Lecture 18: Overview of the Taylor-Wiles method

Andrew Snowden
March 11, 2010

1. Statement of theorem

The goal of this lecture is to sketch a proof of the following modularity lifting theorem.

Theorem 1. *Let $F/\mathbf{Q}$ be a totally real number field and let $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$ be a continuous representation of its absolute Galois group, with $p > 5$. Assume that ρ satisfies the following conditions:*

- *ρ ramifies at only finitely many places.*
- *ρ is odd, i.e., $\det \rho(c) = -1$ for all complex conjugations $c \in G_F$.*
- *ρ is potentially crystalline and ordinary at all places above p.*
- *$\overline{\rho}|_{G_{F(\zeta_p)}}$ is absolutely irreducible.*
- *There exists a parallel weight two Hilbert modular form f such that ρ_f is potentially crystalline and ordinary at all places above p and $\overline{\rho} = \overline{\rho}_f$.*

Then there exists a Hilbert modular form g such that $\rho = \rho_g$.

We will prove this theorem by proving an $R = \mathbf{T}$ theorem, where R is a deformation ring of $\overline{\rho}$ with certain local conditions imposed and $\mathbf{T}$ is a certain Hecke algebra. Clearly, if we have an appropriate $R = \mathbf{T}$ theorem then we get a modularity lifting theorem, as ρ defines a homomorphism $R \to \overline{\mathbf{Q}}_p$ and thus (by $R = \mathbf{T}$), a homomorphism $\mathbf{T} \to \overline{\mathbf{Q}}_p$, which is the same as a modular form.

2. Initial reductions

As we have previously explained, by using base change we may pass to totally real solvable extensions of F. The hypotheses of the theorem imply that $\det \rho$ is of the form $\chi_p \psi$ where ψ is a finite order character of G_F. It is not difficult to see that there is a totally real solvable extension F'/F such that $\psi|_{G_{F'}} = (\psi')^2$ for some finite order character ψ' of G_F. Thus $(\psi')^{-1} \rho_f|_{G_{F'}}$ has determinant χ_p. Since twisting by a character does not affect modularity, it is enough to show that $(\psi')^{-1} \rho|_{G_{F'}}$ is modular. We may therefore assume $\det \rho = \chi_p$. Similarly, after possibly another base change, we can assume that $\det \rho_f = \chi_p$ as well.

Let $v \nmid p$ be a place of F. Call a representation $G_{F_v} \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$ *Steinberg* if it is of the form

$$\begin{pmatrix} \chi_p & * \\ & 1 \end{pmatrix}.$$

If $\rho_v : G_{F_v} \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$ is any continuous representation, then there is a finite extension F'_v/F_v such that $\rho_v|_{G_{F'_v}}$ is either unramified or Steinberg. We may thus make a global solvable extension F'/F such that $\rho|_{G_{F'}}$ and $\rho_f|_{G_{F'}}$ are unramified or Steinberg at all places away from p. Let S be the set of places (away from p) at which ρ is ramified (and thus Steinberg), and let S' be the corresponding set for ρ_f. By making another solvable extension, we may assume that $\rho|_{G_{F_v}}$ and $\rho_f|_{G_{F_v}}$ are crystalline at $v \mid p$. Finally, we may pass to another solvable extension and assume that $\overline{\rho}|_{G_{F_v}}$ and $\overline{\rho}_f|_{G_{F_v}}$ are trivial at all places v above p or in $S \cup S'$.

Now, we will not be able to prove the strongest possible form of an $R = \mathbf{T}$ theorem. We must impose the following hypothesis: the local deformation spaces used to construct R must be connected. Practically speaking, this means that $\rho|_{G_{F_v}}$ and $\rho_f|_{G_{F_v}}$ must lie on the same irreducible component of the universal semi-stable deformation space of $\overline{\rho}|_{G_{F_v}}$. What are the components of this space? For $v \mid p$ there are three components: ordinary crystalline, ordinary non-crystalline and non-ordinary. Thus our "ordinary and crystalline" hypotheses ensure that there is no problem at the places above p. Unramified representations always lie on the same component, so there is no problem outside of $S \cup S'$. However, if $v \nmid p$ then the universal semi-stable deformation space of the trivial representation has two components: unramified and Steinberg. We must therefore assume $S = S'$, which is a non-trivial assumption that may not be satisfied by the ρ_f that is given to us. However, one can always find a congruence with a form f' which does satisfy this condition. (Finding this f' is not at all trivial, but occurs outside the scope of the $R = \mathbf{T}$ theorem, and we will not discuss it further in this lecture.)

By making a further base change, we may assume that F has even degree over $\mathbf{Q}$ and that S has even cardinality.

3. The $R = \mathbf{T}$ theorem: set-up

We begin by precisely stating the situation in which we have placed ourselves. We have a representation

$$\overline{\rho} : G_F \to \mathrm{GL}_2(k)$$

where k is a finite field of characteristic p, a finite set S of places of F away from p and a modular representation ρ_f lifting $\overline{\rho}$. Let S_p denote the places of F above p. We assume the following hypotheses:

- (A1) ρ_f is crystalline and ordinary at all places in S_p, Steinberg at all places in S and unramified at all other places.
- (A2) $\det \rho_f = \chi_p$.
- (A3) $\overline{\rho}|_{G_{F(\zeta_p)}}$ is absolutely irreducible.
- (A4) $\overline{\rho}|_{G_{F_v}}$ is trivial for $v \in S_p \cup S$.
- (A5) F has even degree over $\mathbf{Q}$ and S has even cardinailty.

Note that the representation we had previously called ρ has completely disappeared from the set-up. It may not be absolutely necessary to assume (A4), but it does not cost us anything to do so, and makes study of the local deformation rings a bit easier.

We now define the ring R. Let $\widetilde{R}$ be the universal deformation ring of $\overline{\rho}$ unramified outside of $S \cup S_p$ and with determinant χ_p. (Here we take coefficients in some fixed $\mathscr{O}/\mathbf{Z}_p$ with residue field k.) For a place v let $\widetilde{R}_v$ be the universal deformation ring of $\overline{\rho}|_{G_{F_v}}$ with determinant χ_p. For $v \in S_p$ let R_v be the quotient of $\widetilde{R}_v$ classifying ordinary crystalline representations. For $v \in S$ let R_v be the quotient of $\widetilde{R}_v$ classifying Steinberg representations. We then let R be the tensor product of $\widetilde{R}$ with $\otimes R_v$ over $\otimes \widetilde{R}_v$. The latter tensor products are over $S \cup S_p$ and we should complete these tensor products.

We now define the Hecke algebra. Let D be the unique quaternion algebra over F ramifying at all the infinite places and the places in S (and nowhere else). This exists by (A5). For a compact open set U of $(D \otimes \mathbf{A}_F^f)^\times$ let $S_2(U)$ denote the set of functions

$$X(U) = D^\times \backslash (D \otimes \mathbf{A}_F^f)^\times / ((\mathbf{A}_F^f)^\times \cdot U) \to \mathscr{O}.$$

For places v at which U is maximal and D unramified, there is a Hecke operator T_v acting on $S_2(U)$.

Let U° be "the" maximal compact open subgroup of $(D \otimes \mathbf{A}_F^f)^\times$. Let $\mathbf{T}^{(p)}$ be the subalgebra of $\mathrm{End}(S_2(U^\circ))$ generated by the Hecke operators T_v for $v \notin S_p \cup S$. Let $\mathbf{T}$ be the subalgebra generated by the T_v for $v \notin S$. Thus $\mathbf{T}$ contains the Hecke operators above p and $\mathbf{T}^{(p)}$ does not. By the Jacquet-Langlands correspondence and conditions (A1) and (A2), our modular form f can be transferred to an element of $S_2(U^\circ)$ which is an eigenform for $\mathbf{T}$. The form f defines a homomorphism $\mathbf{T} \to \mathscr{O}$, the kernel of which is contained in a unique maximal ideal $\mathfrak{m}$. The form f is actually irrelevant; all that matters is the ideal $\mathfrak{m}$. It has the following two properties (which characterize it uniquely):

- For $v \notin S \cup S_p$, the image of T_v in $\mathbf{T}/\mathfrak{m}$ is equal to $\mathrm{tr}\, \overline{\rho}(\mathrm{Frob}_v)$.
- For $v \in S_p$, the Hecke operator T_v does not belong to $\mathfrak{m}$.

The first condition means that $\mathfrak{m}$ is associated to the representation $\overline{\rho}$; the second is the ordinarity condition. We regard $\mathfrak{m}$ as an ideal of $\mathbf{T}^{(p)}$ by contraction. (Remark: we need the group U° to satisfy a certain smallness condition which our group U° does not. To get a correct definition of U° one picks an auxiliary place v_{aux} with certain nice properties and takes $U^\circ_{v_{\mathrm{aux}}}$ to be sufficiently small; away from v_{aux} the group U° is maximal. One must also modify the definition of R to allow for ramification at v_{aux}. We will ignore this subtlety for now.)

As we have seen, there is a representation

$$G_F \to \mathrm{GL}_2(\mathbf{T}_{\mathfrak{m}}^{(p)}),$$

which lifts $\overline{\rho}$. This induces a surjection $\widetilde{R} \to \mathbf{T}_{\mathfrak{m}}^{(p)}$. The above representation is Steinberg at all the places in S (since D ramifies at S and local and global Langlands are compatible). However, it is not necessarily ordinary at the places in S_p (though it is automatically crystalline). This should not be surprising, as we have not told $\mathbf{T}_{\mathfrak{m}}^{(p)}$ anything about what is happening at p. There is a map $\mathbf{T}_{\mathfrak{m}}^{(p)} \to \mathbf{T}_{\mathfrak{m}}$; composing this with the above representation gives a representation

$$G_F \to \mathrm{GL}_2(\mathbf{T}_{\mathfrak{m}}).$$

This representation *is* ordinary at the places above p; one should think that the Hecke operators at p specify the local component of the deformation space at p. Thus the map $\widetilde{R} \to \mathbf{T}_{\mathfrak{m}}$ factors through R. Unfortunately, this map is no longer surjective. However, it is not very far from being surjective and the problem can be controlled locally at p: for $v \in S_p$ there is a modified local deformation ring R'_v which is a finite R_v-algebra and isomorphic to R_v after p is inverted. Define R' to be like R but use R'_v for $v \in S_p$. Then there is a natural surjection $R' \to \mathbf{T}_{\mathfrak{m}}$. Our goal is to prove:

Theorem 2. *The map $R'[1/p] \to \mathbf{T}_{\mathfrak{m}}[1/p]$ is an isomorphism and R' is finite over $\mathscr{O}$.*

The ring $\mathbf{T}_{\mathfrak{m}}$ is torsion-free by consturction. This theorem does not allow us to control the torsion in R', except to say that it is finite. One expects that R' is torsion free; this may actually be proved in the case we are in (the ordinary case), but I do not know for certain. One can modify the proof of the above theorem to show that R is finite over $\mathscr{O}$, which is often more relevant but does not seem to follow formally from the finiteness of R'.

4. Taylor-Wiles primes

The basic idea to the proof of Theorem 2 (called the Taylor-Wiles method) is to find a tower of maps $R_n \to T_n$ lifting $R' \to \mathbf{T}_{\mathfrak{m}}$ and then build a sort of inverse limit R_∞ and T_∞ out of the R_n and T_n, which is a nice ring. We can then prove that $R_\infty[1/p] \to T_\infty[1/p]$ is an isomorphism and deduce from this the statement we want. Actually, the Hecke algebras will not be so important; they will be replaced by spaces of modular forms.

We find the rings R_n be introducing certain auxiliary deformation rings. By a *TW set of places* we mean a finite set Q of places of F satisfying the following conditions:

- Q is disjoint from S_p and S. (And does not contain v_{aux}.)
- $\mathbf{N}\,v = 1 \pmod p$ for all $v \in Q$.
- The eigenvalues of $\overline{\rho}(\mathrm{Frob}_v)$ are distinct and belong to k.

(The "belong to k" part is not serious — we can replace k by its quadratic extension and then all eigenvalues of all Frobenii belong to k.) Given such a set Q of places, we define R_Q similarly to R' except we allow ramification at the places in Q. Note that $R_\emptyset = R'$. We will typically write $R_\emptyset$ in place of R' for notational uniformity.

Although we did not impose any deformation conditions at the places in Q, the conditions on the places in Q has strong consequences. Let $v \in Q$. Then the universal deformation $G_F \to \mathrm{GL}_2(R_Q)$ restricted to G_{F_v} is a sum of two characters $\eta_1 \oplus \eta_2$. These characters are necessarily tamely ramified, since their reduction is unramified, and in fact the image of inertia is p-power. By class field theory, η_1 defines a map $F_v^\times \to R_Q^\times$. We thus get a map $(\mathscr{O}_{F_v}/\mathfrak{p}_v)^\times \to R_Q^\times$, which factors through the maximal p-power quotient of $(\mathscr{O}_{F_v}/\mathfrak{p}_v)^\times$. Define Δ_Q to be the product of the maximal p-power quotients of $(\mathscr{O}_{F_v}/\mathfrak{p}_v)^\times$ for $v \in Q$. Then we have just given R_Q the structure of an $\mathscr{O}[\Delta_Q]$-algebra. This was not quite canonical, since we had to choose η_1. Define a *TW datum* to be a pair $(Q, \{\alpha_v\})$ where Q is a TW set of primes and α_v is a chosen eigenvalue of $\overline{\rho}(\mathrm{Frob}_v)$ for each place $v \in Q$. Given such a datum we get a canonical $\mathscr{O}[\Delta_Q]$-algebra structure on R_Q, since we can take η_1 to correspond to α_v. The following result is not difficult:

Proposition 3. *The canonical map $R_Q \to R_\emptyset$ is surjective. Its kernel is $\mathfrak{a}_Q R_Q$, where $\mathfrak{a}_Q$ is the augmentation ideal of $\mathscr{O}[\Delta_Q]$.*

We now define the auxiliary Hecke algebras and spaces of modular forms. Thus let $(Q, \{\alpha_v\})$ be a TW-datum. We define compact open subgroups $U_Q \subset V_Q$. At places $v \notin Q$, we define $U_{Q,v} = V_{Q,v} = U_v^\circ$. Let $v \in Q$. We then define

$$V_{Q,v} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathscr{O}_{F_v}) \;\middle|\; c \in \mathfrak{p}_v \right\}$$

and

$$U_{Q,v} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathscr{O}_{F_v}) \;\middle|\; c \in \mathfrak{p}_v \text{ and } ad^{-1} \text{ maps to 1 in } \Delta_Q \right\}.$$

Of course, $V_\emptyset = U_\emptyset = U^\circ$. Note that U_Q is normal in V_Q and V_Q/U_Q is identified with Δ_Q.

Let $\mathbf{T}(V_Q)$ be the subalgebra of $\mathrm{End}(S_2(V_Q))$ generated by the T_v for $v \notin S \cup Q$, and let $\mathbf{T}_+(V_Q)$ be the subalgebra generated by these T_v together with the U_v for $v \in Q$. We have a map $\mathbf{T}(V_Q) \to \mathbf{T}(V_\emptyset)$ and can thus regard $\mathfrak{m}$ as an ideal of $\mathbf{T}(V_Q)$. We also have a map $\mathbf{T}(V_Q) \to \mathbf{T}_+(V_Q)$. Let $\mathfrak{n}_Q$ be the ideal of $\mathbf{T}_+(V_Q)$ generated by $\mathfrak{m}$ and $U_v - \alpha_v$ for $v \in Q$. We then have the following result:

Proposition 4. *We have an isomorphism $S_2(V_Q)_{\mathfrak{n}_Q} = S_2(U^\circ)_{\mathfrak{m}}$.*

Proof. We just indicate the map $S_2(U^\circ)_{\mathfrak{m}} \to S_2(V_Q)_{\mathfrak{n}_Q}$ in the case that $Q = \{v\}$ (it suffices to treat this case by an inductive argument). By Hensel's lemma we have a factorization

$$X^2 - T_v X + \mathbf{N}\, v = (X - A)(X - B)$$

for A and B in $\mathbf{T}(U^\circ)_{\mathfrak{m}}$, with A mapping to α_v modulo $\mathfrak{m}$. We thus have a map

$$S_2(U^\circ)_{\mathfrak{m}} \to S_2(V_Q), \qquad f \mapsto Af - \begin{pmatrix} 1 & \\ & \varpi_v \end{pmatrix} f.$$

Here ϖ_v denotes a uniformizer at v and the operator U_v is defined using the double coset of $\begin{pmatrix} \varpi_v & \\ & 1 \end{pmatrix}$. One must show that the above map actually lands in $S_2(V_Q)_{\mathfrak{n}_Q}$ (which we think of as a summand of $S_2(V_Q)$) and that it is an isomorphism. Note in particular, that the proposition implies that $S_2(V_Q)_{\mathfrak{n}_Q}$ consists only of old forms. We note that there is also an isomorphism $\mathbf{T}_+(V_Q)_{\mathfrak{n}_Q} = \mathbf{T}_{\mathfrak{m}}$, though we will not need it. □

Let $\mathbf{T}_+(U_Q)$ be the subalgebra of $\mathrm{End}(S_2(U_Q))$ generated by the T_v for $v \notin S \cup Q$ and the U_v for $v \in Q$. There is a natural map $\mathbf{T}_+(U_Q) \to \mathbf{T}'_+(V_Q)$. We let $\mathfrak{m}_Q$ be the contraction of $\mathfrak{n}_Q$ under this map. We let T_Q be the localization $\mathbf{T}_+(U_Q)_{\mathfrak{m}_Q}$ and we let M_Q be the localization $S_2(U_Q)_{\mathfrak{m}_Q}$. Note that $T_\emptyset = \mathbf{T}_{\mathfrak{m}}$ and that $V_Q/U_Q = \Delta_Q$ acts on M_Q. We then have

Proposition 5. *The space M_Q is free over $\mathscr{O}[\Delta_Q]$. There is a natural isomorphism $M_Q/\mathfrak{a}_Q M_Q \to M_\emptyset$.*

Proof. The map $X(U_Q) \to X(V_Q)$ is a Galois cover with group Δ_Q. (This uses the smallness hypothesis on U°.) From this, one easily deduces that M_Q is free over $\mathscr{O}[\Delta_Q]$ and that $M_Q/\mathfrak{a}_Q M_Q$ is naturally isomorphic to $S_2(V_Q)_{\mathfrak{n}_Q}$. To get the isomorphism with $M_\emptyset$ apply the previous proposition. □

We have a Galois representation $G_F \to \mathrm{GL}_2(T_Q^{(p)})$, which yields a surjection $\widetilde{R}_Q \to T_Q^{(p)}$ (where $\widetilde{R}_Q$ is the universal deformation ring of $\overline{\rho}$ unramified outside $S \cup S_p \cup Q$). This Galois representation is not necessarily ordinary at the places above p, but the induced representation $G_F \to \mathrm{GL}_2(T_Q)$ is. The resulting map $\widetilde{R}_Q \to T_Q$ is not longer surjective, but there is a natural surjection $R_Q \to T_Q$ of $\widetilde{R}_Q$-algebras.

In the next section, it will be important to have framed versions of everything. For $v \in S \cup S_p$ we let $R_v^\square$ be the framed local deformation ring. (It is actually the only one that makes sense; what we had called R_v before does not really exist as a ring.) We let $(R'_v)^\square$ be the modification at places above p. We let B be the tensor product of the $R_v^\square$ for $v \in S$ and the $(R'_v)^\square$ for $v \in S_p$. We let $R_Q^\square$ be like R_Q but have framings at all places in $S \cup S_p$. It is an algebra over B. Finally, we define $T_Q^\square = T_Q \otimes_{R_Q} R_Q^\square$ and $M_Q^\square = M_Q \otimes_{T_Q} T_Q^\square$.

5. The patching argument

For each TW set of primes we have constructed a ring R_Q and given it the structure of a module over $\mathscr{O}[\Delta_Q]$, which is a ring of the form $\mathscr{O}[T_1, \ldots, T_n]/(T_i^{p^{a_i}} = 1)$ where $n = \#Q$. We would like to use various Q's to build a ring R_∞ which is an algebra over $\mathscr{O}[\![T_1, \ldots, T_n]\!]$ for some n (which does not obviously factor through a large quotient). To do this, we need to hold $\#Q$ fixed and let its elements have norm congruent to 1 modulo higher and higher powers of p. There will not be natural maps between the various R_Q's, but we will nonetheless manage to find maps between pieces of these rings by a sort of pigeonhole principle.

We now assume that we can find integers h and g and for each n a TW set of primes Q_n satisfying the following conditions:

- $\#Q_n = h$
- $\mathbf{N}\, v = 1 \pmod{p^n}$ for all $v \in Q_n$
- $R_{Q_n}^\square$ is topologically generated by g elements over B.

We extend each Q_n to a TW datum by arbitrarily choosing eigenvalues. We write $R_n^\square$ in place of $R_{Q_n}^\square$, and make this convention for other notations (e.g., $M_n^\square$). We did not give motivation for the last condition, but it is a natural condition to impose if we want patched ring $R_\infty^\square$ to be finitely generated. We fix surjections $B[\![z_1, \ldots, z_g]\!] \to R_n^\square$ for each n.

For a complete local ring A let $\mathfrak{m}_A$ denote its maximal ideal. Also, let $\mathfrak{m}_A^{(n)}$ denote the ideal generated by nth powers of elements of A; this is not the same as $\mathfrak{m}_A^n$. Let $\ell = 4(\#S_p + \#S) - 1$ and define

$$P = \mathscr{O}[\![x_1, \ldots, x_\ell, y_1, \ldots, y_h]\!].$$

We make $R_n^\square$ into a P-algebra by letting the x_i be the framing variables and letting the y_i act through a chosen surjection $\mathscr{O}[\![y_1, \ldots, y_h]\!] \to \mathscr{O}[\Delta_n]$. For an integer n let $\mathfrak{c}_n$ be the ideal of P generated by

$$(\pi^n, x_1^{p^n}, \ldots, x_\ell^{p^n}, (y_1+1)^{p^n} - 1, \ldots, (y_h+1)^{p^n} - 1)$$

(where π is a uniformizer of $\mathscr{O}$). Let s denote the rank of M_0 over $\mathscr{O}$. For an integer n let $r_n = snp^n(h+\ell)$. We remind the reader that $R_n^\square$ is an algebra over B and that $M_n^\square$ is an $R_n^\square$-module.

A *patching datum of level* n consists of the following:

- A complete local B-algebra D with $\mathfrak{m}_D^{(r_n)} = 0$.
- A map of $\mathscr{O}$-algebras $P/\mathfrak{c}_n \to D$.
- A surjection of B-algebras $D \to R_0^\square/(\mathfrak{c}_n R_0^\square + \mathfrak{m}_{R_0^\square}^{(r_n)})$.
- A surjection of B-algebras $B[\![z_1, \ldots, z_g]\!] \to D$.
- A D-module L which is finite free over $P/\mathfrak{c}_n$ of rank s.
- A surjection of $B[\![z_1, \ldots, z_g]\!]$ modules $L \to M_0^\square/\mathfrak{c}_n M_0^\square$.

The number of elements of D is finite (it can be bounded in terms of B and n). We thus find that, up to the obvious notion of isomorphism, there are only finitely many patching data of a given level.

Let $m \geq n$ be integers. Put

$$D_{n,m} = R_m^\square/(\mathfrak{c}_n R_m^\square + \mathfrak{m}_{R_m^\square}^{(r_n)}), \qquad L_{n,m} = M_m^\square/\mathfrak{c}_n M_m^\square.$$

One verifies that $(D_{n,m}, L_{n,m})$ is a patching datum of level n. Since there only only finitely many patching data of a given level, we can pass to a subsequence and assume $D_{n,m} = D_{n,n}$ and $L_{n,m} = L_{n,n}$ for all $m \geq n$. Denote the common value by D_n and L_n. Then the maps

$$D_{n+1}/(\mathfrak{c}_n D_{n+1} + \mathfrak{m}_{D_{n+1}}^{(r_n)}) \to D_n, \qquad L_{n+1}/\mathfrak{c}_n L_n \to L_n$$

are isomorphisms.

Let $R_\infty^\square$ be the inverse limit of the D_n and $M_\infty^\square$ the inverse limit of the L_n. The space $M_\infty^\square$ is a free P-module of rank s. The ring $R_\infty^\square$ is a P-algebra and a B-algebra, and there is a given surjection

$$B[\![z_1, \ldots, z_g]\!] \to R_\infty^\square.$$

Since P is a power series ring, the map $P \to R_\infty^\square$ can be lifted through the above surjection. We now have the following lemma:

Lemma 6. *Let $R \to S$ be a map of noetherian domains of the same dimension and let M be a non-zero S-module which is finite projective over R. Then $R \to S$ is a finite map. If R and S are regular then M is a finite projective faithful S-module.*

Now, by the way we chose our deformation conditions, B is a domain and $B[1/p]$ is smooth over $\mathbf{Q}_p$. (These are theorems that we need to prove!) Note that B being a domain is the hypothesis mentioned at the beginning of these notes, that our local deformation spaces needed to be irreducible. We now assume:

$$\dim B = 1 + h + \ell - g.$$

We will address this assumption below. This dimension assumption implies that P and $B[\![z_1, \ldots, z_g]\!]$ have the same dimension. We conclude from the lemma that $B[\![z_1, \ldots, z_g]\!]$ is finite over P and $M[1/p]$ is a faithful $B[\![z_1, \ldots, z_g]\!][1/p]$ module. The former implies that $R_\infty^\square$ is finite over P while the latter implies that $M_\infty^\square[1/p]$ is a faithful $R_\infty^\square[1/p]$ module (since the map $B[\![z_1, \ldots, z_g]\!] \to \mathrm{End}(M_\infty^\square)$ factors through $R_\infty^\square$).

Now, by the construction of $R_\infty^\square$ and $M_\infty^\square$ we have isomorphisms

$$R_\infty^\square/(y_1, \ldots, y_h)R_\infty^\square \to R_0^\square, \qquad M_\infty^\square/(y_1, \ldots, y_h)M_\infty^\square \to M_0^\square.$$

It follows that $R_0^\square$ is finite over $\mathscr{O}[\![x_1, \dots, x_\ell]\!]$, which implies that R_0 is finite over $\mathscr{O}$. Since $M_0^\square$ is free over P, we see that the action of $R_0^\square[1/p]$ on $M_0^\square[1/p]$ is still faithful. Since this action came via the map $R_0^\square \to T_0^\square$, we conclude that $R_0^\square[1/p] \to T_0^\square[1/p]$ is injective. Since we already knew this to be surjective, it must be an isomorphism.

6. Resolving the assumptions

In the last section we proved Theorem 2 assuming the following: there exist integers h and g satisfying

$$\dim B = 1 + h + \ell - g$$

such that for every integer n there is a set of primes Q_n satisfying:

- $\#Q_n = h$
- $\mathbf{N}\, v = 1 \pmod{p^n}$ for all $v \in Q_n$
- R_{Q_n} is topologically generated by g elements over B.

In fact, one can find Q_n as above with

$$\begin{aligned} h &= \dim H^1(G_{F,S}, \mathrm{ad}^\circ \overline{\rho}(1)) \\ g &= h - [F : \mathbf{Q}] + \#S + \#S_p - 1. \end{aligned}$$

The proof of this will probably require its own talk; it is purely Galois theoretic and makes no use of modular forms. It uses condition (A3), the assumption $p > 5$ and certain conditions on v_{aux} that we did not state. Now,

$$\dim R_v - \dim \mathscr{O} = \begin{cases} 3 & v \in S \\ 3 + [F_v : \mathbf{Q}_p] & v \in S_p \end{cases}$$

and so

$$\begin{aligned} \dim B - \dim \mathscr{O} &= \sum_{v \in S} 3 + \sum_{v \in S_p} (3 + [F_v : \mathbf{Q}_p]) \\ &= 3\#S + 3\#S_p + [F : \mathbf{Q}] \\ &= h + \ell - g. \end{aligned}$$

(Since B is the tensor product of the R_v over $\mathscr{O}$, the *relative* dimension of B over $\mathscr{O}$ is the sum of the relative dimensions of the R_v over $\mathscr{O}$.) Therefore everything works!