Ring Theoretic Properties of Certain Hecke Algebras

Richard Taylor
D.P.M.M.S.,
Cambridge University,
16 Mill Lane,
Cambridge,
CB2 1SB,
U.K.

Andrew Wiles
Department of Mathematics,
Princeton University,
Washington Road,
Princeton,
NJ 08544,
U.S.A.

7 October 1994

Introduction

In the work of one of us (A.W.) on the conjecture that all elliptic curves defined over $\mathbb{Q}$ are modular, the importance of knowing that certain Hecke algebras are complete intersections was established. The purpose of this article is to provide the missing ingredient in [W2] by establishing that the Hecke algebras considered there are complete intersections. As is recorded in [W2], a method going back to Mazur [M] allows one to show that these algebras are Gorenstein, but this seems to be too weak for the purposes of that paper. The methods of this paper are related to those of chapter 3 of [W2].

We would like to thank Henri Darmon, Fred Diamond and Gerd Faltings for carefully reading the first version of this article. Gerd Faltings has also suggested a simplification of our argument and we would like to thank him for allowing us to reproduce this in the appendix to this paper. R.T. would like to thank A.W. for his invitation to collaborate on these problems and for sharing his many insights into the questions considered. R.T. would also like to thank Princeton University, Université de Paris 7 and Harvard University for their hospitality during some of the work on this paper. A.W. was supported by an NSF grant.

1 Notation

Let p denote an odd prime, let $\mathcal{O}$ denote the ring of integers of a finite extension $K/\mathbb{Q}_p$, let λ denote its maximal ideal and let $k = \mathcal{O}/\lambda$.

If L is a perfect field G_L will denote its absolute Galois group and if the characteristic of L is not p then $\epsilon : G_L \to \mathbb{Z}_p^\times$ will denote the p-adic cyclotomic character. If L is a number field and $\wp$ a prime of its ring of integers then $G_\wp$ will denote a decomposition group at $\wp$ and $I_\wp$ the corresponding inertia group. We will denote by $\mathrm{Frob}_\wp$ the arithmetic Frobenius element of $G_\wp/I_\wp$.

If G is a group and M a G-module we will let M^G and M_G denote respectively the invariants and coinvariants of G on M. If ρ is a representation of G into the automorphisms of some abelian group we shall let V_ρ denote the underlying G-module. If H is a normal subgroup of G then we shall let ρ^H and ρ_H denote the representation of G/H on respectively V_ρ^H and $V_{\rho,H}$.

We shall also fix a continuous representation

$$\overline{\rho} : G_{\mathbb{Q}} \longrightarrow GL_2(k)$$

with the following properties.

- $\overline{\rho}$ is modular in the sense that it is a mod$p$ representation associated to some modular newform of some weight and level.
- The restriction of $\overline{\rho}$ to the group $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}))$ is absolutely irreducible.
- If c denotes complex conjugation then $\det \overline{\rho}(c) = -1$.
- The restriction of $\overline{\rho}$ to the decomposition group at p either has the form

$$\begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$$

  with ψ_1 and ψ_2 distinct characters and with ψ_2 unramified; or is induced from a character χ of the unramified quadratic extension of $\mathbb{Q}_p$ whose restriction to the inertia group is the fundamental character of level 2, $I_p \twoheadrightarrow \mathbb{F}_{p^2}^\times$.
- If $l \neq p$ then
  - either $\overline{\rho}|_{I_l} \sim \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix}$,

– or $\overline{\rho}|_{I_l} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$,

– or $\overline{\rho}|_{G_l}$ is absolutely irreducible and in the case $\overline{\rho}|_{I_l}$ is absolutely reducible we have $l \not\equiv -1 \bmod p$.

(This implies that $\overline{\rho}|_{G_l}$ is either unramified or of type A, B or C as defined in chapter 1 of [W2]. On the other hand if $\overline{\rho}|_{G_l}$ is of type A, B or C then some twist satisfies the condition above.)

In the case that $\overline{\rho}|_{G_p} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$ we will fix the pair of characters ψ_1, ψ_2. Note that in some cases this may involve making a choice.

We will let Q denote a finite set of primes q with the properties

- $\overline{\rho}$ is unramified at q,
- $q \equiv 1 \bmod p$,
- $\overline{\rho}(\mathrm{Frob}_q)$ has distinct eigenvalues, which we shall denote α_q and β_q.

Much of our notation will involve a subscript Q to denote dependence on Q, whenever $Q = \emptyset$ we may simply drop it from the notation.

For $q \in Q$ we shall let Δ_q denote the Sylow p-subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times$. We shall let δ_q denote a generator. We will write Δ_Q for the product of the Δ_q with $q \in Q$. We will let $\mathfrak{a}_Q$ denote the kernel of the map $\mathcal{O}[\Delta_Q] \to \mathcal{O}$ which sends every element of Δ_Q to 1. Let χ_q denote the character

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}\,(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times \twoheadrightarrow \Delta_q,$$

and let $\chi_Q = \prod_{q \in Q} \chi_q$.

We will denote by N_Q the product of the following quantities:

- the conductor of $\overline{\rho}$;
- the primes in Q;
- p, if $\overline{\rho}$ is not flat (i.e. $\overline{\rho}$ does not arise from the action of G_p on the $\overline{\mathbb{Q}}_p$-points of some finite flat group scheme over $\mathbb{Z}_p$) or if $\det \overline{\rho}|_{I_p} \neq \epsilon$. (We remark that if $\overline{\rho}|_{G_p}$ is flat but $\det \overline{\rho}|_{I_p} \neq \epsilon$ then $\overline{\rho}|_{G_p}$ arises from an etale group scheme over $\mathbb{Z}_p$. We also note that in [W2] the term flat is not used when the group scheme is ordinary.)

We will let Γ_Q denote the inverse image under $\Gamma_0(N_Q) \to (\mathbb{Z}/N_Q\mathbb{Z})^\times$ of the product of the following subgroups:

- the Sylow p-subgroup of $(\mathbb{Z}/M\mathbb{Z})^\times$, where M denotes the conductor of $\overline{\rho}$;

- for each $q \in Q$ the unique maximal subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times$ of order prime to p.

Let $\mathbb{T}(\Gamma_Q)$ denote the $\mathbb{Z}$-subalgebra of the complex endomorphisms of the space of weight 2 cusp forms on Γ_Q which is generated by the Hecke operators T_l and $\langle l \rangle$ for $l \not| pN_Q$, by U_q for $q \in Q$ and by U_p if $p|N_Q$. Let $\mathfrak{m}$ denote the ideal of $\mathbb{T}(\Gamma_Q) \otimes_{\mathbb{Z}} \mathcal{O}$ generated by λ, by $\operatorname{tr} \overline{\rho}(\operatorname{Frob}_l) - T_l$ and $\det \overline{\rho}(\operatorname{Frob}_l) - l\langle l \rangle$ for $l \not| pN_Q$, by $U_q - \alpha_q$ for $q \in Q$ and by $U_p - \psi_2(\operatorname{Frob}_p)$ if $p|N_Q$. Note that if $Q \neq \emptyset$ this definition only makes sense if $\mathcal{O}$ is sufficiently large that k contains the eigenvalues of $\overline{\rho}(\operatorname{Frob}_q)$ for all $q \in Q$. It is a deep result following from the work of many mathematicians that $\mathfrak{m}$ is a proper ideal (see [D]), and so maximal. We let $\mathbb{T}_Q$ denote the localisation of $\mathbb{T}(\Gamma_Q) \otimes_{\mathbb{Z}} \mathcal{O}$ at $\mathfrak{m}$. Note that $\mathbb{T}_Q$ is reduced because the operators T_l for $l \not| N_Q$ act semi-simply on the space of cusp forms for Γ_Q and the U_q for $q \in Q$ act semi-simply on all common eigenspaces for the T_l for which the corresponding p-adic representation τ is either ramified at q or for which $\tau(\operatorname{Frob}_q)$ has distinct eigenvalues. There is a natural map $\mathcal{O}[\Delta_Q] \to \mathbb{T}_Q$, which sends $x \in \Delta_Q$ to $\langle y \rangle$ where $y \in \mathbb{Z}$, $y \equiv x \bmod q$ for all $q \in Q$ and $y \equiv 1 \bmod N_\emptyset$.

It follows from the discussion after theorem 2.1 of [W2] or from the work of Carayol [C2] that there is a continuous representation

$$\rho_Q^{mod} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{T}_Q);$$

such that if $l \not| N_Q p$ then ρ_Q^{mod} is unramified at l and we have $\operatorname{tr} \rho_Q^{mod}(\operatorname{Frob}_l) = T_l$ and $\det \rho_Q^{mod}(\operatorname{Frob}_l) = l\langle l \rangle$. In particular the reduction of ρ_Q^{mod} modulo the maximal ideal of $\mathbb{T}_Q$ is $\overline{\rho}$. From [C1] we can deduce the following.

- If $q \in Q$ then $\rho_Q^{mod}|_{G_q} = \phi_1 \oplus \phi_2$ where ϕ_1 is unramified and $\phi_1(\operatorname{Frob}_q) = U_q$, and where $\phi_2|_{I_q} = \chi_q|_{I_q}$.

- If $l \neq p$ and $\overline{\rho}|_{I_l}$ is non-trivial but unipotent then $\rho_Q^{mod}|_{I_l}$ is unipotent.

- If $l \notin Q \cup \{p\}$ and either $\overline{\rho}|_{I_l} = \chi \oplus 1$ or $\overline{\rho}|_{G_l}$ is absolutely irreducible then $\rho_Q^{mod}(I_l) \xrightarrow{\sim} \overline{\rho}(I_l)$.

- $\det \rho_Q^{mod} = \chi_Q \epsilon \phi$ where ϕ is a character of order prime to p.

Moreover if $\overline{\rho}|_{G_p}$ is flat and if $\det \overline{\rho}|_{I_p} = \epsilon$ then $p \not| N_Q$ so $\rho_Q^{mod}|_{G_p}$ is flat (i.e. the reduction modulo every ideal of finite index is flat). If $\overline{\rho}|_{G_p}$ is not flat or if $\det \overline{\rho}|_{I_p} \neq \epsilon$ then $p|N_Q$, $\overline{\rho}|_{G_p} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$ and U_p is a unit in $\mathbb{T}_Q$. It follows from theorem 2 of [W1] (or more directly in the case $\psi_1|_{I_q} \neq \epsilon$ from proposition 12.9 of [G]) that $\rho_Q^{mod}|_{G_p} \sim \begin{pmatrix} \chi_1\epsilon & * \\ 0 & \chi_2 \end{pmatrix}$, where χ_2 is unramified and $\chi_1(I_p)$ has order prime to p. In the case that χ_1 is unramified we know further that $\chi_1 = \chi_2$ (see proposition 1.1 of [W2]) and that this character has finite order. It will be convenient to introduce the twist $\rho'_Q = \rho_Q^{mod} \otimes \chi_Q^{-1/2}$ of ρ_Q^{mod}. In particular we see that $\det \rho'_Q$ is valued in $\mathcal{O}^\times$.

The main theorem of this paper is as follows. Recall that we may write $\mathbb{T}$ for $\mathbb{T}_\emptyset$.

Theorem 1 *The ring $\mathbb{T}$ is a complete intersection.*

We note that if $\mathcal{O}'$ is the ring of integers of a finite extension K'/K then the ring constructed using $\mathcal{O}'$ in place of $\mathcal{O}$ is just $\mathbb{T}_Q \otimes_{\mathcal{O}} \mathcal{O}'$. Also $\mathbb{T}$ is a complete intersection if and only if $\mathbb{T} \otimes_{\mathcal{O}} \mathcal{O}'$ is (using for instance corollary 2.8 on page 209 of [K2]). Thus we may and we shall assume that $\mathcal{O}$ is sufficiently large that the eigenvalues of every element of $\overline{\rho}$ are rational over k and that there is a homomorphism $\pi : \mathbb{T} \twoheadrightarrow \mathcal{O}$. In particular the definition of $\mathbb{T}_Q$ makes sense for all Q. There is an induced map $\pi_Q : \mathbb{T}_Q \to \mathbb{T} \to \mathcal{O}$. The map $\mathbb{T}_Q \to \mathbb{T}$ takes the operators T_l and $\langle l \rangle$ to themselves and the operator U_q to the unique root of $U^2 - T_q U + q\langle q \rangle$ in $\mathbb{T}$ above α_q. We will let $\wp_Q$ denote the kernel of π_Q and will let η_Q denote the ideal $\pi_Q(\mathrm{Ann}_{\mathbb{T}_Q}(\wp_Q))$. Then it is known that $\infty > \#\wp_Q/\wp_Q^2 \geq \#\mathcal{O}/\eta_Q$ with equality if and only if $\mathbb{T}_Q$ is a complete intersection (see the appendix of [W2] or [L], we are using the fact that $\mathbb{T}_Q$ is reduced).

2 Generalisation of a Result of de Shalit

In this section we shall use the methods of de Shalit (see [dS]) to prove the following theorem.

Theorem 2 *The ring $\mathbb{T}_Q$ is a free $\mathcal{O}[\Delta_Q]$ module of $\mathcal{O}[\Delta_Q]$-rank equal to the $\mathcal{O}$-rank of $\mathbb{T}$.*

By lemma 3 of [DT] we may choose a prime R with the following properties:

- $R \nmid 6N_Q p$;
- $R \not\equiv 1 \bmod p$;

- $\overline{\rho}(\mathrm{Frob}_R)$ has distinct eigenvalues α_R and β_R;
- $(1+R)^2 \det \overline{\rho}(\mathrm{Frob}_R) \neq R(\mathrm{tr}\,\overline{\rho}(\mathrm{Frob}_R))^2$.

Let Γ_{Q-} be defined in the same way as Γ_Q but with $(\mathbb{Z}/q\mathbb{Z})^\times$ replacing its maximal subgroup of order prime to p in the definition for each $q \in Q$. Let $\Gamma'_Q = \Gamma_Q \cap \Gamma_1(R)$ and let $\Gamma'_{Q-} = \Gamma_{Q-} \cap \Gamma_1(R)$. The purpose of introducing the auxiliary prime R is to make these groups act freely on the upper half complex plane. Let $\mathbb{T}'(\Gamma'_Q)$ denote the $\mathbb{Z}$-subalgebra of the complex endomorphism ring of the space of weight two modular (not necessarily cusp) forms generated by the operators T_l and $\langle l \rangle$ for $l \not| N_Q R$ and by U_l for $l | N_Q R$. Let $\mathfrak{m}'_Q$ denote the maximal ideal of $\mathbb{T}'(\Gamma'_Q) \otimes_{\mathbb{Z}} \mathcal{O}$ generated by the following elements:

- λ;
- $T_l - \mathrm{tr}\,\overline{\rho}(\mathrm{Frob}_l)$ and $l\langle l \rangle - \det \overline{\rho}(\mathrm{Frob}_l)$ for $l \not| N_Q R p$;
- $U_q - \alpha_q$ for $q \in Q$ or $q = R$;
- $U_l - \mathrm{tr}\,\overline{\rho}_{I_l}(\mathrm{Frob}_l)$ if $l | N_\emptyset$ and $l \neq p$;
- $U_p - \psi_2(\mathrm{Frob}_p)$ if $p | N_\emptyset$;
- $T_p - \mathrm{tr}\,\overline{\rho}_{I_p}(\mathrm{Frob}_p)$ if $p \not| N_\emptyset$.

Let $\mathbb{T}'_Q$ denote the localisation of $\mathbb{T}'(\Gamma'_Q) \otimes_{\mathbb{Z}} \mathcal{O}$ at $\mathfrak{m}'_Q$. Let Y'_Q denote the quotient of the upper half complex plane by Γ'_Q and let X'_Q denote its standard compactification. Complex conjugation c acts continuously on these Riemann surfaces. We let $H^1(Y'_Q, \mathcal{O})^\pm$ and $H^1(X'_Q, \mathcal{O})^\pm$ denote the ± 1 eigenspaces of c on $H^1(Y'_Q, \mathcal{O})$ and $H^1(X'_Q, \mathcal{O})$. All these definitions go over verbatim, but with $Q-$ replacing Q.

Lemma 1 $\mathbb{T}'_Q \cong \mathbb{T}_Q$ *and* $\mathbb{T}'_{Q-} \cong \mathbb{T}$.

This is a standard argument which we will only sketch. First observe that because $\overline{\rho}$ is irreducible $\mathbb{T}'_Q$ and $\mathbb{T}'_{Q-}$ can be defined using the ring generated by the Hecke operators on the spaces of weight two cusp forms $S_2(\Gamma'_Q)$ and $S_2(\Gamma'_{Q-})$ (rather than spaces of all modular forms). The same arguments as in the proof of proposition 2.15 of [W2] show that we can drop the Hecke operators T_p if $p \not| N_Q$ and the Hecke operators U_l for $l \neq p$ and $l | N_\emptyset$ from the definition without changing the Hecke algebra. Next we will show that we need only consider the algebras generated in the endomorphisms of $S_2(\Gamma_Q)^2 \subset S_2(\Gamma'_Q)$ and $S_2(\Gamma)^{2^{\#Q+1}} \subset S_2(\Gamma'_{Q-})$. This follows from the following facts.

- As $R \not\equiv 1 \bmod p$ and $\det \overline{\rho}$ is unramified at R, no component of $\mathbb{T}'_Q$ nor of $\mathbb{T}'_{Q-}$ can correspond to an eigenform with a non-trivial action of $(\mathbb{Z}/R\mathbb{Z})^\times$.

- As $\alpha_R/\beta_R \neq R^{\pm 1}$ in k, no component of $\mathbb{T}'_Q$ nor of $\mathbb{T}'_{Q-}$ can correspond to an eigenform which is special at R (i.e. an eigenform which corresponds to a cuspidal automorphic representation of $GL_2(\mathbb{A})$ whose component at R is special).

- As for each prime $q \in Q$, $\alpha_q/\beta_q \neq q^{\pm 1}$ in k, no component of $\mathbb{T}'_{Q-}$ can correspond to an eigenform which is special at q.

The ring generated by the Hecke operators T_l and $\langle l \rangle$ for $l \not| pN_QR$, by U_q for $q \in Q \cup \{R\}$ and by U_p if $p|N_Q$ on $S_2(\Gamma_Q)^2$ is isomorphic to $\mathbb{T}(\Gamma_Q)[u_R]/(u_R^2 - T_R u_R + R\langle R \rangle)$. In fact U_R acts by the matrix

$$\begin{pmatrix} T_R & 1 \\ -R\langle R \rangle & 0 \end{pmatrix}$$

on $S_2(\Gamma_Q)^2$. Similarly the ring generated by the Hecke operators T_l and $\langle l \rangle$ for $l \not| pN_QR$, by U_q for $q \in Q \cup \{R\}$ and by U_p if $p|N_Q$ on $S_2(\Gamma)^{2^{\#Q+1}}$ is isomorphic to $\mathbb{T}(\Gamma)[u_q \ : \ q \in Q \cup \{R\}]/(u_q^2 - T_q u_q + q\langle q \rangle \ : \ q \in Q \cup \{R\})$. Tensoring with $\mathcal{O}$ and localising at the appropriate maximal ideal we get the desired isomorphism. We have to use the fact that $u_R^2 - T_R u_R + R\langle R \rangle$ has two roots in $\mathbb{T}_Q$ with distinct reductions modulo the maximal ideal and the similar facts over $\mathbb{T}$ for $u_q^2 - T_q u_q + q\langle q \rangle$ with $q \in Q \cup \{R\}$.

Because $\overline{\rho}$ is irreducible we see that $H^1(Y'_Q, \mathcal{O})_{\mathfrak{m}'_Q} = H^1(X'_Q, \mathcal{O})_{\mathfrak{m}'_Q}$ and that $H^1(Y'_{Q-}, \mathcal{O})_{\mathfrak{m}'_{Q-}} = H^1(X'_{Q-}, \mathcal{O})_{\mathfrak{m}'_{Q-}}$. By corollary 1 of theorem 2.1 of [W2] we see that $H^1(X'_Q, \mathcal{O})^{\pm}_{\mathfrak{m}'_Q}$ are free rank one $\mathbb{T}'_Q$-modules and that $H^1(X'_{Q-}, \mathcal{O})^{\pm}_{\mathfrak{m}'_{Q-}}$ are free rank one $\mathbb{T}'_{Q-}$-modules. Hence it will suffice to prove the following proposition.

Proposition 1 *$H^1(Y'_Q, \mathcal{O})^-$ is a free $\mathcal{O}[\Delta_Q]$-module, with $\mathcal{O}[\Delta_Q]$-rank equal to the $\mathcal{O}$-rank of $H^1(Y'_{Q-}, \mathcal{O})^-$.*

Because $H^1(Y'_{Q-}, K) = H^1(Y'_Q, K)^{\Delta_Q}$ we need only show that $H^1(Y'_Q, \mathcal{O})^-$ is a free $\mathcal{O}[\Delta_Q]$-module. Because $R \geq 5$, Γ'_{Q-} acts freely on the upper half complex plane and so may be identified with the fundamental group of Y'_{Q-}. In particular we see that Γ'_{Q-} is a free group. Similarly Γ'_Q acts freely on the upper half complex plane and we get identifications

$$H^1(Y'_Q, \mathcal{O}) \cong H^1(\Gamma'_Q, \mathcal{O}) \cong H^1(\Gamma'_{Q-}, \mathcal{O}[\Delta_Q]),$$

the latter arising from Shapiro's lemma. Under these identifications complex conjugation goes over to the involution induced by conjugation by $\xi = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and trivial action on the coefficients. (This follows because the action of c on Y'_Q is induced by the map $z \mapsto -\overline{z}$ of the upper half complex plane to itself.)

Because Γ'_{Q-} is a free group, the cocycles $Z^1(\Gamma'_{Q-}, \mathcal{O}[\Delta_Q])$ are a free $\mathcal{O}[\Delta_Q]$-module. (If $\gamma_1, ..., \gamma_a$ are free generators of Γ'_{Q-} then we have an isomorphism

$$\begin{array}{rcl} Z^1(\Gamma'_{Q-}, \mathcal{O}[\Delta_Q]) & \xrightarrow{\sim} & \mathcal{O}[\Delta_Q]^a \\ \psi & \mapsto & (\psi(\gamma_1), ..., \psi(\gamma_a)).) \end{array}$$

On the other hand ξ acts trivially on Δ_Q and so the coboundaries are contained in $Z^1(\Gamma'_{Q-}, \mathcal{O}[\Delta_Q])^+$. Thus $H^1(Y'_Q, \mathcal{O})^- \cong Z^1(\Gamma'_{Q-}, \mathcal{O}[\Delta_Q])^-$ is a free $\mathcal{O}[\Delta_Q]$-module, as desired.

Before leaving this section we remark the following corollaries of theorem 2.

Corollary 1 *If $q \notin Q$ then $\mathbb{T}_{Q\cup\{q\}}/(\delta_q - 1) \xrightarrow{\sim} \mathbb{T}_Q$. Moreover $(\delta_q - 1)\mathbb{T}_{Q\cup\{q\}}$ and $(1 + \delta_q + ... + \delta_q^{\#\Delta_q - 1})\mathbb{T}_{Q\cup\{q\}}$ are annihilators of each other in $\mathbb{T}_{Q\cup\{q\}}$.*

Corollary 2 *If for some Q the ring $\mathbb{T}_Q$ is a complete intersection then so is $\mathbb{T}$.*

The proof is by showing that under the assumption that $\mathbb{T}_{Q\cup\{q\}}$ is a complete intersection, so is $\mathbb{T}_Q$. The argument in section 2 of [K1] shows that if a complete local noetherian ring S is a complete intersection, if $f \in S$ and if $\mathrm{Hom}_S(S/(f), S) = \mathrm{Hom}_S(S/(f), \mathrm{Ann}\,_S(f))$ is a free $S/(f)$ module then $S/(f)$ is a complete intersection. We apply this result with $S = \mathbb{T}_{Q\cup\{q\}}$ and $f = \delta_q - 1$. The final condition is met because the annihilator of $\delta_q - 1$ in $\mathbb{T}_{Q\cup\{q\}}$ is a free rank one $\mathbb{T}_Q$ module by the last corollary.

Corollary 3 *$\eta_Q = \eta \# \Delta_Q$.*

We remind the reader that η_Q is defined at the end of section one and that $\eta = \eta_\emptyset$. The proof of the corollary is by showing that $\eta_{Q\cup\{q\}} = \eta_Q \# \Delta_q$ if $q \notin Q$. Write $Q' = Q \cup \{q\}$ and let θ denote the natural surjection $\mathbb{T}_{Q'} \twoheadrightarrow \mathbb{T}_Q$. It suffices to prove that in $\mathbb{T}_{Q'}$ we have the equation $\mathrm{Ann}\,\wp_{Q'} = (1 + \delta_q + ... + \delta_q^{\#\Delta_q - 1})\theta^{-1}(\mathrm{Ann}\,_{\mathbb{T}_Q}(\wp_Q))$. However $\theta^{-1}(\mathrm{Ann}\,_{\mathbb{T}_Q}(\wp_Q))$ is just the set of elements t of $\mathbb{T}_{Q'}$ for which $t\wp_{Q'} \subset (\delta_q - 1)\mathbb{T}_{Q'}$. The inclusion $\mathrm{Ann}\,\wp_{Q'} \supset (1 + \delta_q + ... + \delta_q^{\#\Delta_q - 1})\theta^{-1}(\mathrm{Ann}\,_{\mathbb{T}_Q}(\wp_Q))$ is now clear. Conversly if $t \in \mathrm{Ann}\,\wp_{Q'}$

then t annihilates $\ker\theta$ and hence $t = (1 + \delta_q + ... + \delta_q^{\#\Delta_q - 1})s$. Then we see that $s\wp_{Q'} \subset (\delta_q - 1)\mathbb{T}_{Q'}$, i.e. that $s \in \theta^{-1}(\mathrm{Ann}_{\mathbb{T}_Q}(\wp_Q))$. The other inclusion now follows.

Corollary 4 $\#(\mathfrak{a}_Q\mathbb{T}_Q/\wp_Q\mathfrak{a}_Q\mathbb{T}_Q)\#(\mathcal{O}/\eta) = \#(\mathcal{O}/\eta_Q)$.

To prove this corollary note that $\mathfrak{a}_Q/\mathfrak{a}_Q^2 \cong \bigoplus_{q\in Q} \mathcal{O}/\#\Delta_q$. Thus it follows from theorem 2 that $\mathfrak{a}_Q\mathbb{T}_Q/\mathfrak{a}_Q^2\mathbb{T}_Q \cong \mathbb{T}_Q \otimes_{\mathcal{O}[\Delta_Q]} \mathfrak{a}_Q/\mathfrak{a}_Q^2 \cong \bigoplus_{q\in Q} \mathbb{T}/\#\Delta_q$ and so we deduce that $\mathfrak{a}_Q\mathbb{T}_Q/\wp_Q\mathfrak{a}_Q\mathbb{T}_Q \cong \bigoplus_{q\in Q} \mathcal{O}/\#\Delta_q$. This corollary now follows from the last one.

3 Some Algebra

In this section we shall establish certain criteria for rings to be complete intersections. We shall rely on the numerical criterion established in the appendix of [W2]. In that appendix there is a Gorenstein hypothesis which can be checked in the cases where we will apply the results of this section. However in order to state the results of this section in somewhat greater generality we shall reference the paper [L], where the Gorenstein hypothesis in the appendix of [W2] is removed, rather than the appendix of [W2] directly.

Fix a finite flat reduced local $\mathcal{O}$ algebra T with a section $\pi : T \twoheadrightarrow \mathcal{O}$. We will consider complete local noetherian $\mathcal{O}$ algebras R together with maps $R \twoheadrightarrow T$. We will denote by J_R the kernel of the map $R \twoheadrightarrow T$, by π_R the induced map $R \twoheadrightarrow \mathcal{O}$, by $\wp_R$ the kernel of π_R and by η_R the image under π_R of the annihilator in R of $\wp_R$. We will let $\Psi_R = (\wp_R^2 \cap J_R)/\wp_R J_R$.

If $S \twoheadrightarrow R \twoheadrightarrow T$ then $\wp_S^2 \twoheadrightarrow \wp_R^2$, J_S is the pre-image of J_R and so $\Psi_S \twoheadrightarrow \Psi_R$.

We have an exact sequence

$$(0) \to \Psi_R \to J_R/\wp_R J_R \to \wp_R/\wp_R^2 \to \wp_T/\wp_T^2 \to (0).$$

From this we deduce the following facts.

- $\#\Psi_R < \infty$. (To see this it suffices to show that $(\Psi_R)_{\wp_R} = (0)$. However as T is reduced $(J_R)_{\wp_R} = (\wp_R)_{\wp_R}$ and so the map $(J_R/\wp_R J_R)_{\wp_R} \to (\wp_R/\wp_R^2)_{\wp_R}$ is an isomorphism. The result follows.)

- $\#\Psi_R\#(\wp_R/\wp_R^2) = \#(\wp_T/\wp_T^2)\#(J_R/\wp_R J_R)$.

Lemma 2 *Suppose we have the inequalities* $\#(\wp_T/\wp_T^2) \leq \#(\mathcal{O}/\eta_T)\#\Psi_R$ *and* $\#(\mathcal{O}/\eta_T)\#(J_R/\wp_R J_R) \leq \#(\mathcal{O}/\eta_R) < \infty$ *and suppose R is a finite flat $\mathcal{O}$-algebra. Then R is a complete intersection.*

To show this first note that we have the inequalities

$$\begin{array}{rcl} \#(\wp_R/\wp_R^2) & = & \#(\wp_T/\wp_T^2)\#(J_R/\wp_R J_R)/\#\Psi_R \\ & \leq & \#(\wp_T/\wp_T^2)\#(\mathcal{O}/\eta_R)/(\#\Psi_R\#(\mathcal{O}/\eta_T)) \\ & \leq & \#(\mathcal{O}/\eta_R). \end{array}$$

Now applying the criterion of [L] we see that R is a complete intersection.

Lemma 3 *We have the inequality:*

$$\#(\mathcal{O}/\eta_R) \leq \#(J_R/\wp_R J_R)\#(\mathcal{O}/\eta_T).$$

As $\mathrm{Fitt}_R(J_R) \subset \mathrm{Ann}_R(J_R)$ we see that $\mathrm{Fitt}_{\mathcal{O}}(J_R/\wp_R J_R) \subset \pi_R \mathrm{Ann}_R(J_R)$. On the other hand it is easy to see that

$$\mathrm{Ann}_R(\wp_R) \supset \{s \in R | s\wp_R \subset J_R\}\mathrm{Ann}_R(J_R).$$

Applying π_R we see that

$$\eta_R \supset \eta_T \mathrm{Fitt}_{\mathcal{O}}(J_R/\wp_R J_R),$$

and the lemma follows.

Lemma 4 *If R is a complete intersection which is finite and flat over $\mathcal{O}$ and $\eta_R \neq (0)$ then $\#(\wp_T/\wp_T^2) \leq \#(\mathcal{O}/\eta_T)\#\Psi_R$. If R is a power series ring the same result is true without the assumptions that it is finite over $\mathcal{O}$ and that $\eta_R \neq (0)$.*

For the first part we see that, as R is a complete intersection, $\#(\wp_R/\wp_R^2) = \#(\mathcal{O}/\eta_R)$ (see [L]). Thus we see that

$$\#\Psi_R\#(\mathcal{O}/\eta_R) = \#(\wp_T/\wp_T^2)\#(J_R/\wp_R J_R) \geq \#(\wp_T/\wp_T^2)\#(\mathcal{O}/\eta_R)/\#(\mathcal{O}/\eta_T).$$

The first result follows. For the second result note that we can factor $R \twoheadrightarrow T$ as $R \twoheadrightarrow R' \twoheadrightarrow T$ with R' a complete intersection which is finite and flat over $\mathcal{O}$ and for which $\wp_{R'}/\wp_{R'}^2 \xrightarrow{\sim} \wp_T/\wp_T^2$ (by the proof of lemma 9 of [L]). Then $\#\mathcal{O}/\eta_{R'} = \#\wp_{R'}/\wp_{R'}^2 < \infty$ and so $\#\wp_T/\wp_T^2 \leq \#(\mathcal{O}/\eta_T)\#\Psi_{R'}$. However $\Psi_R \twoheadrightarrow \Psi_{R'}$, so the result follows.

We now return to the notation of the first section. We will let Ψ_Q denote $\Psi_{\mathbb{T}_Q}$ and J_Q denote $J_{\mathbb{T}_Q}$.

Proposition 2 *Suppose that for a series of sets Q_n we have ideals I_n in $\mathbb{T}_{Q_n}$ with the following properties.*

1. *I_n is contained in $\mathfrak{m}^2_{\mathbb{T}_{Q_n}}$ and $\mathbb{T}_{Q_n}/I_n$ has finite cardinality.*

2. *$I_{n+1}\mathbb{T} \subset I_n\mathbb{T}$ and $\bigcap_n I_n\mathbb{T} = (0)$.*

3. *There is a surjective map of $\mathcal{O}$-algebras $\mathbb{T}_{Q_{n+1}}/I_{n+1} \twoheadrightarrow \mathbb{T}_{Q_n}/I_n$ such that the diagram*

$$\begin{array}{ccc} \mathbb{T}_{Q_{n+1}}/I_{n+1} & \longrightarrow & \mathbb{T}_{Q_n}/I_n \\ \downarrow & & \downarrow \\ \mathbb{T}/I_{n+1}\mathbb{T} & \longrightarrow & \mathbb{T}/I_n\mathbb{T} \end{array}$$

commutes. (Note that this map is not assumed to take a given Hecke operator to itself.)

4. *$\lim_{\leftarrow} \mathbb{T}_{Q_n}/I_n$ is a power series ring.*

Then for n sufficiently large $\mathbb{T}_{Q_n}$ is a complete intersection, and hence $\mathbb{T}$ is a complete intersection (by corollary 2 of theorem 2).

Let P denote $\lim_{\leftarrow} \mathbb{T}_{Q_n}/I_n$. We get a natural map $P \twoheadrightarrow \mathbb{T}$ and can choose maps $P \to \mathbb{T}_{Q_n}$ compatible with the maps $\mathbb{T}_{Q_n} \twoheadrightarrow \mathbb{T}$ and $\mathbb{T}_{Q_n} \twoheadrightarrow \mathbb{T}_{Q_n}/I_n$. Because $I_n \subset \mathfrak{m}^2_{\mathbb{T}_{Q_n}}$ we see that the map $P \to \mathbb{T}_{Q_n}$ is surjective. We have a sequence

$$\Psi_P \longrightarrow\!\!\!\!\!\rightarrow \Psi_{Q_n} \longrightarrow ((J_{Q_n} + I_n) \cap (\wp^2_{Q_n} + I_n))/(J_{Q_n}\wp_{Q_n} + I_n).$$

(Note that although the maps $P \to \mathbb{T}_{Q_n}$ and $\Psi_P \to \Psi_{Q_n}$ are not compatible as n varies the composite map above is.) Moreover $\Psi_P = \lim_{\leftarrow}((J_{Q_n}+I_n)\cap(\wp^2_{Q_n}+I_n))/(J_{Q_n}\wp_{Q_n}+I_n)$ (using the fact that $\mathbb{T}_{Q_n}/I_n$ is finite for all n) and so as Ψ_P is finite we have that the map $\Psi_P \to ((J_{Q_n} + I_n) \cap (\wp^2_{Q_n} + I_n))/(J_{Q_n}\wp_{Q_n} + I_n)$ is injective for n sufficiently large. Thus for n sufficiently large $\Psi_P \stackrel{\sim}{\to} \Psi_{Q_n}$. We deduce the inequality

$$\#(\wp/\wp^2) \leq \#(\mathcal{O}/\eta)\#\Psi_P = \#(\mathcal{O}/\eta)\#\Psi_{Q_n},$$

where the first inequality follows from lemma 4. The proposition follows on applying corollary 4 of theorem 2 and lemma 2.

Corollary 1 *Suppose that we have an integer r and a series of sets Q_m with the following properties:*

1. *if $q \in Q_m$ then $q \equiv 1 \bmod p^m$;*

2. *$\overline{\rho}$ is unramified at q and $\overline{\rho}(\mathrm{Frob}_q)$ has distinct eigenvalues;*

3. $\#Q_m = r$;

4. $\mathbb{T}_{Q_m}$ *can be generated as an* $\mathcal{O}$*-algebra by* r *elements.*

Then $\mathbb{T}$ *is a complete intersection.*

To prove this corollary it is useful to have the following definition. By a level n structure we shall mean a quadruple $B = (A, \alpha, \beta, \gamma)$, where

- A is an $\mathcal{O}$-algebra,
- $\alpha : \mathcal{O}[[T_1, ..., T_r]] \twoheadrightarrow A$,
- $\beta : \mathcal{O}[[S_1, ..., S_r]]/(p^n, (S_1+1)^{p^n} - 1, ..., (S_r+1)^{p^n} - 1) \to A$ makes A a free module over $\mathcal{O}[[S_1, ..., S_r]]/(p^n, (S_1+1)^{p^n} - 1, ..., (S_r+1)^{p^n} - 1)$,
- and $\gamma : A/(S_1, ..., S_r) \xrightarrow{\sim} \mathbb{T}/p^n$.

If B is a structure of level n and $n' \leq n$ then it induces a structure of level n' by reducing $\operatorname{mod}(p^{n'}, (S_1+1)^{p^{n'}} - 1, ..., (S_r+1)^{p^{n'}} - 1)$.

Let $A_m = \mathbb{T}_{Q_m}/(p^m, \delta_q^{p^m} - 1 | q \in Q_m)$. This extends to a level m structure that we will denote B_m. For $n \leq m$ we will let $B_{m,n}$ denote the level n structure induced by B_m. There are only finitely many isomorphism classes of structures of level n and so we may choose recursively integers $m(n)$ with the following two properties.

1. $B_{m(n),n-1} \cong B_{m(n-1),n-1}$.
2. $B_{m(n),n} \cong B_{m,n}$ for infinitely many integers m.

Let I_n denote the kernel of the map from $\mathbb{T}_{Q_{m(n)}}$ to the ring underlying $B_{m(n),n}$. We claim that the pairs $(Q_{m(n)}, I_n)$ for $n \geq 2$ satisfy the requirements of proposition 2 (we use $n \geq 2$ to ensure that $I_n \subset \mathfrak{m}_{Q_n}^2$). We need only check that $\lim_{\leftarrow} B_{m(n),n}$ is a power series ring. On the one hand it is a finite free $\mathcal{O}[[S_1, ..., S_r]]$-module, and so has Krull dimension $r+1$. On the other hand it is a quotient of $\mathcal{O}[[T_1, ..., T_r]]$ and so must in fact equal $\mathcal{O}[[T_1, ..., T_r]]$.

4 Galois Cohomology

It remains to find a sequence of sets Q_m with the properties of corollary 1 of proposition 2. We must recall some definitions in Galois cohomology. We define $H^1_f(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho})$.

1. If $l \neq p$ then $H^1_f(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho}) = H^1(\mathbb{F}_l, (\mathrm{ad}^0\overline{\rho})^{I_l}) = \ker(H^1(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho}) \to H^1(I_l, \mathrm{ad}^0\overline{\rho}))$.

2. If $\overline{\rho}|_{G_p}$ is flat and $\det \overline{\rho}|_{I_p} = \epsilon$ then we will let $H^1_f(\mathbb{Q}_p, \mathrm{ad}^0\overline{\rho})$ denote those elements in $H^1(\mathbb{Q}_p, \mathrm{ad}^0\overline{\rho}) \subset \mathrm{Ext}^1_{k[G_p]}(V_{\overline{\rho}}, V_{\overline{\rho}})$ which correspond to extensions which can be realised as the $\overline{\mathbb{Q}_p}$-points on the generic fibre of a finite flat group scheme over $\mathbb{Z}_p$.

3. If $\overline{\rho}|_{G_p} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$ with $\psi_1|_{I_p} \neq \epsilon$ then we let $H^1_f(\mathbb{Q}_p, \mathrm{ad}^0\overline{\rho})$ denote the kernel of $H^1(\mathbb{Q}_p, \mathrm{ad}^0\overline{\rho}) \to H^1(I_p, (\mathrm{ad}^0\overline{\rho})/\mathrm{Hom}_k(V_{\overline{\rho}}/F, F))$, where F denotes the line in $V_{\overline{\rho}}$ where G_p acts by the character ψ_1.

4. Finally if $\overline{\rho}|_{G_p} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$ with $\psi_1|_{I_p} = \epsilon$ but $\overline{\rho}$ is not flat then we will let $H^1_f(\mathbb{Q}_p, \mathrm{ad}^0\overline{\rho})$ denote the kernel of the map $H^1(\mathbb{Q}_p, \mathrm{ad}^0\overline{\rho}) \to H^1(\mathbb{Q}_p, (\mathrm{ad}^0\overline{\rho})/\mathrm{Hom}_k(V_{\overline{\rho}}/F, F))$, where F denotes the line in $V_{\overline{\rho}}$ where G_p acts by the character ψ_1.

We define $H^1_Q(\mathbb{Q}, \mathrm{ad}^0\overline{\rho})$ to be the inverse image under

$$H^1(\mathbb{Q}, \mathrm{ad}^0\overline{\rho}) \longrightarrow \prod_{l \notin Q} H^1(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho})$$

of $\prod_{l \notin Q} H^1_f(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho})$.

We also define $H^1_f(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho}(1))$ to be the annihilator of $H^1_f(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho})$ under the pairing of Tate local duality $H^1(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho}) \times H^1(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho}(1)) \to k$. We then define $H^1_{Q^*}(\mathbb{Q}, \mathrm{ad}^0\overline{\rho}(1))$ to be the inverse image under

$$H^1(\mathbb{Q}, \mathrm{ad}^0\overline{\rho}(1)) \longrightarrow \prod_{l \notin Q} H^1(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho}(1))$$

of $\prod_{l \notin Q} H^1_f(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho}(1))$.

Lemma 5 $\dim_k H^1_Q(\mathbb{Q}, \mathrm{ad}^0\overline{\rho}) \leq \dim_k H^1_{Q^*}(\mathbb{Q}, \mathrm{ad}^0\overline{\rho}(1)) + \#Q$

To see this we apply proposition 1.6 of [W2]. For $l \notin Q$ and $l \neq p$ we see that $h_l = 1$ because the index of $H^1_f(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho})$ in $H^1(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho})$ is equal to $\#H^1(I_l, \mathrm{ad}^0\overline{\rho})^{G_{\mathbb{F}_l}}$ which in turn equals

$$\#((\mathrm{ad}^0\overline{\rho}(-1))_{I_l})^{G_{\mathbb{F}_l}} = \#((\mathrm{ad}^0\overline{\rho}(1))^{I_l})_{G_{\mathbb{F}_l}} = \#H^0(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho}(1)).$$

For $q \in Q$ we have that $h_q = \#H^0(\mathbb{Q}_q, \mathrm{ad}^0\overline{\rho}(1)) = \#k$. It remains to check that $h_p h_\infty \leq 1$. In the case that $\overline{\rho}|_{G_p}$ is not flat or $\det \overline{\rho}|_{I_p} \neq \epsilon$ this is proved in parts (iii) and (iv) of proposition 1.9 of [W2]. Thus suppose that $\overline{\rho}|_{G_p}$ is flat and $\det \overline{\rho}|_{I_p} = \epsilon$. We must show that $\dim_k H^1_f(\mathbb{Q}_p, \mathrm{ad}^0\overline{\rho}) \leq 1 + \dim_k H^0(\mathbb{Q}_p, \mathrm{ad}^0\overline{\rho})$ ($= 1$ if $\overline{\rho}|_{G_p}$ is indecomposable and $= 2$ otherwise).

Following [FL] let $\mathcal{M}$ denote the abelian category of k vector spaces M with a distinguished subspace M^1 and a k-linear isomorphism $\phi : M/M^1 \oplus M^1 \xrightarrow{\sim} M$. Then there are equivalences of categories between:

- $\mathcal{M}^{op}$;
- finite flat group schemes $A/\mathbb{Z}_p$ with an action of k;
- $k[G_p]$-modules which are isomorphic as modules over $\mathbb{F}_p[G_p]$ to the $\overline{\mathbb{Q}_p}$ points of some finite flat group scheme over $\mathbb{Z}_p$.

See section 9 of [FL] for details. The only point here is that an action of k on the generic fibre of a finite flat group scheme over $\mathbb{Z}_p$ extends uniquely to an action on the whole scheme. Let $M(\overline{\rho})$ denote the object of $\mathcal{M}$ corresponding to $\overline{\rho}$. Then $\dim_k M(\overline{\rho}) = 2$ and $\dim_k M(\overline{\rho})^1 = 1$ (since $\det \overline{\rho}|_{I_p} = \epsilon$). We get an embedding $\mathrm{Ext}^1_{\mathcal{M}}(M(\overline{\rho}), M(\overline{\rho})) \hookrightarrow H^1(\mathbb{Q}_p, \mathrm{ad}\overline{\rho})$. We will show that

1. $\dim_k \mathrm{Ext}^1_{\mathcal{M}}(M(\overline{\rho}), M(\overline{\rho})) = 2$ if $\overline{\rho}|_{G_p}$ is indecomposable and $= 3$ otherwise;
2. the composite map $\mathrm{Ext}^1_{\mathcal{M}}(M(\overline{\rho}), M(\overline{\rho})) \hookrightarrow H^1(\mathbb{Q}_p, \mathrm{ad}\overline{\rho}) \xrightarrow{\mathrm{tr}} H^1(\mathbb{Q}_p, k)$ is non-trivial, where tr denotes the map induced by the trace.

The lemma will then follow.

For the first point it is explained in lemma 4.4 of [R] how to calculate $\mathrm{Ext}^1_{\mathcal{M}}(M(\overline{\rho}), M(\overline{\rho}))$. Let $\{e_0, e_1\}$ be a basis of $M(\overline{\rho})$ with $e_1 \in M(\overline{\rho})^1$. Let $\phi(e_0, 0) = \alpha e_0 + \beta e_1$ and $\phi(0, e_1) = \gamma e_0 + \delta e_1$. Then $\mathrm{Ext}^1_{\mathcal{M}}(M(\overline{\rho}), M(\overline{\rho}))$ can be identified as a k-vector space with $M_2(k)$ modulo the subspace of matrices of the form

$$\begin{pmatrix} r & 0 \\ s & t \end{pmatrix} \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} - \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} r & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} 0 & (r-t)\gamma \\ s\alpha + (t-r)\beta & s\gamma \end{pmatrix},$$

for any $r, s, t \in k$. Thus $\dim_k \mathrm{Ext}^1_{\mathcal{M}}(M(\overline{\rho}), M(\overline{\rho})) = 2$ if $\gamma \neq 0$ and $= 3$ if $\gamma = 0$. However $\gamma = 0$ if and only if $M(\overline{\rho})^1$ is a subobject of $M(\overline{\rho})$ in $\mathcal{M}$. This is true if and only if $\overline{\rho}$ has a one dimensional quotient on which inertia acts by ϵ which itself is true if and only if $\overline{\rho}|_{G_p}$ is decomposable.

For the second point consider the $k[G_p]$-module $\overline{\rho} \otimes \tau$ where τ is the unramified representation

$$\mathrm{Frob}_p \longmapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then $\overline{\rho} \otimes \tau$ is an extension of $\overline{\rho}$ by itself. Moreover its extension class maps to the element of $H^1(\mathbb{Q}_p, k) = \mathrm{Hom}(\mathbb{Q}_p^\times, k)$ which is trivial on $\mathbb{Z}_p^\times$ and takes $p \mapsto 2$. Finally it is isomorphic to the action of G_p on the $\overline{\mathbb{Q}_p}$ points of a finite flat group scheme over $\mathbb{Z}_p$, because this is true over an unramified extension.

Lemma 6 *$\mathbb{T}_Q$ can be generated as an $\mathcal{O}$ algebra by $\dim_k H^1_Q(\mathbb{Q}, \mathrm{ad}^0\overline{\rho})$ elements.*

Let $\mathfrak{m}_Q$ denote the maximal ideal of $\mathbb{T}_Q$. It will suffice to show that there is an embedding of k-vector spaces

$$\kappa : \mathrm{Hom}_k(\mathfrak{m}_Q/(\mathfrak{m}_Q^2, \lambda), k) \hookrightarrow H^1_Q(\mathbb{Q}, \mathrm{ad}^0\overline{\rho}).$$

We first define

$$\kappa : \mathrm{Hom}_k(\mathfrak{m}_Q/(\mathfrak{m}_Q^2, \lambda), k) \longrightarrow H^1(\mathbb{Q}, \mathrm{ad}\overline{\rho}).$$

If θ is a non-zero element of the left hand group we may extend it uniquely to a map of local $\mathcal{O}$-algebras $\tilde{\theta} : \mathbb{T}_Q \twoheadrightarrow k[\epsilon]$ where $\epsilon^2 = 0$. Let $\rho_\theta = \tilde{\theta} \circ \rho'_Q$. We get an exact sequence

$$(0) \longrightarrow V_{\overline{\rho}} \longrightarrow V_{\rho_\theta} \longrightarrow V_{\overline{\rho}} \longrightarrow (0),$$

and hence a class $\kappa(\theta)$ in $\mathrm{Ext}^1_{k[G_\mathbb{Q}]}(\overline{\rho}, \overline{\rho}) \cong H^1(\mathbb{Q}, \mathrm{ad}\overline{\rho})$. Because $\det \rho_\theta$ is valued in $k \subset k[\epsilon]$ we see that $\kappa(\theta)$ actually lies $H^1(\mathbb{Q}, \mathrm{ad}^0\overline{\rho})$.

We claim that $\mathrm{res}_l \kappa(\theta)$ lies in $H^1_f(\mathbb{Q}_l, \mathrm{ad}^0\overline{\rho})$ for $l \notin Q$. This computation is very similar to some in [W2], but is not actually carried out there, so we give an argument here. First suppose that $l \neq p$ and that either $p \not| \# \overline{\rho}(I_l)$ or $\overline{\rho}|_{G_l}$ is absolutely irreducible. In this case $\rho'_Q(I_l) \stackrel{\sim}{\to} \overline{\rho}(I_l)$ and $\det \rho'_Q|_{I_l}$ has order prime to l. Because either $p \not| \# \overline{\rho}(I_l)$ or $p = 3$ and $\mathrm{ad}\overline{\rho}(I_l) \cong A_4$ we have that $H^1(\overline{\rho}(I_l), \mathrm{ad}^0\overline{\rho}) = (0)$ and so $\rho_\theta|_{I_l} \cong \overline{\rho}|_{I_l} \otimes_k k[\epsilon]$. The result follows in this case. Secondly suppose that $\overline{\rho}|_{I_l}$ is unipotent and nontrivial. Then the same is true for $\rho'_Q|_{I_l}$ and then also for ρ_θ. However the Sylow p-subgroup of I_l is pro-cyclic and so $\rho_\theta|_{I_l}$ must also be of the form $\overline{\rho} \otimes_k k[\epsilon]$ and $\mathrm{res}_l \kappa(\theta) \in H^1(I_l, \mathrm{ad}^0(\overline{\rho}))$ must vanish. In the case $l = p$, $\overline{\rho}$ is flat and $\det \overline{\rho}|_{I_p} = \epsilon$ the claim is immediate from the definitions. In the case $l = p$ and $\overline{\rho}|_{G_p} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$ with $\psi_1|_{I_p} \neq \epsilon$

use the fact that $\rho'_Q|_{I_p} \sim \begin{pmatrix} \tilde{\psi}_1 & * \\ 0 & 1 \end{pmatrix}$ where $\tilde{\psi}_1$ denotes the Teichmuller lifting of $\psi_1|_{I_p}$. Finally in the case $l = p$, $\overline{\rho}|_{G_p} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$ with $\psi_1|_{I_p} = \epsilon$ but $\overline{\rho}$ not flat use the fact that

$$\rho'_Q|_{G_p} \sim \begin{pmatrix} \delta\epsilon & * \\ 0 & \delta \end{pmatrix}$$

where δ is an unramified character of order prime to p.

It remains to show that κ is injective. Suppose it were not. Then we could find a non-zero θ such that $\rho_\theta \sim \overline{\rho} \otimes_k k[\epsilon]$. Thus $\operatorname{tr} \rho'_Q$ is valued in $\mathcal{O} + \ker \tilde{\theta}$ and in particular $\mathbb{T}_Q$ is not generated as an $\mathcal{O}$-algebra by $\operatorname{tr} \rho'_Q$. We will show this is not the case. If $q \in Q$ and $\delta \in \Delta_q$ then we can find $\sigma \in G_q$ such that $(U_q\delta)^2 - (\operatorname{tr} \rho'_Q(\sigma))(U_q\delta) + \det \rho'_Q(\sigma) = 0$. ($\sigma$ will in fact lie above Frob_q.) This polynomial has distinct roots in k and so both its roots in $\mathbb{T}_Q$ lie in the sub-$\mathcal{O}$-algebra T generated by the image of $\operatorname{tr} \rho'_Q$. Thus for all $\delta \in \Delta_q$, $U_q\delta \in T$. Hence $U_q \in T$, and as U_q is a unit, $\delta \in T$. Moreover for all $l \notin Q$ for which $\overline{\rho}$ is unramified we see that $T_l\chi_Q(\mathrm{Frob}_l)^{-1/2} \in T$ and hence $T_l \in T$. If $p|N_Q$ then $U_p\chi_Q(\mathrm{Frob}_p)^{-1/2}$ is a root of the polynomial $X^2 - (\operatorname{tr} \rho'_Q(\sigma))X + \det \rho'_Q(\sigma)$ for any element σ of G_p which lies above Frob_p. For some σ over Frob_p this polynomial has two distinct roots in k and so $U_p \in T$. Thus $T = \mathbb{T}_Q$ as we required.

Finally we turn to the proof of the main theorem. As in [W2] (after equation (3.8)) we may find a set of primes Q_m with the following properties:

1. if $q \in Q_m$ then $q \equiv 1 \bmod p^m$;
2. if $q \in Q_m$ then $\overline{\rho}$ is unramified at q and $\overline{\rho}(\mathrm{Frob}_q)$ has distinct eigenvalues;
3. $H^1_{\emptyset^*}(\mathbb{Q}, \mathrm{ad}^0\overline{\rho}(1)) \hookrightarrow \bigoplus_{q \in Q_m} H^1(\mathbb{F}_q, \mathrm{ad}^0\overline{\rho}(1))$.

As for each such q, $H^1(\mathbb{F}_q, \mathrm{ad}^0\overline{\rho}) = k$ we see that by shrinking Q_m we may suppose that the latter map is an isomorphism. Then we have that $\#Q_m = \dim_k H^1_{\emptyset^*}(\mathbb{Q}, \mathrm{ad}^0\overline{\rho}(1))$. Also $H^1_{Q_m^*}(\mathbb{Q}, \mathrm{ad}^0\overline{\rho}(1))$ is the kernel of the map in 3. above and so is trivial. Thus by lemma 5 we see that $\dim_k H^1_{Q_m}(\mathbb{Q}, \mathrm{ad}^0\overline{\rho}) \leq \#Q_m$ and so $\mathbb{T}_{Q_m}$ can be generated by $\#Q_m = \dim_k H^1_{\emptyset^*}(\mathbb{Q}, \mathrm{ad}^0\overline{\rho}(1))$ elements. The main theorem now follows from corollary 1.

References

[C1] H.Carayol, *Sur les représentations p-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. Ec. Norm. Super. 19 (1986) 409-468.

[C2] H.Carayol, *Formes modulaires et représentations Galoisiennes à valeurs dans un anneau local complet*, in "p-adic monodromy and the Birch-Swinnerton-Dyer conjecture" (eds. B.Mazur and G.Stevens), Contemporary Math. 165 (1994).

[D] F.Diamond, *The refined conjecture of Serre*, to appear in the proceedings of the 1993 Hong Kong conference on modular forms and elliptic curves.

[DT] F.Diamond and R.Taylor, *Lifting modular mod l representations*, Duke Math. J. 74 (1994) 253-269.

[FL] J.-M.Fontaine and G.Lafaille, *Construction de représentations p-adiques*, Ann. Sci. Ec. Norm. Super. 15 (1982) 547-608.

[G] B.Gross, *A tameness criterion for Galois representations associated to modular forms* mod$p$, Duke Math. J. 61 (1990), 445-517.

[K1] E.Kunz, *Almost complete intersections are not Gorenstein*, J. of Algebra 28 (1974), 111-115.

[K2] E.Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser 1985.

[L] H.Lenstra, *Complete intersections and Gorenstein rings*, to appear in the proceedings of the 1993 Hong Kong conference on modular forms and elliptic curves.

[M] B.Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES 47 (1977), 133-186.

[dS] E. de Shalit, *On certain Galois representations related to the modular curve $X_1(p)$*, to appear in Compositio Math.

[R] R.Ramakrishna, *On a variation of Mazur's deformation functor*, Comp. Math. 87 (1993), 269-286.

[W1] A.Wiles, *On ordinary λ-adic representations associated to modular forms*, Invent. Math. 94 (1988), 529-573.

[W2] A.Wiles, *Modular elliptic curves and Fermat's last theorem*, preprint (1994).

Appendix

The purpose of this appendix is to explain certain simplifications to the arguments of chapter 3 of [W2] and to section 3 of this paper. These simplifications were found by G.Faltings and we would like to thank him for allowing us to include them here. We should make it clear that the arguments of this appendix (just as those of chapter 3 of [W2] and section 3 of this paper) apply only to proving conjecture 2.16 of [W2] for the minimal Hecke ring and minimal deformation problem. In order to prove theorem 3.3 of [W2] one needs to invoke theorem 2.17 and the arguments of chapter 2 of [W2].

We will keep the notation and assumptions of the main body of this paper. Let Q denote a finite set of primes as described in section 1 of this paper. By a deformation of $\overline{\rho}$ of type Q we shall mean a complete noetherian local $\mathcal{O}$-algebra A with residue field k together with an equivalence class of continuous representations $\rho : G_{\mathbb{Q}} \to GL_2(A)$ with the following properties:

- $\rho \bmod \mathfrak{m}_A = \overline{\rho}$;
- $\epsilon^{-1} \det \rho$ is a character of finite order prime to p;
- if $l \notin Q \cup \{p\}$ and $\overline{\rho}|_{I_l}$ is semi-simple then $\rho(I_l) \xrightarrow{\sim} \overline{\rho}(I_l)$;
- if $l \notin Q \cup \{p\}$ and $\overline{\rho}|_{I_l} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ then $\rho|_{I_l} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$;
- if $\overline{\rho}$ is flat and $\det \overline{\rho}|_{I_p} = \epsilon$ then ρ is flat;
- if either $\overline{\rho}$ is not flat or if $\det \overline{\rho}|_{I_p} \neq \epsilon$ then $\rho|_{G_p} \sim \begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix}$ where ϕ_2 is unramified and $\phi_2 \bmod \mathfrak{m}_A = \psi_2$.

As in chapter 1 of [W2] there is a universal lift $\rho_Q^{univ} : G_{\mathbb{Q}} \to GL_2(R_Q)$ of type Q. Recall that the universal property is for lifts up to conjugation. Moreover one checks (c.f. the second paragraph of the proof of lemma 6) that there is a natural isomorphism

$$\mathrm{Hom}_k(\mathfrak{m}_{R_Q}/(\lambda, \mathfrak{m}_{R_Q}^2), k) \cong H_Q^1(\mathbb{Q}, \mathrm{ad}^0 \overline{\rho}).$$

There is also a natural map $R_Q \to \mathbb{T}_Q$ so that ρ_Q^{univ} pushes forward to a conjugate of ρ_Q'.

Recall that if $Q = \emptyset$ we shall often drop it from the notation. In this appendix we shall reprove the following result.

Theorem 3 *$R \tilde{\to} \mathbb{T}$ and these rings are complete intersections.*

We note that if $\mathcal{O}'$ is the ring of integers of a finite extension K'/K then the rings $\mathbb{T}'_Q$ and R'_Q constructed using $\mathcal{O}'$ in place of $\mathcal{O}$ are just $\mathbb{T}_Q \otimes_{\mathcal{O}} \mathcal{O}'$ and $R_Q \otimes_{\mathcal{O}} \mathcal{O}'$. Also $\mathbb{T}_Q$ is a complete intersection if and only if $\mathbb{T}_Q \otimes_{\mathcal{O}} \mathcal{O}'$ is (using for instance corollary 2.8 on page 209 of [K2]). Thus we may and we shall assume that $\mathcal{O}$ is sufficiently large that the eigenvalues of every element of $\overline{\rho}(G_{\mathbb{Q}})$ are rational over k.

We recall that in the penultimate paragraph of section 4 of this paper we showed that $\mathbb{T}_Q$ is generated as an $\mathcal{O}$-algebra by $\operatorname{tr} \rho'_Q(G_{\mathbb{Q}})$. Thus we see that the map $R_Q \to \mathbb{T}_Q$ is a surjection.

We will need the following result.

Lemma 7 *If $q \in Q$ then $\rho_Q^{univ}|_{G_q} \sim \begin{pmatrix} \phi_1 & 0 \\ 0 & \phi_2 \end{pmatrix}$ where $\phi_1|_{I_q} = \phi_2|_{I_q}^{-1}$ and both these characters factor through $\chi_q : I_q \twoheadrightarrow \Delta_q$.*

It suffices to check the first assertion. As $\overline{\rho}$ is unramified at q, $\rho_Q^{univ}|_{G_q}$ factors through $\hat{\mathbb{Z}} \ltimes \mathbb{Z}_p(1)$, where $\hat{\mathbb{Z}}$ is topologically generated by some lift f of Frob_q, $\mathbb{Z}_p(1)$ is topologically generated by some element σ and where $f\sigma f^{-1} = \sigma^q$. As $\overline{\rho}(\mathrm{Frob}_q)$ has distinct eigenvalues it is easy to see that after conjugation we may assume that $\rho_Q^{univ}(f) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ where $a \not\equiv b \bmod \mathfrak{m}_{R_Q}$. We will show that $\rho_Q^{univ}(\sigma)$ is a diagonal matrix with entries congruent to $1 \bmod \mathfrak{m}_{R_Q}$. We will in fact prove this mod $\mathfrak{m}_{R_Q}^n$ for all n by induction on n. For $n = 1$ there is nothing to prove. So suppose this is true modulo $\mathfrak{m}_{R_Q}^n$ with $n > 0$. Then

$$\rho_Q^{univ}(\sigma) \equiv \begin{pmatrix} \mu_1 & 0 \\ 0 & \mu_2 \end{pmatrix} (1_2 + N) \bmod \mathfrak{m}_{R_Q}^{n+1},$$

where each $\mu_i \equiv 1 \bmod \mathfrak{m}_{R_Q}$ and where $N \equiv 0 \bmod \mathfrak{m}_{R_Q}^n$. We see that mod $\mathfrak{m}_{R_Q}^{n+1}$ we have

$$\begin{aligned} & 1 + \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} N \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{-1} \\ \equiv & \begin{pmatrix} \mu_1^{q-1} & 0 \\ 0 & \mu_2^{q-1} \end{pmatrix} (1+N)^q \\ \equiv & \begin{pmatrix} \mu_1^{q-1} & 0 \\ 0 & \mu_2^{q-1} \end{pmatrix} (1+qN) \\ \equiv & \begin{pmatrix} \mu_1^{q-1} & 0 \\ 0 & \mu_2^{q-1} \end{pmatrix} + N, \end{aligned}$$

and as $a \not\equiv b \bmod \mathfrak{m}_{R_Q}$ we deduce that N is diagonal $\bmod \mathfrak{m}_{R_Q}^{n+1}$ as required.

We can choose ϕ_2 so that $\phi_2(f) \equiv \beta_q \bmod \mathfrak{m}_{R_Q}$. Then we can define a map $\Delta_q \to R_Q^\times$ to be $\phi_2|_{I_q}^2$. This makes R_Q into an $\mathcal{O}[\Delta_Q]$-algebra. Using the last lemma and the universal properties of R_Q and of R it is easy to see that $R_Q/\mathfrak{a}_Q \tilde{\to} R$. It moreover follows from the discussion preceding theorem 1 of this paper that the map $R_Q \twoheadrightarrow T_Q$ is a map of $\mathcal{O}[\Delta_Q]$-algebras.

The key observation is the following ring theoretic proposition. Theorem 3 follows on applying it to the rings R_{Q_n} and $\mathbb{T}_{Q_n}$ for the sets Q_n constructed in section 4 of this paper. Note that there is a map $\mathcal{O}[[S_1, ..., S_r]] \twoheadrightarrow \mathcal{O}[\Delta_{Q_n}]$ with kernel the ideal $((1+S_1)^{\#\Delta_{q_1}} - 1, ..., (1+S_r)^{\#\Delta_{q_r}} - 1)$, where $Q_n = \{q_1, ..., q_r\}$. Note also that by the displayed isomorphism a couple of lines before theorem 3 there exists a surjection of $\mathcal{O}$-algebras $\mathcal{O}[[X_1, ..., X_r]] \twoheadrightarrow R_{Q_n}$.

Proposition 3 *Suppose r is a non-negative integer and that we have a map of $\mathcal{O}$-algebras $R \twoheadrightarrow T$ with T finite and flat over $\mathcal{O}$. Suppose for each positive integer n we have a map of $\mathcal{O}$-algebras $R_n \twoheadrightarrow T_n$ and a commutative diagram of $\mathcal{O}$-algebras*

$$\begin{array}{ccccc} \mathcal{O}[[S_1, ..., S_r]] & \to & R_n & \twoheadrightarrow & R \\ & & \downarrow & & \downarrow \\ & & T_n & \twoheadrightarrow & T, \end{array}$$

where

1. *there is a surjection of $\mathcal{O}$-algebras $\mathcal{O}[[X_1, ..., X_r]] \twoheadrightarrow R_n$,*
2. *$(S_1, ..., S_r)R_n \subset \ker(R_n \twoheadrightarrow R)$,*
3. *$(S_1, ..., S_r)T_n = \ker(T_n \twoheadrightarrow T)$,*
4. *if $\mathfrak{b}_n$ denotes the kernel of $\mathcal{O}[[S_1, ..., S_r]] \to T_n$ then $\mathfrak{b}_n \subset ((1+S_1)^{p^n} - 1, ..., (1+S_r)^{p^n} - 1)$ and T_n is a finite free $\mathcal{O}[[S_1, ..., S_r]]/\mathfrak{b}_n$-module.*

Then $R \tilde{\to} T$ and these rings are complete intersections.

Reducing $\bmod \lambda$ we see that it suffices to prove this result with k replacing $\mathcal{O}$ everywhere. In this case we see that the last condition becomes $\mathfrak{b}_n \subset (S_1^{p^n}, ..., S_r^{p^n})$. Further we may replace R by its reduction modulo $\mathfrak{m}_R \ker(R \twoheadrightarrow T)$, and so we may assume that R is finite over k. We may replace T_n by $T_n/(S_1^{p^n}, ..., S_r^{p^n})$ and so assume that $\mathfrak{b}_n = (S_1^{p^n}, ..., S_r^{p^n})$. Finally we may replace R_n by its image in $R \oplus T_n$.

Now define an n-structure to be a pair of k-algebras $B \twoheadrightarrow A$ together with a commutative diagram of k-algebras

$$\begin{array}{ccccc} & & k[[S_1,...,S_r]] & & \\ & & \downarrow & & \\ k[[X_1,...,X_r]] & \twoheadrightarrow & B & \twoheadrightarrow & R \\ & & \downarrow & & \downarrow \\ & & A & \twoheadrightarrow & T, \end{array}$$

such that

1. $B \hookrightarrow R \oplus A$,
2. $(S_1,...,S_r)B \subset \ker(B \twoheadrightarrow R)$,
3. $(S_1,...,S_r)A = \ker(A \twoheadrightarrow T)$,
4. A is a finite free $k[[S_1,...,S_r]]/(S_1^{p^n},...,S_r^{p^n})$-module.

Note that $\#B \leq (\#T)^{p^{nr}}\#R$ and so we see that there are only finitely many isomorphism classes of n-structures. If $\mathcal{S}$ is an n-structure and if $m \leq n$ then we may obtain an m-structure $\mathcal{S}^{(m)}$ by replacing A by $A/(S_1^{p^m},...,S_r^{p^m})$ and B by its image in $R \oplus (A/(S_1^{p^m},...,S_r^{p^m}))$.

As explained above, it follows from the hypotheses of the proposition that an n-structure $\mathcal{S}_n$ exists for each n. We next claim that we can find, for each n, n-structures $\mathcal{S}'_n$ such that for $m \leq n$ we have $\mathcal{S}'_m \cong (\mathcal{S}'_n)^{(m)}$. To prove this observe that we can find recursively integers $n(m)$ with the following properties

- $\mathcal{S}_{n(m)}^{(m)} \cong \mathcal{S}_n^{(m)}$ for infinitely many n
- and for $m > 1$, $\mathcal{S}_{n(m)}^{(m-1)} \cong \mathcal{S}_{n(m-1)}^{(m-1)}$.

Then set $\mathcal{S}'_m = \mathcal{S}_{n(m)}^{(m)}$.

Thus we obtain a commutative diagram

$$\begin{array}{ccccccccc} ... & R'_n & ... & R'_2 & \twoheadrightarrow & R'_1 & \twoheadrightarrow & R \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ ... & T'_n & ... & T'_2 & \twoheadrightarrow & T'_1 & \twoheadrightarrow & T \end{array}$$

of $k[[X_1,...,X_r,S_1,...,S_r]]$-algebras. Moreover we have that

- $k[[X_1,...,X_r]] \twoheadrightarrow R'_n \twoheadrightarrow T'_n$,
- T'_n is a finite free $k[[S_1,...,S_r]]/(S_1^{p^n},...,S_r^{p^n})$-module,

- $R'_n/(S_1, ..., S_r) \twoheadrightarrow R$ and $T'_n/(S_1, ..., S_r) \tilde{\rightarrow} T$.

Let R'_∞ denote the quotient of $k[[X_1, ..., X_r]]$ by the intersection of the ideals $\ker(k[[X_1, ..., X_r]] \twoheadrightarrow R'_n)$ and let T'_∞ denote the quotient of $k[[X_1, ..., X_r]]$ by the intersection of the ideals $\ker(k[[X_1, ..., X_r]] \twoheadrightarrow T'_n)$. Then we have a commutative diagram

$$\begin{array}{ccccc} & & k[[S_1, ..., S_r]] & & \\ & & \downarrow & & \\ k[[X_1, ..., X_r]] & \twoheadrightarrow & R'_\infty & \twoheadrightarrow & R \\ & & \downarrow & & \downarrow \\ & & T'_\infty & \twoheadrightarrow & T, \end{array}$$

such that

- $R'_\infty \twoheadrightarrow T'_\infty$,
- T'_∞ is a finite free $k[[S_1, ..., S_r]]$-module,
- $R'_\infty/(S_1, ..., S_r) \twoheadrightarrow R$ and $T'_\infty/(S_1, ..., S_r) \tilde{\rightarrow} T$.

We deduce that T'_∞ has Krull dimension r and hence we deduce that the map $k[[X_1, ..., X_r]] \twoheadrightarrow T'_\infty$ has trivial kernel. That is we have isomorphisms $k[[X_1, ..., X_r]] \tilde{\rightarrow} R'_\infty \tilde{\rightarrow} T'_\infty$. Thus $R \tilde{\rightarrow} T$. As T has Krull dimension 0 and $T \cong k[[X_1, ..., X_r]]/(S_1, ..., S_r)$ we see that T is a complete intersection, and the proposition is proved.