ℓ be the representation of G_F on the étale cohomology $H^i(X_{\overline{F}}, \mathbf{Q}_\ell)$, for some fixed i. Then the collection of these Galois representations forms a compatible system. The set S can be taken to be the set of primes where X does not have good reduction. Here, we say that X has good reduction at a place v if there exists a smooth projective scheme $\mathscr{X}/\mathscr{O}_{F_v}$ whose generic fiber is isomorphic to X. The polynomials p_v comes from certain pieces of the zeta function of X (which is by definition independent of ℓ); to find these pieces, the Riemann hypothesis (proved by Deligne) is needed. When X is an abelian variety, this example is more or less the same as the previous one.

Remark 4. Since the compatibility condition is in terms of characteristic polynomials, it is not good at detecting extensions: if $\{\rho_\ell\}$ is a compatible system then so too is $\{\rho_\ell^{\mathrm{ss}}\}$ where ρ^{ss} denotes the semi-simplification of ρ. The converse is not quite true since the ramification of ρ_ℓ cannot be controlled in terms of that of ρ_ℓ^{ss}. We say that a compatible system is *semi-simple* if all of its members are.

2.2. **Compatible systems with general coefficients.** As suggested by the terminology of the previous section, there is a more general notion of compatible system. Let K be a number field. Then an *n-dimensional compatible system of G_F with coefficients in K* is a family $\{\rho_w\}$ indexed by the set of finite places w of K (or possibly some subset thereof) where $\rho_w : G_F \to \mathrm{GL}_n(K_w)$ is a continuous representation, such that conditions analogous to those given in the $K = \mathbf{Q}$ case hold. The polynomial p_v will now have coefficients in K.

Example 5. Let f be a Hilbert modular form over F whose Hecke eigenvalues generate the number field K. Then for each place w of K we have a Galois representation $\rho_w : G_F \to \mathrm{GL}_2(K_w)$, and these form a compatible system. The description of S and p_v are as in Example 1.

Example 6. A $\mathrm{GL}_2(K)$*-type abelian variety* is an abelian variety A/F of dimension $[K : \mathbf{Q}]$ equipped with an injection $\mathscr{O}_K \to \mathrm{End}(A)$. This implies that $T_\ell A \otimes \mathbf{Q}_\ell$ is a free $K \otimes \mathbf{Q}_\ell$ module of rank two. Decomposing this module into its pieces (corresponding to how ℓ splits in K), gives a two dimensional Galois representation $G_F \to \mathrm{GL}_2(K_w)$ for each finite place w of K. These form a compatible system.

2.3. **Properties of compatible systems.** The Chebotarev density theorem immediately yields the following result:

Proposition 7. *Let $\{\rho_w\}$ and $\{\rho'_w\}$ be two semi-simple compatible systems of G_F with coefficients in the same field K. Assume there is some place w_0 of K such that ρ_{w_0} and ρ'_{w_0} are isomorphic. Then ρ_w and ρ'_w are isomorphic for all w.*

As a corollary, we obtain the following, which we will use constantly:

Proposition 8. *Let $\{\rho_w\}$ be a two-dimensional compatible system of semi-simple representations of G_F with coefficients in K, and let w_1 and w_2 be two places of K. Then ρ_{w_1} is modular if and only if ρ_{w_2} is. In particular, if any member of a compatible system is modular then all members are.*

Proof. This follows from the previous proposition since modular representations always come in compatible systems; see Example 5. □

3. Potential modularity

In this section, we sketch give a sketch of Taylor's potential modularity. The original arguments are in the papers [Tay] and [Tay2]. The basic idea is as follows. We are given a two dimensional mod p Galois representation $\overline{\rho}$ of G_F, where F is totally real, which we want to show is potentially modular. We find a two dimensional ℓ-adic Galois representation σ, which we know to modular. This new representation is completely independent of $\overline{\rho}$. However, using a very general theorem of Moret-Bailly, we show that there is a GL_2-type abelian variety A over some finite extension F'/F whose mod ℓ representation is $\overline{\sigma}|_{F'}$ and whose mod p representation is $\overline{\rho}|_{F'}$. Modularity lifting implies that the ℓ-adic representation of A is modular. General properties of compatible systems then give the modularity of the p-adic representation of A, and thus of the mod p representation $\overline{\rho}|_{F'}$ as well.

We now make this precise. We begin by recalling the theorem of Moret-Bailly [MB]:

Theorem 9 (Moret-Bailly)**.** *Let X be a smooth geometrically irreducible variety over a number field F. Let S be a finite set of places of F and for each $v \in S$ let L_v/F_v be a finite Galois extension and let $U_v \subset X(F_v)$ be a non-empty open subset (for the v-adic topology). Then there exists a finite Galois extension F'/F which splits over each L_v (i.e., $F' \otimes_F L_v$ is a direct product of L_v's) and a point $x \in X(F')$ such that the image of x in $X(L_v)$ under any map $F' \to L_v$ belongs to U_v.*

Using this result, we deduce the following crucial result, which "links" arbitrary residual representations.

Proposition 10. *Let F be a totally real number field and let $\overline{\rho}_1 : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ and $\overline{\rho}_2 : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ be irreducible odd representations, with $p \neq \ell$. Then there exists a finite totally real Galois extension F'/F and a two-dimensional compatible system $\{\rho_w\}$ of representations of $G_{F'}$ with coefficients in some number field K, such that for some place $v_1 \mid p$ of K the representation $\overline{\rho}_{v_1}$ is equivalent to $\overline{\rho}_1$ while for some place $v_2 \mid \ell$ the representation $\overline{\rho}_{v_2}$ is equivalent to $\overline{\rho}_2$. Furthermore, the field F'/F can be taken to be linearly disjoint from any given finite extension of F and the system $\{\rho_w\}$ can be taken so that ρ_{v_1} (resp. ρ_{v_2}) is ordinary crystalline at all places over p (resp. ℓ).*

Proof. For simplicity we assume that $\overline{\rho}_1$ and $\overline{\rho}_2$ take values in $\mathrm{GL}_2(\mathbf{F}_p)$ and $\mathrm{GL}_2(\mathbf{F}_\ell)$ respectively, and that both have cyclotomic determinant. We give some comments on the general case following the proof.

Let Y/F be the moduli space classifying elliptic curves whose p-torsion is $\overline{\rho}_1$ and whose ℓ-torsion is $\overline{\rho}_2$. More precisely, regard $\overline{\rho}_1$ and $\overline{\rho}_2$ as finite étale group schemes G_1 and G_2 over F. Pick an isomorphism $G_1 \to G_1^\vee$ of G_1 with its Cartier dual such that the corresponding pairing $G_1 \times G_1 \to \mathbf{G}_m$ is symplectic, which is possible by the assumption on the determinant of ρ_1; do the same for G_2. For a scheme T/F let $Y(T)$ be the groupoid of elliptic curves E/T equipped with isomorphisms $E[p] \to (G_1)_T$ and $E[\ell] \to (G_2)_T$ such that the Weil pairing on $E[p]$ corresponds to the given pairing on $(G_1)_T$, and similarly for ℓ. It is not difficult to see that Y is representable by a scheme. In fact, the open modular curve $Y(p\ell)$ of full level splits into a several connected components over $\overline{\mathbf{Q}}$ and our space Y is a twisted form of any one of these components. This shows that Y is smooth and geometrically irreducible.

We are now going to apply the theorem of Moret-Bailly. Take S to be the set of infinity places of F and for $v \in S$ let $L_v = F_v$, the real numbers, and let $U_v = Y(L_v)$. Clearly, U_v is an open subset of $Y(L_v)$. To apply the theorem we need $Y(F_v)$ to be non-empty. This is the case because the representations $\overline{\rho}_1$ and $\overline{\rho}_2$ are odd: if E/F_v is any elliptic curve then $E[p]$ is automatically equivalent to $(G_1)_{F_v}$, and similarly for $E[\ell]$.

Thus any elliptic curve over F_v can be given the additional structure needed to define a point of $Y(F_v)$. Moret-Bailly now gives a finite totally real Galois extension F'/F (totally real because it splits over each F_v for $v \mid \infty$) and an elliptic curve E/F' such that $E[p] = \overline{\rho}_1|_{F'}$ and $E[\ell] = \overline{\rho}_2|_{F'}$. The compatible system can now be taken to be the Tate modules of E.

We now show that E may be taken to be ordinary crystalline at all places above ℓ. (The arguments at p are identical, and can be carried out simultaneously.) Add to S all the places of F above ℓ. Fix for the moment a place v of F over ℓ. Let $\overline{U}_v$ be the subset of $Y(\overline{F}_v)$ consisting of elliptic curves with good ordinary reduction. This is clearly a non-empty set, since there exist elliptic curves with good ordinary reduction, and these can be given arbitrary level structure over $\overline{F}_v$. We now show that it is open. Let $j : Y(\overline{F}_v) \to \overline{F}_v$ be the j-invariant; it is a continuous function for the v-adic topology. The subset V of $Y(\overline{F}_v)$ where the elliptic curve has good reduction consists of those curves for which j is integral; it is therefore open. The subset of V where the elliptic curve has ordinary reduction is open, since this only depends upon the reduction of the curve: if E and E' are two curves whose j-invariants are v-adically close then they have the same reduction, and so one is ordinary if and only if the other is. This shows that $\overline{U}_v$ is open. Let L_v/F_v be any Galois extension such that $\overline{U}_v \cap Y(L_v)$ is non-empty, and take U_v to be this intersection. We now apply Moret-Bailly as before. The elliptic curve E/F' that we produce has good ordinary reduction at all places over ℓ by the construction of the sets U_v, and so the Tate module ρ_{v_2} is ordinary crystalline at all places over ℓ.

Finally, we show that F'/F can be taken linearly disjoint from any given finite extension of F. Thus let M/F be a finite extension, which we can and do assume to be Galois. Observe that $Y(F_v)$ is non-empty for all sufficiently large v: indeed, if v is sufficiently large then Y will be smooth at v and its reduction will have rational points by the Weil bounds; smoothness allows us to lift these mod v points to $\mathscr{O}_{F_v}$ points. Let S' be a finite collection of finite places of F satisfying the following conditions: (1) for each $v \in S'$ the set $Y(F_v)$ is non-empty; (2) no place of S' lies over p or ℓ; and (3) no place of S' ramifies in M; (4) the elements Frob_v with $v \in S'$ generate the finite group $\mathrm{Gal}(M/F)$. We now again modify the Moret-Bailly set-up. We add the set S' to the set S, and for $v \in S'$ we take $L_v = F_v$ and $U_v = Y(F_v)$. The field F'/F that Moret-Bailly produces splits at all elements of S' and is therefore linearly disjoint from M. □

Remark 11. In the above proof we assume that $\overline{\rho}_1$ and $\overline{\rho}_2$ had cyclotomic determinant and were valued in the prime field. The first of these conditions is straightforward to relax by passing to an appropriate finite extension of F and twisting. To remove the second assumption one proceeds as follows. Pick a number field K which is sufficiently large so that $\overline{\rho}_1$ can be regarded as taking values in the residue field of K at some place above p, and similarly for ℓ. Then, instead of considering moduli spaces of elliptic curves, consider moduli spaces of $\mathrm{GL}_2(K)$-type abelian varieties. The theory of these moduli spaces is developed in [Rap].

Remark 12. In the previous theorem we required that $\overline{\rho}_1$ and $\overline{\rho}_2$ be irreducible. This is not really needed, but we included since we have defined compatible systems to be rational objects, and so one can typically only form the semi-simplification of their reductions.

We now produce a large supply of "universally" modular Galois representations.

Proposition 13. *Let F be a totally real field and ℓ a prime number. There exists a Galois representation $\sigma : G_F \to \mathrm{GL}_2(\overline{\mathbf{Q}}_\ell)$ satisfying the following conditions:*

(a) *σ is modular.*
(b) *σ is ordinary and crystalline at all places above ℓ.*
(c) *$\overline{\sigma}|_{F(\zeta_\ell)}$ is (absolutely) irreducible.*

Furthermore, these conditions hold after restricting σ to any finite totally real extension of F.

Proof. An exercise in class field theory allows one to produce an imaginary quadratic extension E/F and a character $\psi : G_E \to \overline{\mathbf{Q}}_\ell^\times$ such that the representation $\sigma = \mathrm{Ind}_E^F(\psi)$ satisfies conditions (b) and (c) of the proposition. (One picks E to split at all places of F above ℓ. If $v \mid \ell$ is a place of F and w_1 and w_2 the two places of E above F then one takes ψ so that $\psi|_{E_{w_1}}$ is finitely ramified and $\psi|_{E_{w_2}}$ differs from the cyclotomic character by a finitely ramified character.) A theorem of Hecke states that σ is modular. If F'/F is a finite extension then $\sigma|_{F'} = \mathrm{Ind}_{EF'}^{F'}(\psi|_{F'})$ and the same arguments apply. □

We can now prove potential modularity for residual representations:

Theorem 14. *Let F be a totally real field and let $\overline{\rho} : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ be an odd representation such that $\overline{\rho}|_{F(\zeta_p)}$ is (absolutely) irreducible. Then there exists a finite totally real Galois extension F'/F, which can be taken to be linearly disjoint from any finite extension of F, such that $\overline{\rho}|_{F'}$ is modular. Furthermore, the modular form can be taken to be ordinary at all places of F' above p and of level prime to p.*

Proof. Let σ be as in Proposition 13, where ℓ can be any prime different from p (and maybe larger than 5). By Proposition 10, we can find a finite extension F'/F, linearly disjoint from whatever we want, a compatible system $\{\rho_w\}$ of representations of $G_{F'}$ with coefficients in some number field K and two places $v_1 \mid p$ and $v_2 \mid \ell$ of K such that: (1) ρ_{v_1} is ordinary crystalline at all places above p and its reduction is equivalent to $\overline{\rho}$; (2) ρ_{v_2} is ordinary crystalline at all places above ℓ and its reduction is equivalent to $\overline{\sigma}$. The modularity lifting theorem that we have proved now establishes that ρ_{v_2} itself is modular. By compatibility, ρ_{v_1} is modular (see Proposition 8), and thus $\overline{\rho}$ is as well. Since ρ_{v_1} is ordinary crystalline at all places above p, the modular form giving rise to it has prime to p level and is ordinary at all places above p. □

We can now prove potential modularity for p-adic representations:

Theorem 15. *Let F be a totally real field, let $p > 5$ be a prime and let $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$ be a continuous representation satisfying the following conditions:*

- (A1) *ρ is odd.*
- (A2) *ρ ramifies at only finitely many places.*
- (A3) *$\overline{\rho}|_{F(\zeta_p)}$ is (absolutely) irreducible.*
- (A4) *ρ is ordinary crystalline at all places above p.*

Then there exists a finite totally real Galois extension F'/F, which can be taken to be linearly disjoint from any given finite extension of F, such that $\rho|_{F'}$ is modular.

Proof. By the previous theorem, we can find a finite extension F'/F such that $\overline{\rho}|_{F'}$ comes from a modular form which is ordinary crystalline at all places above p. The modularity lifting theorem we have proved gives the modularity of $\rho|_{F'}$. □

Remark 16. Condition (A4) be relaxed if one is willing to use more general modularity lifting theorems. However, (A1)–(A3) are essential to the method of proof.

Remark 17. This clause about being able to produce the field F' so that it is linearly disjoint from a given extension of F is often used to make F' linearly disjoint from the kernel of $\overline{\rho}$. This implies that $\overline{\rho}$ and $\overline{\rho}|_{F'}$ have the same image. Thus $\overline{\rho}|_{F'}$ will still be irreducible.

4. Putting representations into compatible systems

We now use potential modularity to put p-adic representations in compatible systems. I learned the proof of this result from a lecture given by Taylor at the Summer School on Serre's Conjecture held at Luminy in 2007. Taylor attributed the proof to Dieulefait; a sketch of the argument can be found in [Die, §3.2]. However, I have not found a detailed proof in the literature.

Proposition 18. *Let F be a totally real field, let $p > 5$ be a prime and let $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$ be a continuous representation satisfying (A1)–(A4). Then there exists a compatible system $\{\rho_w\}$ of G_F with coefficients in some number field K such that for some place v_0 of K the representation ρ_{v_0} is equivalent to ρ.*

Proof. Apply Theorem 15 to produce a finite Galois totally real extension F'/F linearly disjoint from $\ker \overline{\rho}$ and a modular form f over F' such that $\rho|_{F'} = \rho_f$ (we regard the coefficient field of f as being embedded in $\overline{\mathbf{Q}}_p$). Let I be the set of fields F'' which are intermediate to F' and F and for which $\mathrm{Gal}(F'/F'')$ is solvable. For $i \in I$ we write F_i for the corresponding field. For each i we can use solvable descent to find a modular form f_i such that $\rho|_{F_i} = \rho_{f_i}$. Let K_i denote the field of coefficients of f_i, which we regard as being embedded in $\overline{\mathbf{Q}}_p$. Let K be a number field which is Galois over $\mathbf{Q}$, into which each K_i embeds and which contains all roots of unity of order $[F' : F]$. Fix an embedding $K \to \overline{\mathbf{Q}}_p$ and embeddings $K_i \to K$ such that the composite $K_i \to K \to \overline{\mathbf{Q}}_p$ is the given embedding. Let v_0 be the place of K determined by the embedding $K \to \overline{\mathbf{Q}}_p$. For each place v of K and each $i \in I$ we have a representation $r_{i,v} : G_{F_i} \to \mathrm{GL}_2(K_v)$ associated to the modular form f_i. It is absolutely irreducible. Note that after composing r_{i,v_0} with the embedding $\mathrm{GL}_2(K_{v_0}) \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$ we obtain $\rho|_{G_{F_i}}$.

By Brauer's theorem, we can write

$$1=\sum_{i\in I} n_i \operatorname{Ind}_{\mathrm{Gal}(F'/F_i)}^{\mathrm{Gal}(F'/F)}(\chi_i)$$

where the n_i are integers (possibly negative) and the χ_i are characters of $\mathrm{Gal}(F'/F_i)$ valued in $K^\times$. (Here we use the fact that K contains all roots of unity of order $[F':F]$.) This equality is taken in the Grothendieck group of representations of $\mathrm{Gal}(F'/F)$ over K. Note that by taking the dimension of each side we find $\sum n_i[F_i:F]=1$.

Let v be a place of K. For a number field M write $\mathcal{C}_{M,v}$ for the category of semi-simple continuous representations of G_M on finite dimensional K_v-vector spaces. The category $\mathcal{C}_{M,v}$ is a semi-simple abelian category. We let $K(\mathcal{C}_{M,v})$ be its Grothendieck group. It is the free abelian category on the set of irreducible continuous representations of G_M on K_v-vector spaces. We let $(,)$ be the integer valued pairing on $K(\mathcal{C}_{M,v})$ given by $(A,B)=\dim_{K_v}\operatorname{Hom}(A,B)$. This is well-defined because $\mathcal{C}_{M,v}$ is semi-simple. It is symmetric. If M'/M is a finite extension then we have adjoint functors $\operatorname{Ind}_{M'}^{M}:\mathcal{C}_{M',v}\to\mathcal{C}_{M,v}$ and $\operatorname{Res}_{M'}^{M}:\mathcal{C}_{M,v}\to\mathcal{C}_{M',v}$. (One must check, of course, that induction and restriction preserve semi-simplicity — we leave this to the reader.) These functors induce maps on the K-groups which are adjoint with respect to $(,)$. If M_1 and M_2 are two extensions of M and r_1 belongs to $\mathcal{C}_{M_1,v}$ and r_2 belongs to $\mathcal{C}_{M_2,v}$ then we have the formula

$$(\operatorname{Ind}_{M_1}^{M}(r_1),\operatorname{Ind}_{M_2}^{M}(r_2))=\sum_{g\in S}(\operatorname{Res}_{M_1^gM_2}^{M_1^g}(r_1^g),\operatorname{Res}_{M_1^gM_2}^{M_2}(r_2)) \tag{1}$$

where S is a set of representatives for $G_{M_1}\backslash G_M/G_{M_2}$, M_1^g is the field determined by $gG_{M_1}g^{-1}$ and r_1^g is the representation of $gG_{M_1}g^{-1}$ given by $x\mapsto r_1(g^{-1}xg)$. This formula is gotten by using Frobenius reciprocity and Mackey's formula.

Define

$$\rho_v=\sum_{i\in I} n_i\operatorname{Ind}_{F_i}^{F}(r_{i,v}\otimes\chi_i),$$

which is regarded as an element of $K(\mathcal{C}_{F,v})$. We now show that each ρ_v is (the class of) an absolutely irreducible two dimensional representation. To begin with, we have

$$\begin{aligned}\rho_{v_0}\otimes_{K_{v_0}}\overline{\mathbf{Q}}_p&=\sum_{i\in I} n_i\operatorname{Ind}_{F_i}^{F}((r_{i,v_0}\otimes_{K_{v_0}}\overline{\mathbf{Q}}_p)\otimes_K\chi_i)\\&=\sum_{i\in I} n_i\operatorname{Ind}_{F_i}^{F}((\rho|_{F_i})\otimes_K\chi_i)\\&=\left[\sum_{i\in I} n_i\operatorname{Ind}_{F_i}^{F}(\chi_i)\right]\otimes_K\rho\\&=\rho\end{aligned}$$

This shows that ρ_{v_0} is (the class of) an absolutely irreducible representation.

Now let v be an arbitrary finite place of K. We have

$$\begin{aligned}(\rho_v,\rho_v)&=\sum_{i,j\in I} n_in_j(\operatorname{Ind}_{F_i}^{F}(r_{i,v}\otimes\chi_i),\operatorname{Ind}_{F_j}^{F}(r_{j,v}\otimes\chi_j))\\&=\sum_{i,j\in I}\sum_{g\in S_{ij}} n_in_j(\operatorname{Res}_{F_i^gF_j}^{F_i^g}((r_{i,v}\otimes\chi_i)^g),\operatorname{Res}_{F_i^gF_j}^{F_j}(r_{j,v}\otimes\chi_j))\end{aligned}$$

where we have used (1). Here S_{ij} is a set of representatives for $G_{F_1}\backslash G_F/G_{F_2}$. The representation $r_{i,v}|_{F'}$ is the representation coming from the form f' and so is absolutely irreducible. It follows that the restriction of $r_{i,v}$ to any subfield of F' is absolutely irreducible. Thus the representations occurring in the pairing in the second line above are irreducible. It follows that the pairing is then either 1 or 0 if the representations are isomorphic or not. Therefore, if let $\delta_{v,i,j,g}$ be 1 or 0 according to whether $\operatorname{Res}_{F_i^gF_2}^{F_i^g}(r_{i,v}\otimes\chi_i)^g$ is isomorphic to $\operatorname{Res}_{F_i^gF_2}^{F_j}(r_{j,v}\otimes\chi_j)$ then we find

$$(\rho_v,\rho_v)=\sum_{i,j\in I}\sum_{g\in S_{ij}} n_in_j\delta_{v,i,j,g}.$$

Now, the $\{r_{i,v}\}_v$ and the $\{r_{j,v}\}_v$ form a compatible system. It follows that $\delta_{v,i,j,g}$ is independent of v. The above formula thus gives

$$(\rho_v, \rho_v) = (\rho_{v'}, \rho_{v'})$$

if v' is another place of K. Taking $v' = v_0$ and using that ρ_{v_0} is an absolutely irreducible representation gives $(\rho_v, \rho_v) = 1$. Now, if we write $\rho_v = \sum m_i \pi_i$ where $m_i \in \mathbf{Z}$ and the π_i are mutually non-isomorphic irreducible representations then we have $(\rho_v, \rho_v) = \sum m_i^2 (\pi_i, \pi_i)$. Since the terms are all non-negative integers and the sum is 1, we find $\rho_v = \pm\pi$ with $(\pi, \pi) = 1$. Thus π is an absolutely irreducible representation. Now, $\dim \rho_v = 2$ since each $r_{i,v}$ is two dimensional and $\sum n_i [F_i : F] = 1$. Since $\dim \pi$ is non-negative, we must have $\rho_v = \pi$. This proves that ρ_v is the class of an absolutely irreducible representation.

Of course, it must be shown that the ρ_v actually form a compatible system! This is fairly easy after what we have done, and we leave this task to the reader. □

Remark 19. The compatible system constructed above is in fact *strongly compatible*. For a discussion of this, see [Tay, Theorem 6.6].

5. Lifting residual representations

We now show that one can lift most residual representations to characteristic zero representations.

Proposition 20. *Let F be a totally real field, $p > 5$ a prime and $\overline{\rho} : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ an odd representation such that $\overline{\rho}|_{F(\zeta_p)}$ is (absolutely) irreducible. Assume that for each plave $v \mid p$ of F the representation $\overline{\rho}|_{F_v}$ admits a lift to $\overline{\mathbf{Z}}_p$ which is ordinary crystalline. Then there exists a continuous representation $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$ satisfying (A1)–(A4) lifting $\overline{\rho}$. One can take ρ to be unramified at the same places where $\overline{\rho}$ is unramified (excluding places above p).*

Proof. Let S be the set of primes away from p at which $\overline{\rho}$ ramifies and let S_p denote the set of primes above p. For $v \in S \cup S_p$ we have the universal framed deformation ring $R_v^\square$ of $\overline{\rho}|_{F_v}$. For $v \in S_p$ we let $R_v^\dagger$ be the quotient of $R_v^\square$ parameterizing ordinary crystalline representations, in the same manner as we have done before. The ring $R_v^\dagger$ is non-zero since we have assumed that $\overline{\rho}|_{F_v}$ admits an ordinary crystalline lift. Our previous work therefore shows that it is $\mathscr{O}$-flat and has relative dimension dimension is $3 + [F_v : \mathbf{Q}_p]$ over $\mathscr{O}$. For $v \in S$ we pick a non-zero $\mathscr{O}$-flat quotient $R_v^\dagger$ of $R_v^\square$ of relative dimension 3 over $\mathscr{O}$. It takes a little bit of work to show that such a quotient exists, but it is not very hard. (The calculations appear in [Sno], and they probably are also somewhere in [KW].) We let $\widetilde{B}$ (resp. B) be the completed tensor product of the $R_v^\square$ (resp. $R_v^\dagger$) for $v \in S \cup S_p$. We let $R^\square$ be the universal framed deformation ring for $\overline{\rho}$ unramified outside of S. We put $R^\dagger = R^\square \otimes_{\widetilde{B}} B$ and let $R^\ddagger$ be the unframed version of $R^\dagger$.

Now, we have a presentation for $R^\square$ over $\widetilde{B}$ [Ki, Prop. 4.1.5]:

$$R^\square = \widetilde{B}[\![x_1, \ldots, x_{r+n-1}]\!]/(f_1, \ldots, f_{r+s})$$

where $s = \sum_{v \mid \infty} \dim H^0(F_v, \mathrm{ad}^\circ \overline{\rho})$, n is the cardinality of $S \cup S_p$ and r is some non-negative integer. Tensoring this over $\widetilde{B}$ with B gives

$$R^\dagger = B[\![x_1, \ldots, x_{r+n-1}]\!]/(f_1, \ldots, f_{r+s})$$

Now, since $\overline{\rho}$ is odd, we have $s = [F : \mathbf{Q}]$. On the other hand, the dimension of B is $[F : \mathbf{Q}] + 3n + 1$. We conclude that $R^\dagger$ has dimension at least $4n$. Since $R^\dagger$ is a power series ring over $R^\ddagger$ in $4n - 1$ variables, we find that $R^\ddagger$ has dimension at least 1.

Let F'/F be a finite totally real extension over which $\overline{\rho}$ becomes modular, by an ordinary modular form of level prime to p. We can then define deformation rings for $\overline{\rho}|_{F'}$ analgous to the ones we have defined for $\overline{\rho}$. We will denote these rings with an overline. There is a natural map $\overline{R} \to R$ (the universal unframed deformation rings unramified outside of S), which is easily verified to be a finite map of rings. It follows that the induced map $\overline{R}^\ddagger \to R^\ddagger$ is finite as well. Now, to establish our modularity lifting theorem we identified $\overline{R}^\ddagger[1/p]$ with a Hecke algebra using a patching argument. Out of this argument we obtained another piece of information: that $\overline{R}^\ddagger$ itself, without p inverted, is finite over $\mathscr{O}$. (Actually, we did not quite use the ring $\overline{R}^\ddagger$, we needed to make a slight modification of the local deformation ring at p. Nonetheless, the same argument establishes the finiteness of $\overline{R}^\ddagger$.) We now conclude that $R^\ddagger$ itself is finite over $\mathscr{O}$.

We have thus show that $R^\ddagger$ is finite over $\mathscr{O}$ and has Krull dimension at least one. These two properties imply that $R^\ddagger$ cannot consist soley of p-power torsion. Therefore $R^\ddagger[1/p]$ is non-zero, and so there exists some homomorphism $R^\ddagger \to \overline{\mathbf{Q}}_p$. The corresponding deformation is the representation ρ that we are required to produce. □

Remark 21. One can still prove that $\overline{\rho}$ admits a nice lift without the assumption that $\overline{\rho}|_{F_v}$ admit an ordinary crystalline lift for each $v \mid p$. Of course, without this assumption the resulting lift cannot be assured to be ordinary. Not surprisingly, this more general statement makes use of more general modularity lifting theorems.

6. Remarks on Serre's conjecture

Recall Serre's conjecture:

Conjecture 22. *Any odd semi-simple representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ is modular.*

When $\overline{\rho}$ is reducible it is easy to see that it is easy to see that $\overline{\rho}$ is modular. This is very far from the case when $\overline{\rho}$ is irreducible. However, Khare and Wintenberger proved this a few years ago. We now give some idea of the proof.

To begin with, Serre made a stronger conjecture, specifying the optimal weight and level of a modular form giving rise to $\overline{\rho}$. (See Akshay's talk for more details along these lines.) The level $N(\overline{\rho})$ is just the prime-to-p Artin conductor of $\overline{\rho}$. Thus is $N(\overline{\rho})$ always prime to p, and $\ell \mid N(\overline{\rho})$ if and only if $\overline{\rho}$ is ramified at ℓ. The weight $k(\overline{\rho})$ is more complicated to define, but it can be bounded in terms of p. It is known that if $\overline{\rho}$ is modular then it is modular of this optimal weight and level. Furthermore, the work we have done in §4 and §5 can be generalized to show that $\overline{\rho}$ lifts to a strongly compatible system of weight $k(\overline{\rho})$ and conductor $N(\overline{\rho})$. This uses more advanced modularity lifting theorems. (The weight of a p-adic representation is defined using p-adic Hodge theory. The conductor of a p-adic representation is a product of the usual prime-to-p part together with a p-part coming from p-adic Hodge theory. If $\{\rho_\ell\}$ is a strongly compatible system then all the ρ_ℓ have the same weight and conductor.)

We begin by discussing the level one case of Serre's conjecture. We have the following result:

Proposition 23 (Serre, Tate)**.** *Conjecture 22 holds if $N(\overline{\rho}) = 1$ and $p = 2$ or $p = 3$.*

The $p = 2$ case is due to Tate, the $p = 3$ case to Serre. In fact, there are no cusp forms of level 1 and small weight, so the above proposition is really saying that there are no irreducible representations $G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ ramified only at p for $p = 2, 3$.

This result allows one to try to attempt an inductive argument. Let $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ have $N(\overline{\rho}) = 1$. Lift $\overline{\rho}$ to a compatible system $\{\rho_\ell\}$ of conductor 1 and weight $k = k(\overline{\rho})$. By the above result, we know that the reduction of ρ_3 is modular. We would like to use a modularity lifting theorem to conclude that ρ_3 is modular. Of course, this is going to require a more powerful modularity lifting theorem than we have discussed. Such theorems do exist (and can handle, for instance, the fact that $\overline{\rho}_3$ will be reducible), but they are not completely unconditional: the weight has to be small compared to p. Thus if one is going to apply a modularity lifting theorem in characteristic 3 the weight has to be quite small (maybe 3 or 4). Our compatible system $\{\rho_\ell\}$ can have arbitrarily large weight, so this is a real problem! (One might think to try to lift our original $\overline{\rho}$ to a small weight p-adic representation unramified outside of p, and then put this in a compatible system. This is possible, but the small weight p-adic representation will typically have a conductor at p; this means that the 3-adic representation will ramify at p and we can no longer use the theorems of Serre and Tate.)

To get around this problem, Khare (who proved the level one case before he and Wintenberger established the general case) employs an inductive argument on the weight and the prime. I do not know the details of how this works, so I cannot explain it.

Now consider the general case, where $N(\overline{\rho})$ is no longer assumed to be 1. The proof of Khare–Wintenberger is again an induction, but now the level is considered as well. Here is one way the level can be cut down: lift $\overline{\rho}$ to a compatible system $\{\rho_\ell\}$. Say $\ell \mid N(\overline{\rho})$. Then look at $\overline{\rho}_\ell$. By definition, its Serre-level is prime to ℓ. If we were just inducting on the level, then we could assume that $\overline{\rho}_\ell$ were modular (since it has smaller level than $\overline{\rho}$). Of course, we would then like to conclude that ρ_ℓ is modular as well. However, the available modularity lifting theorems may not be strong enough for us to make this deduction — for instance, the weight could be too larger compared to ℓ. I think the argument of Khare–Wintenberger runs induction on several things at once to get around this sort of issue. Again, I do not know the details, so I will leave it at that.

References

[Die] L. Dieulefait, *Uniform behavior of families of Galois representations on Siegel modular forms and the endoscopy conjecture*, Bol. Soc. Mat. Mexicana (3) **13** (2007), no. 2, 243–253.

[Ki] M. Kisin, *Modularity of 2-dimensional Galois representations*, Current Developements in Mathematics (2005), 191–230.

[KW] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (II)*, preprint, 76 pages.

[MB] L. Moret-Bailly, *Groupes de Picard et problèmes de Skolem II.*, Ann. Sci. de l'É.N.S. (4) **22** (1989) no. 2, 181–194.

[Rap] M. Rapoport, *Compactifications de l'espace de modules de Hilbert-Blumental*, Compositio Math. **36** (1978), no. 3, 255–335.

[Tay] R. Taylor, *Remarks on a conjecture of Fontaine and Mazur*, J. Inst. Math. Jussieu 1 (2002), no. 1, 125–143.

[Tay2] R. Taylor, *On the meromorphic continuation of degree two L-functions*, Documenta Math., Exta Volume: John H. Coates' Sixtieth Birthday (2006), 729–779 (electronic).

[Sno] A. Snowden, *Weight two representations of totally real fiels*, arxiv/0905.4266.