GALOIS DEFORMATION, MODULAR LIFTING AND $R = T$ THEOREMS

HARUZO HIDA

Contents

Date: May 10, 2011.
The author is partially supported by the NSF grant: DMS 0753991 and DMS 0854949.

1. Introduction

In this course, we discuss the following two topics:

1. Basics of Galois deformation theory (and representation theory of pro-finite groups);
2. Sketch of proofs of different $R = T$ theorems.

The purpose of the lectures was to introduce the audience to control theorems and to show how such theorems have been useful in establishing that certain Hecke algebras are universal deformation rings for certain mod p representations.

The universality of the Hecke algebra was first proved by A. Wiles [W1], assuming a ring theoretic property of the Hecke algebra, which was in turn proved in [TW]. The appendix to [TW], contains an alternative method for proving the universality of the Hecke algebra, assuming that the ramification of deformations outside p is minimal. This latter method has been simplified by F. Diamond and K. Fujiwara (see [HMI]). In these notes, we describe Fujiwara's treatment, assuming that the deformations are unramified outside p.

We fix a prime $p > 2$, an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and field embeddings $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ and $i_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Let F be a number field and $F^{(p)}/F$ be the maximal field extension inside $\overline{\mathbb{Q}}$ unramified outside p and ∞. Put $\mathfrak{G}_F = \mathrm{Gal}(F^{(p)}/F)$. In this note, W is a discrete valuation ring over the p-adic integer ring $\mathbb{Z}_p$ with residue field $\mathbb{F}$.

2. Galois deformation rings

We prove existence of the universal Galois deformation rings.

2.1. **The Iwasawa algebra as a deformation ring.**

We can interpret the Iwasawa algebra Λ as a universal Galois deformation ring. Fix a continuous character $\overline{\psi} : \mathfrak{G}_{\mathbb{Q}} \to \mathbb{F}^\times$. We write CL_W for the category of p-profinite local W-algebras A with $A/\mathfrak{m}_A = \mathbb{F}$. A character $\rho : \mathfrak{G}_{\mathbb{Q}} \to A^\times$ for $A \in CL_W$ is called a W-deformation (or just simply a deformation) of $\overline{\psi}$ if $(\rho \mod \mathfrak{m}_A) = \overline{\psi}$. A couple $(\mathcal{R}, \boldsymbol{\rho})$ made of an object $\mathcal{R}$ of CL_W and a character $\boldsymbol{\rho} : \mathfrak{G}_F \to \mathcal{R}^\times$ is called a *universal couple* for ψ if for any deformation $\rho : \mathfrak{G}_F \to A$ of $\overline{\psi}$, we have a unique morphism $\phi_\rho : \mathcal{R} \to A$ in CL_W (so it is a local W-algebra homomorphism) such that $\phi_\rho \circ \boldsymbol{\rho} = \rho$. By the universality, if exists, the couple $(\mathcal{R}, \boldsymbol{\rho})$ is determined uniquely up to isomorphisms. The ring $\mathcal{R}$ is called the universal deformation ring and $\boldsymbol{\rho}$ is called the universal deformation of $\overline{\psi}$.

Consider the group of p-power roots of unity $\mu_{p^\infty} = \bigcup_n \mu_{p^n} \subset \overline{\mathbb{Q}}^\times$. Then writing $\zeta_n = \exp\left(\frac{2\pi i}{p^n}\right)$, we can identify the group μ_{p^n} with $\mathbb{Z}/p^n\mathbb{Z}$ by $\zeta_n^m \leftrightarrow (m \mod p^n)$. The Galois action of $\sigma \in \mathfrak{G}_{\mathbb{Q}}$ sends ζ_n to $\zeta_n^{\nu_n(\sigma)}$ for $\nu_n(\sigma) \in \mathbb{Z}/p^n\mathbb{Z}$. Then $\mathfrak{G}_{\mathbb{Q}}$ acts on $\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}$ by a character $\nu := \varprojlim_n \nu_n : \mathfrak{G}_{\mathbb{Q}} \to \mathbb{Z}_p^\times$, which is called the p-adic cyclotomic character. The logarithm power series $\log(1+x) = \sum_{n=1}^\infty -\frac{(-x)^n}{n}$ and exponential power series $\exp(x) = \sum_{n=0}^\infty \frac{x^n}{n!}$ converges absolutely p-adically on $p\mathbb{Z}_p$. Note that $\mathbb{Z}_p^\times = \mu_{p-1} \times \Gamma$ for $\Gamma = 1 + p\mathbb{Z}_p$ by $\mathbb{Z}_p^\times \mapsto (\omega(z) = \lim_{n\to\infty} z^{p^n}, \omega(z)^{-1}z) \in \mu_{p-1} \times \Gamma$. We define $\log_p : \mathbb{Z}_p^\times \to \Gamma$ by $\log_p(\zeta, s) = \log(s) \in p\mathbb{Z}_p$ for $\zeta\mu_{p-1}$ and $s \in 1 + p\mathbb{Z}_p = \Gamma$.

Exercise 2.1. *Compute the radius of convergence of* $\exp(x)$ *and* $\log(x)$ *in* $\mathbb{C}_p$ *under the standard* p*-adic norm* $|\cdot|_p$ *with* $|p|_p = p^{-1}$.

Let $\Lambda_W = W[[X]]$ (a one variable power series ring with coefficients in W) and $\Lambda = \mathbb{Z}_p[[X]]$. Since $s \mapsto \binom{s}{n} = \frac{(s-n+1)(s-n+2)\cdots s}{n!}$ has integer valued on the set $\mathbb{Z}_+$ of positive integers and p-adically continuous, it extends to a polynomial map $\mathbb{Z}_p \ni s \mapsto \binom{s}{n} \in \mathbb{Z}_p$. Then $(1+X)^s = \sum_{n=0}^{\infty} \binom{s}{n} X^n \in \mathbb{Z}_p$, getting an additive character $\mathbb{Z}_p \ni s \mapsto (1+X)^s \in \Lambda^\times$. Let $\gamma = 1+p$; so, $\Gamma = \gamma^{\mathbb{Z}_p}$. Consider the character $\kappa : \mathfrak{G}_{\mathbb{Q}} \to \Lambda^\times$ given by $\kappa(\sigma) = (1+X)^{\log_p(\nu_p(\sigma))/\log_p(\gamma)}$.

Exercise 2.2. *Prove* $1 + p\mathbb{Z}_p = \gamma^{\mathbb{Z}_p}$.

Since $\mathbb{Q}[\mu_{p^\infty}]$ is the maximal abelian extension of $\mathbb{Q}$ unramified outside p and ∞ by class field theory (or else, by the theorem of Kronecker-Weber), we have $\mathfrak{G}_{\mathbb{Q}}/\overline{[\mathfrak{G}_{\mathbb{Q}}, \mathfrak{G}_{\mathbb{Q}}]} = \mathrm{Gal}(\mathbb{Q}[\mu_{p^\infty}]/\mathbb{Q})$. On the other hand, we identified $\mathrm{Gal}(\mathbb{Q}[\mu_{p^\infty}]/\mathbb{Q})$ with $\mathbb{Z}_p^\times$ by ν_p. We write $[z] \in \mathrm{Gal}(\mathbb{Q}[\mu_{p^\infty}]/\mathbb{Q})$ for automorphism of $\mathbb{Q}[\mu_{p^\infty}]$ with $\nu_p([z]) = z$. Then we have $\kappa([\gamma^s]) = (1+X)^s$. Since $\overline{\psi}$ has values in $\mathbb{F}_p^\times \cong \mu_{p-1}$, we may identify the character $\overline{\psi}$ with a character $\psi : \mathfrak{G}_{\mathbb{Q}} \to \mu_{p-1} \subset \mathbb{Z}_p^\times$. Define $\boldsymbol{\psi} : \mathfrak{G}_{\mathbb{Q}} \to \Lambda^\times$ by $\boldsymbol{\psi}(\sigma) := \kappa(\sigma)\psi(\sigma)$; then $\boldsymbol{\psi} \equiv \overline{\psi} \mod \mathfrak{m}_\Lambda$, where $\mathfrak{m}_\Lambda$ is the maximal ideal of Λ; so, $\mathfrak{m}_\Lambda = (p, X)$. Thus $(\Lambda, \boldsymbol{\psi})$ is a deformation of $(\mathbb{F}, \overline{\psi})$ with $\boldsymbol{\psi}([\gamma]) = (1+X)$.

Proposition 2.3. *The couple* $(\Lambda_W = W[[X]], \boldsymbol{\psi})$ *(for a variable* X*) is the universal couple for* $\overline{\psi}$.

Proof. Since $\mathbb{Q}[\mu_{p^\infty}]$ is the maximal abelian extension of $\mathbb{Q}$ unramified outside p and ∞, each deformation $\rho : \mathfrak{G}_{\mathbb{Q}} \to A^\times$ factors through $\mathrm{Gal}(Q[\mu_{p^\infty}]/\mathbb{Q}) = \Gamma \times \mathrm{Gal}(\mathbb{Q}[\mu_p]/\mathbb{Q})$. Then the character ρ is determined by $\rho(\gamma)$, because $\rho|_{\mathbb{Q}[\mu_p]}$ is given by ψ and $\Gamma = \gamma^{\mathbb{Z}_p}$. Then we have $\phi_\rho : \Lambda_W = W[[X]] \to A$ by sending X to $\rho(\gamma) - 1$, and we have $\phi_\rho \circ \boldsymbol{\psi} = \rho$. □

For a given n-dimensional representation $\overline{\rho} : \mathfrak{G}_F \to GL_n(\mathbb{F})$, a deformation $\rho : \mathfrak{G}_F \to GL_n(R)$ is a continuous representation with $\rho \mod \mathfrak{m}_R \cong \overline{\rho}$. Two deformations $\rho, \rho' : \mathfrak{G}_F \to GL_n(R)$ for $R \in CL_W$ is equivalent, if there exists an invertible matrix $x \in GL_n(R)$ such that $x\rho(\sigma)x^{-1} = \rho'(\sigma)$ for all $\sigma \in \mathfrak{G}_F$. We write $\rho \sim \rho'$ if ρ and ρ' are equivalent. A couple $(R_{\overline{\rho}}, \boldsymbol{\rho})$ for a deformation $\boldsymbol{\rho} : \mathfrak{G}_F \to GL_n(R_{\overline{\rho}})$ is called a universal couple over W, if for any given deformation $\rho : \mathfrak{G}_F \to GL_n(R)$ there exists a unique W-algebra homomorphism $\iota_\rho : R_{\overline{\rho}} \to R$ such that $\iota_\rho \circ \boldsymbol{\rho} \sim \rho$.

2.2. **Pseudo representations.** In order to show the existence of the universal deformation ring, pseudo representations are very useful. We recall the definition of pseudo representations (due to Wiles) when $n = 2$. See [MFG] §2.2.2 for a higher dimensional generalization due to R. Taylor.

In this subsection, the coefficient ring A is always an object in CL_W with maximal ideal $\mathfrak{m}_A$. We write $\mathbb{F} = A/\mathfrak{m}_A$. Note that 2 is invertible in A as $p > 2$. We would like to characterize the trace of a representation of a group G.

We describe in detail traces of degree 2 representations $\rho : G \to GL_2(A)$ when G contains c such that $c^2 = 1$ and $\det \rho(c) = -1$. Let $V(\rho) = A^2$ on which G acts by ρ. Since 2 is invertible in A, we know that $V = V(\rho) = V_+ \oplus V_-$ for $V_\pm = \frac{1 \pm c}{2} V$. For $\overline{\rho} = \rho \mod \mathfrak{m}_A$, we write $\overline{V} = V(\overline{\rho})$. Then similarly as above, $\overline{V} = \overline{V}_+ \oplus \overline{V}_-$ and $\overline{V}_\pm = V_\pm/\mathfrak{m}_A V_\pm$. Since $\dim_{\mathbb{F}} \overline{V} = 2$ and $\det \overline{\rho}(c) = -1$, $\dim_{\mathbb{F}} \overline{V}_\pm = 1$. This shows that $\overline{V}_\pm = \mathbb{F}\overline{v}_\pm$ for $\overline{v}_\pm \in \overline{V}_\pm$. Take $v_\pm \in V_\pm$ such that $v_\pm \mod \mathfrak{m}_A V_\pm = \overline{v}_\pm$, and define $\phi_\pm : A \to V_\pm$ by $\phi(a) = av_\pm$. Then $\phi_\pm \mod \mathfrak{m}_A V$ is surjective by Nakayama's lemma. Note that $\phi_\pm : A \cong V_\pm$ as A-modules. In other words, $\{v_-, v_+\}$ is an A–base of V. We write $\rho(r) = \left(\begin{smallmatrix} a(r) & b(r) \\ c(r) & d(r) \end{smallmatrix}\right)$ with respect to this base. Thus $\rho(c) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Define another function $x : G \times G \to A$ by $x(r, s) = b(r)c(s)$. Then we have

(W1) $a(rs) = a(r)a(s) + x(r, s)$, $d(rs) = d(r)d(s) + x(s, r)$ and
$x(rs, tu) = a(r)a(u)x(s, t) + a(u)d(s)x(r, t) + a(r)d(t)x(s, u) + d(s)d(t)x(r, u)$;
(W2) $a(1) = d(1) = d(c) = 1$, $a(c) = -1$ and $x(r, s) = x(s, t) = 0$ if $s = 1, c$;
(W3) $$x(r, s)x(t, u) = x(r, u)x(t, s).$$

These are easy to check: We have

$$\begin{pmatrix} a(r) & b(r) \\ c(r) & d(r) \end{pmatrix}\begin{pmatrix} a(s) & b(s) \\ c(s) & d(s) \end{pmatrix} = \begin{pmatrix} a(rs) & b(rs) \\ c(rs) & d(rs) \end{pmatrix}.$$

Then by computation, $a(rs) = a(r)a(s) + b(r)c(s) = a(r)a(s) + x(r, s)$. Similarly, we have $b(rs) = a(r)b(s) + b(r)d(s)$ and $c(rs) = c(r)a(s) + d(r)c(s)$. Thus

$$\begin{aligned} x(rs, tu) &= b(rs)c(tu) = (a(r)b(s) + b(r)d(s))(c(t)a(u) + d(t)c(u)) \\ &= a(r)a(u)x(s, t) + a(r)d(t)x(s, u) + a(u)d(s)x(r, t) + d(s)d(t)x(r, u). \end{aligned}$$

A triple $\{a, d, x\}$ satisfying the three conditions (W1-3) is called a *pseudo representation* of Wiles of (G, c). For each pseudo-representation $\tau = \{a, d, x\}$, we define

$$\mathrm{Tr}(\tau)(r) = a(r) + d(r) \quad \text{and} \quad \det(\tau)(r) = a(r)d(r) - x(r, r).$$

By a direct computation using (W1-3), we see

$$a(r) = \frac{1}{2}(\mathrm{Tr}(\tau)(r) - \mathrm{Tr}(\tau)(rc)), \quad d(r) = \frac{1}{2}(\mathrm{Tr}(\tau)(r) + \mathrm{Tr}(\tau)(rc))$$

and

$$x(r, s) = a(rs) - a(r)a(s), \quad \det(\tau)(rs) = \det(\tau)(r)\det(\tau)(s).$$

Thus the pseudo-representation τ is determined by the trace of τ as long as 2 is invertible in A.

Proposition 2.4 (A. Wiles, 1988). *Let G be a group and $R = A[G]$. Let $\tau = \{a, d, x\}$ be a pseudo-representation (of Wiles) of (G, c). Suppose either that there exists at least one pair $(r, s) \in G \times G$ such that $x(r, s) \in A^\times$ or that $x(r, s) = 0$ for all $r, s \in G$. Then there exists a representation $\rho : R \to M_2(A)$ such that $\mathrm{Tr}(\rho) = \mathrm{Tr}(\tau)$ and $\det(\rho) = \det(\tau)$ on G. If A is a topological ring, G is a topological group and all maps in τ are continuous on G, then ρ is a continuous representation of G into $GL_2(A)$ under the topology on $GL_2(A)$ induced by the product topology on $M_2(A)$.*

Proof. When $x(r, s) = 0$ for all $r, s \in G$, we see from (W1) that $a, d : G \to A$ satisfies $a(rs) = a(r)a(s)$ and $d(rs) = d(r)d(s)$. Thus a, d are characters of G, and we define $\rho : G \to GL_2(A)$ by $\rho(g) = \left(\begin{smallmatrix} a(g) & 0 \\ 0 & d(g) \end{smallmatrix}\right)$, which satisfies the required property.

We now suppose $x(r, s) \in A^\times$ for $r, s \in G$. Then we define $b(g) = x(g, s)/x(r, s)$ and $c(g) = x(r, g)$ for $g \in G$. Then by (W3), $b(g)c(h) = x(r, h)x(g, s)/x(r, s) = x(g, h)$. Put $\rho(g) = \left(\begin{smallmatrix} a(g) & b(g) \\ c(g) & d(g) \end{smallmatrix}\right)$. By (W2), we see that $\rho(1)$ is the identity matrix and $\rho(c) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. By computation,

$$\rho(g)\rho(h) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}\begin{pmatrix} a(h) & b(h) \\ c(h) & d(h) \end{pmatrix} = \begin{pmatrix} a(g)a(h)+b(g)c(h) & a(g)b(h)+b(g)d(h) \\ c(g)a(h)+d(g)c(h) & d(g)d(h)+c(g)b(h) \end{pmatrix}.$$

By (W1), $a(gh) = a(g)a(h) + x(g, h) = a(g)a(h) + b(g)c(h)$ and $d(gh) = d(g)d(h) + x(h, g) = d(g)d(h) + b(h)c(g)$. Now let us look at the lower left corner:

$$c(g)a(h) + d(g)c(h) = x(r, g)a(h) + d(g)x(r, h).$$

Now apply (W1) to $(1, r, g, h)$ in place of (r, s, t, u), and we get

$$c(gh) = x(r, gh) = a(h)x(r, g) + d(g)x(r, h),$$

because $x(1, g) = x(1, h) = 0$. As for the upper right corner, we apply (W1) to $(g, h, 1, s)$ in place of (r, s, t, u). Then we get

$$b(gh)x(r, s) = x(gh, s) = a(g)x(h, s) + d(h)x(g, s) = (a(g)b(h) + d(h)b(g))x(r, s),$$

which shows that $\rho(gh) = \rho(g)\rho(h)$. We now extends ρ linearly to $R = A[G]$. This shows the first assertion. The continuity of ρ follows from the continuity of each entries, which follows from the continuity of τ. □

Start from an absolutely irreducible representation $\overline{\rho} : G \to GL_n(\mathbb{F})$. Here a representation of a group into $GL_n(K)$ for a field K is called *absolutely irreducible* if it is irreducible as a representation into $GL_n(\overline{K})$ for an algebraic closure $\overline{K}$ of K.

Exercise 2.5. *Give an example of irreducible representations of a group G into $GL_2(\mathbb{Q})$ which is not absolutely irreducible.*

We fix an absolutely irreducible representation $\overline{\rho} : G \to GL_2(\mathbb{F})$ with $\det(\overline{\rho})(c) = -1$. If we have a representation $\rho : G \to GL_2(A)$ with $\rho \mod \mathfrak{m}_A \sim \overline{\rho}$, then $\det(\rho(c)) \equiv \det(\overline{\rho}(c)) \equiv -1 \mod \mathfrak{m}_A$. Since $c^2 = 1$, if 2 is invertible in A ($\Leftrightarrow$ the characteristic of $\mathbb{F}$ is different from 2), $\det(\rho(c)) = -1$. This is a requirement to have a pseudo-representation τ_ρ of Wiles associated to ρ. Since $\overline{\rho}$ is absolutely irreducible, we find $r, s \in G$ such that $b(r) \not\equiv 0 \mod \mathfrak{m}_A$ and $c(s) \not\equiv 0 \mod \mathfrak{m}_A$. Thus τ_ρ satisfies the condition of Proposition 2.4. Conversely if we have a pseudo representation $\tau : G \to A$ such that $\tau \equiv \overline{\tau} \mod \mathfrak{m}_A$ for $\overline{\tau} = \tau_{\overline{\rho}}$, again we find $r, s \in G$ such that $x(r, s) \in A^\times$. The correspondence $\rho \mapsto \tau_\rho$ induces a bijection:

$$\text{(2.1)} \quad \{\rho : G \to GL_2(A) : \text{representation}|\rho \mod \mathfrak{m}_A \sim \overline{\rho}\} / \sim \leftrightarrow \\ \{\tau : G \to A : \text{pseudo-representation}|\tau \mod \mathfrak{m}_A = \overline{\tau}\},$$

where $\overline{\tau} = \tau_{\overline{\rho}}$ and "$\sim$" is the conjugation under $GL_2(A)$. The map is surjective by Proposition 2.4 combined with Proposition 2.6 and one to one by Proposition 2.6 we admit, because a pseudo-representation is determined by its trace.

Proposition 2.6 (Carayol, Serre, 1994)**.** *Let A be an pro-artinian local ring with finite residue field $\mathbb{F}$. Let $R = A[G]$ for a profinite group G. Let $\rho : R \to M_n(A)$ and $\rho' : R \to M_{n'}(A)$ be two continuous representations. If $\overline{\rho} = \rho \mod \mathfrak{m}_A$ is absolutely irreducible and $\mathrm{Tr}(\rho(\sigma)) = \mathrm{Tr}(\rho'(\sigma))$ for all $\sigma \in G$, then $\rho \sim \rho'$.*

See [MFG] Proposition 2.13 for a proof of this result.

2.3. **Two dimensional non-abelian universal deformations.** We fix an absolutely irreducible representation $\overline{\rho} : G \to GL_2(\mathbb{F})$ for a profinite group G. Assume that we have $c \in G$ with $c^2 = 1$ and $\det(\overline{\rho}(c)) = -1$. First we consider a universal pseudo-representation. Let $\overline{\tau} = (\overline{a}, \overline{d}, \overline{x})$ be the pseudo representation associated to $\overline{\rho}$. A couple consisting of an object $R_{\overline{\tau}} \in CL_W$ and a pseudo-representation $T = (A, D, X) : G \to R_{\overline{\tau}}$ is called a universal couple if the following universality condition is satisfied:

(univ) *For each pseudo-representation $\tau : G \to A$ $(A \in CL_W)$ with $\tau \cong \overline{\tau} \mod \mathfrak{m}_A$, there exists a unique W–algebra homomorphism $\iota_\tau : R_{\overline{\tau}} \to A$ such that*

$$\tau = \iota_\tau \circ T.$$

We now show the existence of $(R_{\overline{\tau}}, T)$ for a profinite group G. First suppose G is a finite group. Let $\omega : W^\times \to \mu_{q-1}(W)$ be the Teichmüller character, that is,

$$\omega(x) = \lim_{n\to\infty} x^{q^n} \quad (q = |\mathbb{F}| = |W/\mathfrak{m}_W|).$$

We also consider the following isomorphism: $\mu_{q-1}(W) \ni \zeta \mapsto \zeta \mod \mathfrak{m}_W \in \mathbb{F}^\times$. We write $\varphi : \mathbb{F}^\times \to \mu_{q-1}(W) \subset W^\times$ for the inverse of the above map. We look at the power series ring: $\mathbf{\Lambda} = \mathbf{\Lambda}_G = W[[A_g, D_h, X_{(g,h)}; g, h \in G]]$. We put

$$A(g) = A_g + \varphi(\overline{a}(g)),\ D(g) = D_g + \varphi(\overline{d}(g)) \text{ and } X(g,h) = X_{g,h} + \varphi(\overline{x}(g,h)).$$

We construct the ideal I so that

$$T = (g \mapsto A(g) \mod I, g \mapsto D(g) \mod I, (g,h) \mapsto X(g,h) \mod I)$$

becomes the universal pseudo representation. Thus we consider the ideal I of $\mathbf{\Lambda}$ generated by the elements of the following type:

(w1) $A(rs) - (A(r)A(s) + X(r,s))$, $D(rs) - (D(r)D(s) + X(s,r))$ and $X(rs,tu) - (A(r)A(u)X(s,t) + A(u)D(s)X(r,t) + A(r)D(t)X(s,u) + D(s)D(t)X(r,u))$;

(w2) $A(1) - 1 = A_1$, $D(1) - 1 = D_1$, $D(c) - 1 = D_c$, $A(c) + 1 = A_c$ and $X(r,s) - X(s,t)$ if $s = 1, c$;

(w3) $$X(r,s)X(t,u) - X(r,u)X(t,s).$$

Then we put $R_{\overline{\tau}} = \mathbf{\Lambda}/I$ and define $T = (A(g), D(h), X(g,h)) \mod I$. By the above definition, T is a pseudo-representation with $T \mod \mathfrak{m}_{R_{\overline{\tau}}} = \overline{\tau}$. For a pseudo representation $\tau = (a, d, x) : G \to A$ with $\tau \equiv \overline{\tau} \mod \mathfrak{m}_A$, we define $\iota_\tau : \mathbf{\Lambda} \to A$ with $\iota_\tau(f) \in A$ for a power series $f(A_g, D_h, X_{(g,h)}) \in \mathbf{\Lambda}$ by

$$\begin{aligned} f(A_g, D_h, X_{(g,h)}) &\mapsto f(\tau(g) - \varphi(\overline{\tau}(g))) \\ &= f(a(g) - \varphi(\overline{a}(g)), d(h) - \varphi(\overline{d}(h)), x(g,h) - \varphi(\overline{x}(g,h))). \end{aligned}$$

Since f is a power series of $A_g, D_h, X_{g,h}$ and $\tau(g) - \varphi(\overline{\tau}(g)) \in \mathfrak{m}_A$, the value $f(\tau(g) - \varphi(\overline{\tau}(g)))$ is well defined. Let us see this. If A is artinian, a sufficiently high power $\mathfrak{m}_A^N$ vanishes. Thus if the monomial of the variables $A_g, D_h, X_{(g,h)}$ is of degree higher than N, it is sent to 0 via ι_τ, and $f(\tau(g) - \varphi(\overline{\tau}(g)))$ is a finite sum of terms of degree $\leq N$. If A is pro-artinian, the morphism ι_τ is just the projective limit of the corresponding ones well defined for artinian quotients. By the axioms of pseudo-representation (W1-3), $\iota_\tau(I) = 0$, and hence ι_τ factors through $R_{\overline{\tau}}$. The uniqueness of ι_τ follows from the fact that $\{A_g, D_h, X_{(g,h)} | g, h \in G\}$ topologically generates $R_{\overline{\tau}}$.

Now assume that $G = \varprojlim_N G/N$ for open normal subgroups N (so, G/N is finite). Since $\mathrm{Ker}(\overline{\rho})$ is an open subgroup of G, we may assume that N runs over subgroups of $\mathrm{Ker}(\overline{\rho})$. Since $\overline{\rho}$ factors through $G/\mathrm{Ker}(\overline{\rho})$, $\mathrm{Tr}(\overline{\tau}) = \mathrm{Tr}(\overline{\rho})$ factors through G/N. Therefore we can think of the universal couple $(R_{\overline{\tau}}^N, T_N)$ for $(G/N, \overline{\tau})$. If $N \subset N'$, the algebra homomorphism $\mathbf{\Lambda}_{G/N} \to \mathbf{\Lambda}_{G/N'}$ taking $(A_{gN}, D_{hN}, X_{(gN,hN)})$ to $(A_{gN'}, D_{hN'}, X_{(gN',hN')})$ induces a surjective W–algebra homomorphism $\pi_{N,N'} : R_{\overline{\tau}}^N \to R_{\overline{\tau}}^{N'}$ with $\pi_{N,N'} \circ T_N = T_{N'}$. We then define

$T = \varprojlim_N T_N$ and $R_{\overline{\tau}} = \varprojlim_N R^N_{\overline{\tau}}$. If $\tau : G \to A$ is a pseudo representation, by Proposition 2.4, we have the associated representation $\rho : G \to GL_2(A)$ such that $\mathrm{Tr}(\tau) = \mathrm{Tr}(\rho)$. If A is artinian, then $GL_2(A)$ is a finite group, and hence ρ and $\mathrm{Tr}(\tau) = \mathrm{Tr}(\rho)$ factors through G/N for a sufficiently small open normal subgroup N. Thus we have $\iota_\tau : R_{\overline{\tau}} \xrightarrow{\pi_N} R^N_{\overline{\tau}} \xrightarrow{\iota^N_\tau} A$ such that $\iota_\tau \circ T = \tau$. Since $(A(g), D(h), X(g,h))$ generates topologically $R_{\overline{\tau}}$, ι_τ is uniquely determined.

Writing $\boldsymbol{\rho}$ for the representation $\boldsymbol{\rho} : G \to GL_n(R_{\overline{\tau}})$ associated to the universal pseudo representation T and rewriting $R_{\overline{\rho}} = R_{\overline{\tau}}$, for $n = 2$, we have proven by (2.1) the following theorem, which was first proven by Mazur [M] in in 1989 (see [MFG] Theorem 2.26 for a proof valid for any n).

Theorem 2.7 (Mazur). *Suppose that $\overline{\rho} : G \to GL_n(\mathbb{F})$ is absolutely irreducible. Then there exists the universal deformation ring $R_{\overline{\rho}}$ in CL_W and a universal deformation $\boldsymbol{\rho} : G \to GL_n(R_{\overline{\rho}})$. If we write $\overline{\tau}$ for the pseudo representation associated to $\overline{\rho}$, then for the universal pseudo-representation $T : G \to R_{\overline{\tau}}$ deforming $\overline{\tau}$, we have a canonical isomorphism of W–algebras $\iota : R_{\overline{\rho}} \cong R_{\overline{\tau}}$ such that $\iota \circ \mathrm{Tr}(\boldsymbol{\rho}) = \mathrm{Tr}(T)$.*

Let $(R_{\overline{\rho}}, \boldsymbol{\rho})$ be the universal couple for an absolutely irreducible representation $\overline{\rho} : \mathfrak{G}_{\mathbb{Q}} \to GL_n(\mathbb{F})$. We can also think of $(R_{\det(\overline{\rho})}, \nu)$, which is the universal couple for the character $\det(\overline{\rho}) : \mathfrak{G}_{\mathbb{Q}} \to GL_1(\mathbb{F}) = \mathbb{F}^\times$. As we have studied already, $R_{\det(\overline{\rho})} \cong W[[\Gamma]] = \Lambda_W$. Note that $\det(\boldsymbol{\rho}) : \mathfrak{G}_{\mathbb{Q}} \to GL_1(R_{\overline{\rho}})$ satisfies $\det(\boldsymbol{\rho}) \bmod \mathfrak{m}_{R_{\overline{\rho}}} = \det(\overline{\rho})$. Thus $\det(\boldsymbol{\rho})$ is a deformation of $\det(\overline{\rho})$, and hence by the universality of $(\Lambda_W \cong R_{\det(\overline{\rho})}, \nu)$, there is a unique W–algebra homomorphism $\iota : \Lambda_W \to R_{\overline{\rho}}$ such that $\iota \circ \nu = \det(\boldsymbol{\rho})$. In this way, $R_{\overline{\rho}}$ becomes naturally a Λ_W–algebra via ι.

Corollary 2.8. *Let the notation and the assumption be as above and as in the above theorem. Then the universal ring $R_{\overline{\rho}}$ is canonically an algebra over the Iwasawa algebra $\Lambda_W = W[[\Gamma]]$.*

When $G = \mathfrak{G}_{\mathbb{Q}}$ (or more generally, $\mathfrak{G}_F$), it is known that $R_{\overline{\rho}}$ is noetherian (cf. [MFG] Proposition 2.30). We will come back to this point after relating certain Selmer groups with the universal deformation ring.

2.4. **Ordinary universal deformation rings.** Let $\overline{\rho} : \mathfrak{G}_{\mathbb{Q}} \to GL_2(\mathbb{F})$ be a Galois representation with coefficients in a finite field $\mathbb{F}$ of characteristic p. We consider the following condition for a subfield F of $\mathbb{Q}^{(p)}$:

(ai$_F$) $\overline{\rho}$ restricted to $\mathfrak{G}_F$ is absolutely irreducible;

(rg$_p$) Suppose $\overline{\rho}|_{D_p} \cong \left(\begin{smallmatrix}\overline{\epsilon} & * \\ 0 & \overline{\delta}\end{smallmatrix}\right)$ for each decomposition subgroup D_p at p in $\mathfrak{G}_{\mathbb{Q}}$ and that $\overline{\epsilon}$ is ramified with unramified $\overline{\delta}$ (so, $\overline{\epsilon} \neq \overline{\delta}$ on I_p).

Let CL_W be the category of p–profinite local W–algebras A with $A/\mathfrak{m}_A = \mathbb{F}$. Hereafter we always assume that W–algebra is an object of CL_W. Let $\rho : \mathfrak{G}_{\mathbb{Q}} \to GL_2(A)$ be a deformation of $\overline{\rho}$ and $\phi : \mathfrak{G}_{\mathbb{Q}} \to W^\times$. We consider the following conditions

(det) $\det \rho = \phi$ regarding ϕ as a character having values in $A^\times$ by composing ϕ with the W-algebra structure morphism $W \to A$;

(ord) Suppose $\rho|_{D_p} \cong \left(\begin{smallmatrix}\epsilon & * \\ 0 & \delta\end{smallmatrix}\right)$ for each decomposition subgroup D_p at p in $\mathfrak{G}_{\mathbb{Q}}$ with unramified $\overline{\delta}$ (so, $\overline{\epsilon} \neq \overline{\delta}$ on I_p).

A couple $(R^{ord,\phi} \in CL_W, \boldsymbol{\rho}^{ord,\phi} : \mathfrak{G}_{\mathbb{Q}} \to GL_2(R^{ord,\phi}))$ is called a p–ordinary universal couple (over $\mathfrak{G}_{\mathbb{Q}}$) with determinant ϕ if $\boldsymbol{\rho}^{ord,\phi}$ satisfies (ord) and (det) and for any deformation $\rho : \mathfrak{G}_{\mathbb{Q}} \to GL_2(A)$ of $\overline{\rho}$ $(A \in CL_W)$ satisfying (ord) and (det), there exists a $\underline{\text{unique}}$ W–algebra homomorphism $\varphi = \varphi_\rho : R^{ord,\phi} \to A$ such that $\varphi \circ \boldsymbol{\rho}^{ord,\phi} \sim \rho$ in $GL_2(A)$. If the uniqueness of φ does not hold, we just call $(R^{ord,\phi}, \boldsymbol{\rho}^{ord,\phi})$ a versal p–ordinary couple with determinant ϕ.

Similarly a couple $(R^{ord} \in CL_W, \boldsymbol{\rho}^{ord} : \mathfrak{G}_{\mathbb{Q}} \to GL_2(R^{ord}))$ (resp. $(R^{\phi}, \boldsymbol{\rho}^{\phi})$) is called a p–ordinary universal couple (over $\mathfrak{G}_{\mathbb{Q}}$) (resp. a universal couple with determinant ϕ) if $\boldsymbol{\rho}^{ord}$ satisfies (ord) (resp. $\det(\boldsymbol{\rho}^{\phi}) = \phi$) and for any deformation $\rho : \mathfrak{G}_{\mathbb{Q}} \to GL_2(A)$ of $\overline{\rho}$ $(A \in CL_W)$ satisfying (ord) (resp. $\det(\rho) = \phi$), there exists a $\underline{\text{unique}}$ W–algebra homomorphism $\varphi = \varphi_\rho : R^{ord} \to A$ (resp. $\varphi = \varphi_\rho : R^{\phi} \to A$) such that $\varphi \circ \boldsymbol{\rho}^{ord} \sim \rho$ (resp. $\varphi \circ \boldsymbol{\rho}^{\phi} \sim \rho$) in $GL_2(A)$.

By the universality, if a universal couple exists, it is unique up to isomorphisms in CL_W.

Theorem 2.9 (Mazur)**.** *Under* $(\mathrm{ai}_{\mathbb{Q}})$*, universal couples* $(R, \boldsymbol{\rho})$ *and* $(R^{\phi}, \boldsymbol{\rho}^{\phi})$ *exist. Under* (rg_p) *and* $(\mathrm{ai}_{\mathbb{Q}})$*, universal couples* $(R^{ord}, \boldsymbol{\rho}^{ord} : \mathfrak{G}_{\mathbb{Q}} \to GL_2(R))$ *and* $(R^{ord,\phi}, \boldsymbol{\rho}^{ord,\phi})$ *exist (as long as* $\overline{\rho}$ *satisfies* (ord) *and* (det)*). All these universal rings are noetherian if they exist.*

This fact is proven in Mazur's paper in [M]. The existence of the universal couple $(R, \boldsymbol{\rho} : \mathfrak{G}_{\mathbb{Q}} \to GL_2(R))$ is proven in previous subsection (see Theorem 2.7) by a different method (and its noetherian property is just mentioned). Here we prove the existence of the universal couples $(R^{\phi}, \boldsymbol{\rho}^{\phi})$, $(R^{ord}, \boldsymbol{\rho}^{ord})$ and $(R^{ord,\phi}, \boldsymbol{\rho}^{ord,\phi})$ assuming the existence of a universal couple $(R, \boldsymbol{\rho})$.

Proof. An ideal $\mathfrak{a} \subset R$ is called ordinary if $\boldsymbol{\rho} \mod \mathfrak{a}$ satisfies (ord). Let $\mathfrak{a}^{ord}$ be the intersection of all ordinary ideals, and put $R^{ord} = R/\mathfrak{a}^{ord}$ and $\boldsymbol{\rho}^{ord} = \boldsymbol{\rho} \mod \mathfrak{a}^{ord}$. If $\rho : \mathfrak{G}_{\mathbb{Q}} \to GL_2(A)$ satisfies (ord), we have a unique morphism $\varphi_\rho : R \to A$ such that $(\boldsymbol{\rho} \mod \mathrm{Ker}(\varphi_\rho)) \sim \varphi_\rho \circ \boldsymbol{\rho} \sim \rho$. Thus $\mathrm{Ker}(\varphi_\rho)$ is ordinary, and hence $\mathrm{Ker}(\varphi_\rho) \supset \mathfrak{a}^{ord}$. Thus φ_ρ factors through R^{ord}. The only thing we need to show is the ordinarity of $\boldsymbol{\rho} \mod \mathfrak{a}^{ord}$. Since $\mathfrak{a}^{ord}$ is an intersection of ordinary ideals, we need to show that if $\mathfrak{a}$ and $\mathfrak{b}$ are ordinary, then $\mathfrak{a} \cap \mathfrak{b}$ is ordinary.

To show this, we prepare some notation. Let V be an A–module with an action of $\mathfrak{G}_{\mathbb{Q}}$. Let $I = I_{\mathfrak{P}}$ be an inertia group at p, and put $V_I = V/\sum_{\sigma \in I}(\sigma - 1)V$. Then by (rg_p), ρ is ordinary if and only if $V(\rho)_I$ is A–free of rank 1. The point here is that, writing $\pi : V(\rho) \twoheadrightarrow V(\rho)_I$ for the natural projection, then $\mathrm{Ker}(\pi)$ is an A–direct summand of $V(\rho)$ and hence $V(\rho) \cong \mathrm{Ker}(\pi) \oplus V(\rho)_I$ as A–modules (but not necessarily as $\mathfrak{G}_{\mathbb{Q}}$–modules). Since $V(\rho) \cong A^2$, the Krull-Schmidt theorem tells us that $\mathrm{Ker}(\pi)$ is free of rank 1. Then taking an A–basis (x, y) of $V(\rho)$ so that $x \in \mathrm{Ker}(\pi)$, we write the matrix representation ρ with respect to this basis, we have desired upper triangular form with $V(\rho)_I/\mathfrak{m}_A V(\rho)_I = V(\overline{\delta})$.

Now suppose that $\rho = \boldsymbol{\rho} \mod \mathfrak{a}$ and $\rho' = \boldsymbol{\rho} \mod \mathfrak{b}$ are both ordinary. Let $\rho'' = \boldsymbol{\rho} \mod \mathfrak{a} \cap \mathfrak{b}$, and write $V = V(\rho)$, $V' = V(\rho')$ and $V'' = V(\rho'')$. By definition, $V''/\mathfrak{a}V'' = V$ and $V''/\mathfrak{b}V'' = V'$. This shows by definition: $V_I''/\mathfrak{a}V_I'' = V_I$ and $V_I''/\mathfrak{b}V_I'' = V_I'$. Then by Nakayama's lemma, V_I'' is generated by one element, thus a surjective image of $A = R/\mathfrak{a} \cap \mathfrak{b}$. Since in A, $\mathfrak{a} \cap \mathfrak{b} = 0$, we can embed A into $A/\mathfrak{a} \oplus A/\mathfrak{b}$ by the Chinese remainder theorem. Since $V_I \cong A/\mathfrak{a}$ and $V_I' \cong A/\mathfrak{b}$, the kernel of the diagonal map $V_I'' \to V_I \oplus V_I' \cong A/\mathfrak{a} \oplus A/\mathfrak{b}$ has to be zero. Thus $V_I'' \cong A$, which was desired.

As for R^{ϕ} and $R^{ord,\phi}$, we see easily that

$$R^{\phi} = R/\sum_{\sigma\in\mathfrak{G}_{\mathbb{Q}}} R(\det \boldsymbol{\rho}(\sigma) - \phi(\sigma))$$

$$R^{ord,\phi} = R^{ord}/\sum_{\sigma\in\mathfrak{G}_{\mathbb{Q}}} R^{ord}(\det \boldsymbol{\rho}^{ord}(\sigma) - \phi(\sigma)),$$

which finishes the proof. □

2.5. **Tangent spaces of local rings.** To study when $R_{\overline{\rho}}$ is noetherian, here is a useful lemma for an object A in CL_W:

Lemma 2.10. *If $t^*_{A/W} = \mathfrak{m}_A/(\mathfrak{m}_A^2 + \mathfrak{m}_W)$ is a finite dimensional vector space over $\mathbb{F}$, then $A \in CL_W$ is noetherian. The space $t^*_{A/W}$ is called the co-tangent space of A at $\mathfrak{m}_A \in \operatorname{Spec}(A)$ over $\operatorname{Spec}(W)$.*

Proof. Define t^*_A by $\mathfrak{m}_A/\mathfrak{m}_A^2$, which is called the (absolute) co-tangent space of A at $\mathfrak{m}_A$. Since we have an exact sequence:

$$\mathbb{F} \cong \mathfrak{m}_W/\mathfrak{m}_W^2 \longrightarrow t^*_A \longrightarrow t^*_{A/W} \longrightarrow 0,$$

we conclude that t^*_A is of finite dimension over $\mathbb{F}$. First suppose that $pA = 0$ and $\mathfrak{m}_A^N = 0$ for sufficiently large N. Let $\overline{x}_1, \dots, \overline{x}_m$ be an $\mathbb{F}$–basis of t^*_A. We choose $x_j \in A$ so that $x_j \mod \mathfrak{m}_A^2 = \overline{x}_j$. Then we consider the ideal $\mathfrak{a}$ generated by x_j. We have the inclusion map: $\mathfrak{a} = \sum_j Ax_j \hookrightarrow \mathfrak{m}_A$. After tensoring $A/\mathfrak{m}_A$, we have the surjectivity of the induced linear map: $\mathfrak{a}/\mathfrak{m}_A\mathfrak{a} \cong \mathfrak{a}\otimes_A A/\mathfrak{m}_A \to \mathfrak{m}\otimes_A A/\mathfrak{m}_A \cong \mathfrak{m}/\mathfrak{m}_A^2$ because $\{\overline{x}_1, \dots, \overline{x}_m\}$ is an $\mathbb{F}$–basis of t^*_A. This shows that $\mathfrak{m}_A = \mathfrak{a} = \sum_j Ax_j$. Therefore $\mathfrak{m}_A^k/\mathfrak{m}_A^{k+1}$ is generated by the monomials in x_j of degree k as an $\mathbb{F}$–vector space. In particular, $\mathfrak{m}_A^{N-1}$ is generated by the monomials in x_j of degree $N-1$. Then we define $\pi : B = \mathbb{F}[[X_1, \dots, X_m]] \to A$ by $\pi(f(X_1, \dots, X_m)) = f(x_1, \dots, x_m)$. Since any monomial of degree $> N$ vanishes after applying π, π is a well defined W–algebra homomorphism. Let $\mathfrak{m} = \mathfrak{m}_B = (X_1, \cdots, X_m)$ be the maximal ideal of B. By the above argument, $\pi(\mathfrak{m}^{N-1}) = \mathfrak{m}_A^{N-1}$. Suppose now that $\pi(\mathfrak{m}^{N-j}) = \mathfrak{m}_A^{N-j}$, and try to prove the surjectivity of $\pi(\mathfrak{m}^{N-j-1}) = \mathfrak{m}_A^{N-j-1}$. Since $\mathfrak{m}_A^{N-j-1}/\mathfrak{m}_A^{N-j}$ is generated by monomials of degree $N-j-1$ in x_j, for each $x \in \mathfrak{m}_A^{N-j-1}$, we find a homogeneous polynomial $P \in \mathfrak{m}^{N-j-1}$ of $x_1, \dots, x_m$ of degree $N-j-1$ such that $x - \pi(P) \in \mathfrak{m}_A^{N-j} = \pi(\mathfrak{m}^{N-j})$. This shows the assertion: $\pi(\mathfrak{m}^{N-j-1}) = \mathfrak{m}_A^{N-j-1}$. Thus by induction on j, we get the surjectivity of π.

Now suppose only that $\mathfrak{m}_A^N = 0$. Then in particular, $p^N A = 0$. Thus A is an $W/p^N W$–module. We can still define $\pi : B = W/p^N W[[X_1, \dots, X_m]] \to A$ by sending X_j to x_j. Then by the previous argument applied to B/pB and A/pA, we find that $\pi \mod p : B \otimes_W W/pW \cong B/pB \to A/pA \cong A \otimes_W W/pW$ is surjective. In particular, for the maximal ideal $\mathfrak{m}'$ of $W/p^N W$, $\pi \mod \mathfrak{m}' : B \otimes_W \mathbb{F} \cong B/\mathfrak{m}'B \to A/\mathfrak{m}'A \cong A \otimes_W \mathbb{F}$ is surjective. Then by Nakayama's lemma (cf. [CRT] §2 or [MFG] §2.1.3) applied to the nilpotent ideal $\mathfrak{m}'$, π is surjective.

In general, write $A = \varprojlim_i A_i$ for artinian rings A_i. Then the projection maps induce surjections $t^*_{A_{i+1}} \to t^*_{A_i}$. Since t^*_A is of finite dimensional, for sufficiently large i, $t^*_{A_{i+1}} \cong t^*_{A_i}$. Thus choosing x_j as above in A, we have its image $x_j^{(i)}$ in A_i. Use

$x_j^{(i)}$ to construct $\pi_i : W[[X_1, \dots, X_m]] \to A_i$ in place of x_j. Then π_i is surjective as already shown, and $\pi = \varprojlim_i \pi_i : W[[X_1, \dots, X_m]] \to A$ remains surjective, because projective limit of surjections, if all sets involved are finite sets, remain surjective (Exercise 1). Since $W[[X_1, \dots, X_m]]$ is noetherian ([CRT] Theorem 3.3), its surjective image A is noetherian. □

2.6. **Recall of group cohomology.** To prove noetherian property of Galois deformation ring R, we need to show the tangent space of $\mathrm{Spec}(R)$ has finite dimension. In order to give a Galois theoretic computation of the tangent space of the deformation ring, we introduce here briefly Galois cohomology groups. Consider a profinite group G and a continuous G-module X. Assume that X has either discrete or profinite topology.

Let $\mathbb{T}_p = \mathbb{Q}_p/\mathbb{Z}_p$. For any abelian p-profinite compact or p-torsion discrete module X, we define the Pontryagin dual module X^* by $X^* = \mathrm{Hom}_{cont}(X, \mathbb{T}_p)$ and give X^* the topology of uniform convergence on every compact subgroup of X. The G-action on $f \in X^*$ is given by $\sigma f(x) = f(\sigma^{-1}x)$. Then by Pontryagin duality theory (cf. [FAN]), we have $(X^*)^* \cong X$ canonically.

Exercise 2.11. *Show that if X is finite, $X^* \cong X$ noncanonically.*

Exercise 2.12. *Prove that X^* is a discrete module if X is p-profinite and X^* is compact if X is discrete.*

By this fact, if X^* is the dual of a profinite module $X = \varprojlim_n X_n$ for finite modules X_n with surjections $X_m \twoheadrightarrow X_n$ for $m > n$, $X^* = \bigcup_n X_n^*$ is a discrete module which is a union of finite modules X_n^*.

We denote by $H^q(G, X)$ the continuous group cohomology with coefficients in X. If X is finite, $H^q(G, X)$ is as defined in [MFG] 4.3.3. Thus we have

$$H^0(G, X) = X^G = \{x \in X | gx = x \text{ for all } g \in G\},$$

and if X is finite,

$$H^1(G, X) = \frac{\{G \xrightarrow{c} X : \text{continuous} | c(\sigma\tau) = \sigma c(\tau) + c(\sigma) \text{ for all } \sigma, \tau \in G\}}{\{G \xrightarrow{b} X | b(\sigma) = (\sigma - 1)x \text{ for } x \in X \text{ independent of } \sigma\}},$$

and $H^2(G, X)$ is given by

$$\frac{\{G \xrightarrow{c} X : \text{continuous} | c(\sigma, \tau) + c(\sigma\tau, \rho) = \sigma c(\tau, \rho) + c(\sigma, \tau\rho) \text{ for all } \sigma, \tau, \rho \in G\}}{\{G \xrightarrow{b} X | b(\sigma, \tau) = c(\sigma) + \sigma c(\tau) - c(\sigma\tau) \text{ for a continuous map } c : G \to X\}}.$$

If $X = \varprojlim_n X_n$ (resp. $X = \varinjlim_x X_n$) for finite G-modules X_n, we define

$$H^j(G, X) = \varprojlim_n H^j(G, X_n) \text{ (resp. } H^j(G, X) = \varinjlim_n H^j(G, X_n)).$$

For each Galois character $\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to W^\times$ and a W-module X with continuous action of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, we write $X(\psi)$ for the Galois module whose underlying W-module is X and Galois action is given by ψ. We simply write $X(i)$ for $X(\nu^i)$ for the p-adic cyclotomic character. In particular $\mathbb{Z}_p(1) \cong \varprojlim_n \mu_{p^n}(\overline{\mathbb{Q}})$ as Galois modules.

Let G be the (profinite) Galois group $G = \mathfrak{G}_F$ or $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ for a finite extension $K/\mathbb{Q}_p$. By a result of Tate, Galois cohomology "essentially" has cohomological dimension 2; so, H^0, H^1 and H^2 are important. If $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ for a finite extension $K/\mathbb{Q}_p$, by Tate duality (see [MFG] 4.42),

$$H^{2-i}(G, X) \cong \mathrm{Hom}(H^i(G, X^*(1)), \mathbb{Q}/\mathbb{Z})$$

for finite X.

For a general K-vector space V with a continuous action of G and a G-stable W-lattice L of V, we define $H^q(G, V) = H^q(G, L) \otimes_W K$.

Write $\mathfrak{G}_M = \mathrm{Gal}(F^{(p)}/M)$ for any intermediate field M of $F^{(p)}/F$, where $F^{(p)}/F$ is the maximal extension unramified outside p and ∞. By the inflation-restriction sequence (e.g., [MFG] 4.3.4),

$$0 \to H^1(\mathrm{Gal}(M/F), H^0(\mathfrak{G}_M, X)) \to H^1(\mathfrak{G}_F, X) \to H^1(\mathfrak{G}_M, X)$$

is exact. More generally, we can equip a natural action of $\mathrm{Gal}(M/F)$ on $H^1(\mathfrak{G}_M, X)$ and the sequence is extended to

$$\begin{aligned} 0 \to H^1(\mathrm{Gal}(M/F), H^0(\mathfrak{G}_M, X)) \\ \to H^1(\mathfrak{G}_F, X) \to H^0(\mathrm{Gal}(M/F), H^1(\mathfrak{G}_M, X)) \\ \to H^2(\mathrm{Gal}(M/F), H^0(\mathfrak{G}_M, X)) \end{aligned}$$

which is still exact.

2.7. **Cohomological interpretation of tangent spaces.** Let $R = R_{\overline{\rho}}$. We let $\mathfrak{G}_{\mathbb{Q}}$ acts on $M_n(\mathbb{F})$ by $gv = \overline{\rho}(g)v\overline{\rho}(g)^{-1}$. This $\mathfrak{G}_{\mathbb{Q}}$–module will be written as $ad(\overline{\rho})$.

Lemma 2.13. *Let $R = R_{\overline{\rho}}$ for an absolutely irreducible representation $\overline{\rho} : \mathfrak{G}_{\mathbb{Q}} \to GL_n(\mathbb{F})$. Then*

$$t_{R/W} = \mathrm{Hom}_{\mathbb{F}}(t^*_{R/W}, \mathbb{F}) \cong H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho})),$$

where $H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho}))$ is the continuous first cohomology group of $\mathfrak{G}_{\mathbb{Q}}$ with coefficients in the discrete $\mathfrak{G}_{\mathbb{Q}}$–module $V(ad(\overline{\rho}))$.

The space $t_{R/W}$ is called the tangent space of $\mathrm{Spec}(R)_{/W}$ at $\mathfrak{m}$.

Proof. Let $A = \mathbb{F}[X]/(X^2)$. We write ε for the class of X in A. Then $\varepsilon^2 = 0$. We consider $\phi \in \mathrm{Hom}_{W-alg}(R, A)$. Write $\phi(r) = \phi_0(r) + \phi_\varepsilon(r)\varepsilon$. Then we have from $\phi(ab) = \phi(a)\phi(b)$ that $\phi_0(ab) = \phi_0(a)\phi_0(b)$ and

$$\phi_\varepsilon(ab) = \phi_0(a)\phi_\varepsilon(b) + \phi_0(b)\phi_\varepsilon(a).$$

Thus $\mathrm{Ker}(\phi_0) = \mathfrak{m}_R$ because R is local. Since ϕ is W–linear, $\phi_0(a) = \overline{a} = a \bmod \mathfrak{m}_R$, and thus ϕ kills $\mathfrak{m}_R^2$ and takes $\mathfrak{m}_R$ W–linearly into $\mathfrak{m}_A = \mathbb{F}\varepsilon$. Moreover for $r \in W$, $\overline{r} = r\phi(1) = \phi(r) = \overline{r} + \phi_\varepsilon(r)\varepsilon$, and hence ϕ_ε kills W. Since R shares its residue field $\mathbb{F}$ with W, any element $a \in R$ can be written as $a = r + x$ with $r \in W$ and $x \in \mathfrak{m}_R$. Thus ϕ is completely determined by the restriction of ϕ_ε to $\mathfrak{m}_R$, which factors through $t^*_{R/W}$. We write ℓ_ϕ for ϕ_ε regarded as an $\mathbb{F}$–linear map from $t^*_{R/W}$ into $\mathbb{F}$. Then we can write $\phi(r + x) = \overline{r} + \ell_\phi(x)\varepsilon$. Thus $\phi \mapsto \ell_\phi$ induces a linear map $\ell : \mathrm{Hom}_{W-alg}(R, A) \to \mathrm{Hom}_{\mathbb{F}}(t^*_{R/W}, \mathbb{F})$. Note that $R/(\mathfrak{m}_R^2 + \mathfrak{m}_W) = \mathbb{F} \oplus t^*_{R/W}$. For any $\ell \in \mathrm{Hom}_{\mathbb{F}}(t^*_{R/W}, \mathbb{F})$, we extends ℓ to $R/\mathfrak{m}_R^2$ declaring its value on $\mathbb{F}$ is zero. Then define $\phi : R \to A$ by $\phi(r) = \overline{r} + \ell(r)\varepsilon$. Since $\varepsilon^2 = 0$, ϕ is an W–algebra homomorphism. In particular, $\ell(\phi) = \ell$, and hence ℓ is surjective. Since algebra homomorphisms killing $\mathfrak{m}_R^2 + \mathfrak{m}_W$ are determined by its values on $t^*_{R/W}$, ℓ is injective.

By the universality, we have

$$\mathrm{Hom}_{W-alg}(R, A) \cong \{\rho : \mathfrak{G}_{\mathbb{Q}} \to GL_n(A) | \rho \mod \mathfrak{m}_A = \overline{\rho}\}/\sim .$$

Then we can write $\rho(g) = \overline{\rho}(g) + u'_\rho(g)\varepsilon$. From the mutiplicativity, we have

$$\overline{\rho}(gh) + u'_\rho(gh)\varepsilon = \rho(gh) = \rho(g)\rho(h) = \overline{\rho}(g)\overline{\rho}(h) + (\overline{\rho}(g)u'_\rho(h) + u'_\rho(g)\overline{\rho}(h))\varepsilon,$$

Thus as a function $u' : \mathfrak{G}_{\mathbb{Q}} \to M_n(\mathbb{F})$, we have

$$u'_\rho(gh) = \overline{\rho}(g)u'_\rho(h) + u'_\rho(g)\overline{\rho}(h). \tag{2.2}$$

Define a map $u_\rho : \mathfrak{G}_{\mathbb{Q}} \to ad(\overline{\rho})$ by $u_\rho(g) = u'_\rho(g)\overline{\rho}(g)^{-1}$. Then by a simple computation, we have $gu_\rho(h) = \overline{\rho}(g)u_\rho(h)\overline{\rho}(g)^{-1}$ from the definition of $ad(\overline{\rho})$. Then from the above formula (2.2), we conclude that $u_\rho(gh) = gu_\rho(h) + u_\rho(g)$. Thus $u_\rho : \mathfrak{G}_{\mathbb{Q}} \to ad(\overline{\rho})$ is a 1–cocycle. Starting from a 1–cocycle u, we can reconstruct representation reversing the the above process. Then again by computation,

$$\begin{aligned}\rho \sim \rho' &\iff \overline{\rho}(g) + u'_\rho(g) = (1 + x\varepsilon)(\overline{\rho}(g) + u'_{\rho'}(g))(1 - x\varepsilon) \quad (x \in ad(\overline{\rho})) \\ &\iff u'_\rho(g) = x\overline{\rho}(g) - \overline{\rho}(g)x + u'_{\rho'}(g) \iff u_\rho(g) = (1 - g)x + u_{\rho'}(g).\end{aligned}$$

Thus the cohomology classes of u_ρ and $u_{\rho'}$ are equal if and only if $\rho \sim \rho'$. This shows:

$$\begin{aligned}&\mathrm{Hom}_{\mathbb{F}}(t^*_{R/W}, \mathbb{F}) \cong \mathrm{Hom}_{W-alg}(R, A) \cong \\ &\qquad \{\rho : \mathfrak{G}_{\mathbb{Q}} \to GL_n(A) | \rho \mod \mathfrak{m}_A = \overline{\rho}\}/\sim \cong H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho})).\end{aligned}$$

In this way, we get a bijection between $\mathrm{Hom}_{\mathbb{F}}(t^*_{R/W}, \mathbb{F})$ and $H^1(\mathfrak{G}_{\mathbb{Q}}, ad(\overline{\rho}))$. By tracking down (in the reverse way) our construction, one can check that the map is an $\mathbb{F}$–linear isomorphism. □

For each open subgroup H of a profinite group G, we write H_p for the maximal p–profinite quotient. We consider the following condition:

(Φ) *For any open subgroup H of G, the p-Frattini quotient $\Phi(H_p)$ is a finite group,*

where $\Phi(H_p) = H_p/\overline{(H_p)^p(H_p, H_p)}$ for the the commutator subgroup (H_p, H_p) of H_p.

Proposition 2.14 (Mazur)**.** *By class field theory, $\mathfrak{G}_{\mathbb{Q}}$ satisfies (Φ) , and $R_{\overline{\rho}}$ is a noetherian ring.*

Proof. Let $H = \mathrm{Ker}(\overline{\rho})$. Then the action of H on $ad(\overline{\rho})$ is trivial. By the inflation-restriction sequence for $G = \mathfrak{G}_{\mathbb{Q}}$, we have the following exact sequence:

$$0 \to H^1(G/H, H^0(H, ad(\overline{\rho}))) \to H^1(G, ad(\overline{\rho})) \to \mathrm{Hom}(\Phi(H_p), M_n(\mathbb{F})).$$

From this, it is clear that $\dim_{\mathbb{F}} H^1(G, ad(\overline{\rho})) < \infty$ if $\mathfrak{G}_{\mathbb{Q}}$ satisfies the p-Frattini condition (Φ). The fact that $\mathfrak{G}_{\mathbb{Q}}$ satisfies (Φ) follows from class field theory. Indeed, if F is the fixed field of H, then $\Phi(H_p)$ fixes the maximal p-abelian extension M/F of type $(p, p, \ldots, p)$ unramified outside p. Here a p-abelian extension M/F is of type $(p, p, \ldots, p)$ if $\mathrm{Gal}(M/F)$ is abelian killed by p. By class field theory, $[M : F]$ is finite. □

3. Vertical control theorem

Let $N \geq 1$ and $k \geq 1$ be integers. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ denote a Dirichlet character. Let $S_k(N, \chi)$ (resp. $G_k(N, \chi)$) be the complex vector space of elliptic cusp forms (resp. elliptic modular forms) of weight k for $\Gamma_0(N)$ with Neben character χ.

There is an integral structure on $S_k(N, \chi)$ coming from Fourier expansion. Let $\mathbb{Z}[\chi]$ denote the $\mathbb{Z}$-algebra generated by the values of the character χ. For each $\mathbb{Z}[\chi]$-algebra A sitting inside $\mathbb{C}$ we set

$$S_k(N, \chi, A) = \{f = \sum_{n=1}^{\infty} a(n, f)q^n \mid a(n, f) \in A\}$$

$$G_k(N, \chi, A) = \{f = \sum_{n=0}^{\infty} a(n, f)q^n \mid a(n, f) \in A\}.$$

It is a fact that for A as above,

$$S_k(N, \chi, A) = S_k(N, \chi, \mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A \text{ and } G_k(N, \chi, A) = G_k(N, \chi, \mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A$$

See [GME] III.1 or [LFE] Chapter 5 for different proofs. For a general algebra A, not necessarily in $\mathbb{C}$, we define $\mathcal{F}_k(n, \chi, A)$ by $\mathcal{F}_k(N, \chi, \mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A$, where $\mathcal{F}_k$ is S_k or G_k.

For each $n = 1, 2, \ldots$, there is a Hecke operator $T(n)$ which acts A-linearly on the space $G_k(N, \chi, A)$. It is given by the formula

$$a(m, f|T(n)) = \sum_{d|m, d|n} \chi(d)d^{k-1}a(mn/d^2, f). \tag{3.1}$$

See [MFG] 3.2 for a more intrinsic definition of the operators $T(n)$. It is customary to write $U(p)$ for $T(p)$ if p is a prime and $p|N$, because they have different effect on Fourier expansion.

Fix a complete discrete valuation ring W lying over $\mathbb{Z}_p$. Let T denote the maximal split torus in PGL_2. Thus $\mathrm{T} \xrightarrow{\sim} \mathbb{G}_m$. We have

$$\mathrm{T}(\mathbb{Z}_p) = \mathbb{Z}_p^\times = \mu_{p-1} \times \Gamma,$$

with $\Gamma \xrightarrow{\sim} \mathbb{Z}_p$, via $\gamma^s \mapsto s$, for $\gamma = 1 + p$, and $s \in \mathbb{Z}_p$. Recall the Iwasawa algebra $\Lambda_W = W[[X]]$. Hereafter, we write $\Lambda_W = W[[t]]$ using "t" to indicate variables (as we use X for something else). Then

$$W[[\mathrm{T}(Z_p)]] = \varprojlim_n W[\mathrm{T}(\mathbb{Z}/p^n\mathbb{Z})] \cong \Lambda_W[\mu_{p-1}] \text{ via } \Gamma \ni \gamma^s \mapsto (1+t)^s \in \Lambda_W.$$

If R is a p-profinite ring, then any continuous character $\phi : \Gamma \to R^\times$ extends to a character $\phi : \Lambda \to R$, which we shall again denote by ϕ. We may also consider ϕ as a character $\phi : W[[\mathrm{T}(\mathbb{Z}_p)]] \to W$. Thus if we write ν for the canonical inclusions

$$\nu : \Gamma \hookrightarrow \mathrm{T}(\mathbb{Z}_p) = \mathbb{Z}_p^\times \hookrightarrow W^\times,$$

then we may consider ν as a character $\nu : \Lambda \to W$. In particular we have $\nu^{k-1}(\Phi(t)) = \Phi(\gamma^{k-1} - 1) \in W$, for $\Phi(t) \in \Lambda$. We may also consider ν as a character $\nu : W[[\mathrm{T}(\mathbb{Z}_p)]] \to W$.

Let us now assume that N is such that $(p, N) = 1$, and that $k \geq 2$. For simplicity, we assume that the prime $p \geq 5$. This does not cause much harm if $N = 1$ because the space of p–ordinary cusp forms (that we will be mainly interested in) vanishes if $p \leq 7$ and $N = 1$. We fix a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to W^\times$. Sometimes we will think of the mod N Dirichlet character χ as a mod Np Dirichlet character. If we need to indicate the modulus M defining χ, we will write χ_M instead of just χ.

There is a projective $W[[\mathrm{T}(\mathbb{Z}_p)]]$-module $S_{\Gamma_0(N),\Lambda}[\chi]$ of finite type, the so called space of 'ordinary Λ-adic cusp forms of level Np^∞', which has an action of Hecke operators, again denoted by $T(n)$, such that

$$S_{\Gamma_0(N),\Lambda}[\chi] \otimes_{W[[\mathrm{T}(\mathbb{Z}_p)]],\nu^{k-1}} W \hookrightarrow S_k(Np, \chi, W).$$

Tensoring over $W[[\mathrm{T}(\mathbb{Z}_p)]]$ through ν^{k-1} does not alter the 'Neben' character χ we have fixed, but tensoring over Λ produces all spaces with 'Neben' characters $\chi\omega^a$ (for the Teichmüller character ω) as we will state later. Roughly, this map is realized as follows. Define the Hecke algebra $\mathrm{h}(N, \chi)$ to be the algebra generated over Λ by the Hecke operators $T(n)$ inside $\mathrm{End}_\Lambda(S_{\Gamma_0(N),\Lambda}[\chi])$. Let λ be a Λ-algebra homomorphism of $\mathrm{h}(N, \chi)$ into an algebraic closure of the field of fractions of Λ. For simplicity let us assume that $\lambda(T(n)) \in \Lambda$, for n. Write

$$F(t, q) = \sum_{n=1}^{\infty} \lambda(T(n))(t)q^n \in \Lambda[[q]]]$$

for the corresponding Λ-adic cusp form in $S_{\Gamma_0(N),\Lambda}[\chi]$. Then $F(\gamma^{k-1}-1, q) \in W[[q]]$, and is a classical modular form for $k \geq 2$. These classical forms interpolate the family of p-adic modular forms $F(\gamma^s - 1, q)$ for $s \in \mathbb{Z}_p$. In fact the following theorem is true (see [GME] §3.1–3.2):

Theorem 3.1 (Hida). *Fix a mod N Dirichlet character χ with values in $W^\times$. We have*

- $S_{\Gamma_0(N),\Lambda}[\chi] \otimes_{W[[\mathrm{T}(\mathbb{Z}_p)]],\nu^{k-1}} W \xrightarrow{\sim} S_k^{ord}(Np, \chi, W) \xrightarrow{\sim} S_k^{ord}(N, \chi, W),$ *for all $k \geq 3$,*
- $S_{\Gamma_0(N),\Lambda}[\chi] \otimes_{\Lambda,\nu^{k-1}} W \xrightarrow{\sim} \bigoplus_{a=0}^{p-2} S_k^{ord}(Np, \chi\omega^a, W),$ *for all $k \geq 2$,*

where $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ is the Teichmüller character.

A similar assertion holds for G_k in place of S_k.

In the theorem, the superscript *ord* means the ordinary part of the corresponding space of cusp forms. Let us recall what this means. For an W-module X of finite type, and an W-linear operator $T : X \to X$, we may decompose X

$$X = X^{ord} \oplus X^{nil}$$

where both X^{ord} and X^{nil} are T-stable, and moreover $T : X^{ord} \xrightarrow{\sim} X^{ord}$ and $\bigcap_{m=1}^{\infty} T^m(X^{nil}) = 0$. The idempotent corresponding to X^{ord} in the above decomposition is $\lim_{m\to\infty} T^{m!}$.

Apply this to $X = \mathcal{F}_k(M, \chi, W)$ for $M = N$ and Np with the operator

$$T = \begin{cases} T(p) & \text{if } M = N, \\ U(p) & \text{if } M = Np. \end{cases}$$

Then $\mathcal{F}_k^{ord}(M, \chi, W)$ is the ordinary part, X^{ord}, of $X = \mathcal{F}_k(M, \chi, W)$, where $\mathcal{F}_k$ is S_k or G_k.

The Hecke operator $T(p)$ acting on the space $G_k(N, \chi, W)$ and $T(p)$ acting on the larger space $G_k(Np, \chi, W)$ are not equal; so, we have written $U(p)$ for the p–th Hecke operator acting on $G_k(Np, \chi, W)$. These two operators $T(p)$ and $U(p)$ are congruent modulo p if $k \geq 2$. If further $k \geq 3$, the dimension of $S_k^{ord}(Np, \chi, W) \otimes_{\mathbb{Z}}$

$\mathbb{Z}/p\mathbb{Z}$ coincides with the level N counterpart, because all p–new forms in the level Np space with trivial 'Neben' p–character has eigenvalue $\pm\sqrt{\chi_N(p)}\sqrt{p}^{k-2}$ for $U(p)$ (see [MFM] Theorem 4.6.17), which is divisible by $\sqrt{p}$ if $k \geq 3$. Therefore, if

$$e_0 = \lim_{m\to\infty} T(p)^{m!} \quad \text{and} \quad e = \lim_{m\to\infty} U(p)^{m!},$$

are the ordinary projectors, we conclude that the p–ordinary projector e acting on $S_k(Np, \chi, W)$ induces an isomorphism of $e_0 S_k(N, \chi, W) = S_k^{ord}(N, \chi, W)$ onto $S_k^{ord}(Np, \chi, W)$ as long as $k \geq 3$. Thus the isomorphism between the level N space and the level Np space in the theorem is given by e^{-1} when $k \geq 3$. We emphasize that this isomorphism is induced by e and not by the natural inclusion; that is, $S_k^{ord}(N, \chi, W)$ is possibly distinct from $S_k^{ord}(Np, \chi, W)$ inside $S_k(Np, \chi, W)$. If $k = 2$, the image under e of $S_2^{ord}(N, \chi, W)$ could be smaller than $S_2^{ord}(Np, \chi, W)$.

Remark 3.1. When $k = 1$, the above theorem is false. We describe this phenomenon in more detail in Subsection 4.4, Remark 4.1.

Now define the Hecke algebra $h_k^{ord}(M, \chi, W)$ as the algebra generated by the Hecke operators $T(n)$ inside $\mathrm{End}_W(S_k^{ord}(M, \chi, W))$. We have:

Theorem 3.2 (Vertical control theorem;Hida). *We have*

- $\mathrm{h}(N, \chi) \otimes_{W[[\mathrm{T}(\mathbb{Z}_p)]], \nu^{k-1}} W \xrightarrow{\sim} h_k^{ord}(N, \chi, W)$, *for all* $k \geq 3$,
- $\mathrm{h}(N, \chi) \otimes_{\Lambda, \nu^{k-1}} W \xrightarrow{\sim} \bigoplus_{a=0}^{p-2} h_k^{ord}(Np, \chi\omega^a, W)$, *for all* $k \geq 2$.

Actually the vertical control theorems holds in a more general setting including $p = 2$ and 3 (see [GME] §3.1–3.2).

4. Deformation theory of mod p modular representations

4.1. **Galois representations.** Assume as before that $p \geq 5$, that $(N, p) = 1$ and that $k \geq 2$. However after this subsection, we allow a Dirichlet character modulo Np, since $\chi\omega^a$ appears as the 'Neben' character of the specialization of the Hecke algebra $\mathrm{h}(N, \chi)$. Thus we take a Dirichlet character ψ modulo Np with values in $W^\times$.

Fix an W-algebra homomorphism $\lambda : h_k(Np, \psi, W) \to W$. The following theorem is a consequence of a general theorem due to Eichler, Shimura, and Deligne:

Theorem 4.1. *There exists a continuous Galois representation*

$$\rho_\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(W),$$

satisfying

- ρ_λ *is unramified outside* Np, *and,*
- $\det(1 - \rho_\lambda(\mathrm{Frob}_\ell)X) = 1 - \lambda(T(\ell))X + \psi(\ell)\ell^{k-1}X^2$, *for* $\ell \not| Np$.

Let D_p denote a decomposition group at p. If λ factors through the p–ordinary part $h_k^{ord}(Np, \psi, W)$, the following further information at p is due to Deligne, Mazur and Wiles:

Theorem 4.2. *Suppose that λ factors through $h_k^{ord}(Np, \psi, W)$. Then the Galois representation ρ_λ is p-ordinary. That is, there are characters $\epsilon_{\rho_\lambda} : D_p \to W^\times$, and $\delta_{\rho_\lambda} : D_p \to W^\times$ with δ_{ρ_λ} unramified, such that*

$$\rho_\lambda|_{D_p} \sim \begin{pmatrix} \epsilon_{\rho_\lambda} & * \\ 0 & \delta_{\rho_\lambda} \end{pmatrix},$$

and $\delta_{\rho_\lambda}(\mathrm{Frob}_p) = \lambda(U(p))$.

For a detailed proof of the above two theorems, see, for example, [GME] IV.2.

Let $\overline{\rho}_\lambda$ be the mod p Galois representation defined by reduction:

$$\overline{\rho}_\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(W) \to \mathrm{GL}_2(\mathbb{F}),$$

where $\mathbb{F}$ is the residue field of W. Let us now impose the conditions $(ai_{\mathbb{Q}})$ and (rg_p) on $\overline{\rho}_\lambda$, where:

(ai_F): If $F/\mathbb{Q}$ is a number field, then the restriction of to $\overline{\rho}_\lambda$ to F:

$$\overline{\rho}_{\lambda|F} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\overline{\rho}_\lambda} \mathrm{GL}_2(\mathbb{F}),$$

is absolutely irreducible.

(rg_p): Let I_p denote the inertia subgroup at p. Then

$$\overline{\rho}_\lambda|_{I_p} \sim \begin{pmatrix} \epsilon_{\overline{\rho}_\lambda} & * \\ 0 & \delta_{\overline{\rho}_\lambda} \end{pmatrix}$$

with $\epsilon_{\overline{\rho}_\lambda} \neq \delta_{\overline{\rho}_\lambda}$ on I_p. In view of Theorem 4.2 above, this happens exactly when $\epsilon_{\overline{\rho}_\lambda}$ is ramified at p.

Note that there is a decomposition of the finite Λ-module $\mathrm{h} = \mathrm{h}(N, \chi)$:

$$\mathrm{h} = \oplus \mathrm{h}_{\mathfrak{m}}$$

as $\mathfrak{m}$ varies through the maximal ideals of h. Let $\mathbb{T} = \mathrm{h}_{\mathfrak{m}}$ be the local ring through which $\lambda : h_k^{ord}(Np, \psi, W) \to W$ factors. We write $\mathbb{T}^{red}$ for the quotient of $\mathbb{T}$ by its nilradical. The two algebras $\mathbb{T}$ and $\mathbb{T}^{ord}$ are equal if the character χ is primitive modulo N. The following theorem is due to Hida and Wiles:

Theorem 4.3. *There exists a Galois representation* $\rho_{\mathbb{T}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}^{red})$ *satisfying*

- $\rho_{\mathbb{T}}$ *is unramified outside* Np,
- $\det(1 - \rho_{\mathbb{T}}(\mathrm{Frob}_\ell)X) = 1 - T(\ell)|_{\mathbb{T}^{red}}X + \chi(\ell)\langle\ell\rangle X^2$, *for* $\ell \not| Np$, *where* $\langle\ell\rangle$ *denotes the image of* ℓ *under the natural map*

  $$W[[\mathrm{T}(\mathbb{Z}_p)]] \to \mathrm{h}(N, \chi) \to \mathbb{T}^{red},$$

  and,
- $\rho_{\mathbb{T}}$ *is* p*-ordinary, that is*

  $$\rho_{\mathbb{T}}|_{D_p} \sim \begin{pmatrix} \epsilon_{\rho_{\mathbb{T}}} & * \\ 0 & \delta_{\rho_{\mathbb{T}}} \end{pmatrix}.$$

  with $\delta_{\rho_{\mathbb{T}}}$ *unramified and* $\delta_{\rho_{\mathbb{T}}}(\mathrm{Frob}_p) = U(p)|_{\mathbb{T}^{red}}$.

A construction of the representation as above with coefficients in the total quotient ring of $\mathbb{T}^{red}$ was first given in [H86b]. Later by the technique of pseudo-representations invented by Wiles, we found $\rho_{\mathbb{T}}$ with coefficients in $\mathbb{T}$ in the isomorphism class of the representations constructed by [H86b]. The local behavior of $\rho_{\mathbb{T}}$ described above then follows from Theorem 4.2. See [MFG] 2.2 for generalities on pseudo-representations, and see [MFG] §3.2.3 for the construction of $\rho_{\mathbb{T}}$ by means of pseudo-representations.

4.2. **Deformation rings.** We keep the assumptions and notation of the previous section. In particular $\overline{\rho}_\lambda$ is the reduction of the Galois representation ρ_λ attached to $\lambda : h_k^{ord}(Np, \psi, W) \to W$. However, to make our exposition simple, from now on, we will assume that

$$N = 1.$$

As before, we write ψ for the Dirichlet character modulo p of λ. Thus the local ring $\mathbb{T} = \mathbb{T}^{red}$ is the direct factor of $\mathrm{h}(1, \mathbf{1})$ (through which λ factors) for the identity character $\chi = \mathbf{1}$ (modulo 1). Recall Theorem 2.9:

Theorem 4.4 (Mazur)**.** *If* $(ai_{\mathbb{Q}})$ *and* (rg_p) *hold, then the universal deformation ring* $R = R^{ord}$ *and universal Galois representation* $\boldsymbol{\rho}^{ord} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(R)$ *exist.*

Here R is a p-profinite local W-algebra with $R/\mathfrak{m}_R = \mathbb{F}$. Furthermore $\boldsymbol{\rho}^{ord} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(R)$ satisfies:

- $\boldsymbol{\rho}^{ord}$ is unramified outside p,
- $\boldsymbol{\rho}^{ord}$ is p-ordinary, that is
$$\boldsymbol{\rho}^{ord}|_{D_p} \sim \begin{pmatrix} \boldsymbol{\epsilon} & * \\ 0 & \boldsymbol{\delta} \end{pmatrix},$$
with $\boldsymbol{\delta} : D_p \to R^\times$ unramified, and,
- $\boldsymbol{\rho}^{ord}$ mod $\mathfrak{m}_R \sim \overline{\rho}_\lambda$.

Moreover the couple $(R, \boldsymbol{\rho}^{ord})$ is universal in the sense that for any pair (A, ρ_A) with

- A a p-profinite local W-algebra with $A/\mathfrak{m}_A = \mathbb{F}$,
- $\rho_A : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(A)$ an unramified outside p, p-ordinary representation in the sense above, and,
- ρ_A mod $\mathfrak{m}_A \sim \overline{\rho}_\lambda$,

there is a unique map of local W-algebras $\varphi_A : R \to A$, such that

$$\varphi_A \circ \boldsymbol{\rho}^{ord} \sim \rho_A.$$

See [MFG] 2.3 and 3.2.3 for a proof of the existence of the universal couple (R, ρ_R).

4.3. **Theorem 4.5:** $R = \mathbb{T}$**.** By Theorem 4.3, we see that there exists a map of local W-algebras

$$\varphi_{\mathbb{T}} : R \longrightarrow \mathbb{T}.$$

The following theorem was conjectured by Mazur only under $(ai_{\mathbb{Q}})$:

Theorem 4.5 (Wiles)**.** *For* $\kappa = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$, *assume that* $\overline{\rho}_\lambda$ *satisfies* (rg_p) *and* (ai_κ)*). (In particular it satisfies* $(ai_{\mathbb{Q}})$*.) Then the map* $\varphi_{\mathbb{T}} : R \to \mathbb{T}$ *is an isomorphism of local* W*-algebras.*

Note that the surjectivity of $\varphi_{\mathbb{T}}$ is obvious:

Lemma 4.6. *The map* $\varphi_{\mathbb{T}} : R \to \mathbb{T}$ *is surjective.*

Proof. Let $\mathbb{T}'$ be the Λ-subalgebra of $\mathbb{T}$ generated by $T(l)$ for all primes $l \neq p$. Then $\mathrm{Tr}\rho_{\mathbb{T}}$ has values in $\mathbb{T}'$, and $\varphi_{\mathbb{T}}$ has image $\mathbb{T}'$. We need to prove $\mathbb{T} = \mathbb{T}'$ ($\Leftrightarrow U(p) \in \mathbb{T}'$).

Since $\rho_{\mathbb{T}'}$ has values in $GL_2(\mathbb{T}')$ and

$$H_0(I_p, \rho_{\mathbb{T}'}) \cong \mathbb{T}'$$

as $\overline{\epsilon}|_{I_p} = \boldsymbol{\epsilon}|_{I_p} \mod \mathfrak{m}_{\mathbb{T}}$ is non-trivial. Thus the action of $Frob_p$ on $H_0(I_p, \rho_{\mathbb{T}'}) \cong \mathbb{T}'$ is a multiplication by $\boldsymbol{\delta}(Frob_p) = U(p)$; so, $U(p) \in \mathbb{T}'$. □

4.4. **Theorem 4.7: $R^{ord,\phi} = T^{\phi}$.** We now investigate the deformation problem when the determinant is fixed.

Fix a character $\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to W^{\times}$, unramified outside p and ∞ and let us assume that $\det \overline{\rho}_{\lambda} = \phi \mod \mathfrak{m}_W$. Note that for each local W-algebra A as above, we have the algebra homomorphism $\iota_A : W^{\times} \to A^{\times}$ giving the W–algebra structure on A, so that it makes sense to impose the further condition

$$\det \rho_A = \iota_A \circ \phi$$

on the deformation problem considered above. This new deformation problem also has a solution; call the universal couple $(R^{ord,\phi}, \boldsymbol{\rho}^{ord,\phi})$.

On the other hand ϕ factors through the Galois group of the maximal abelian extension $\mathbb{Q}(\mu_{p^\infty})$ of $\mathbb{Q}$ unramified outside p (and ∞). Since

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \mathbb{Z}_p^{\times} = \mathrm{T}(\mathbb{Z}_p),$$

we can think of ϕ as a character

$$\phi : W[[\mathrm{T}(\mathbb{Z}_p)]] \to W. \tag{4.1}$$

Now set

$$T^{\phi} = \mathbb{T} \otimes_{W[[\mathrm{T}(\mathbb{Z}_p)]],\phi} W = \mathbb{T}/P_{\phi}\mathbb{T},$$

where P_{ϕ} is the kernel of ϕ in (4.1). Also set $\rho_{T^{\phi}} = \rho_{\mathbb{T}} \mod P_{\phi}$. We now have the following key theorem:

Theorem 4.7 (Wiles-Taylor)**.** *Assume that $\overline{\rho}_{\lambda}$ satisfies (rg_p) and (ai_{κ})), where $\kappa = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$. Then*

$$(R^{ord,\phi}, \boldsymbol{\rho}^{ord,\phi}) \cong (T^{\phi}, \rho_{T^{\phi}}).$$

The above theorem was first proved by Wiles in [W1] as Theorem 3.3, under the assumption that T^{ϕ} is a local complete intersection. The local complete intersection property was then proved by Taylor and Wiles in [TW], where they also give another direct proof of the theorem. As mentioned in the Introduction, we wish to describe this latter method of Taylor-Wiles [TW] incorporating improvements due to Diamond and Fujiwara. We will follow Fujiwara's treatment [Fu] (see also [HMI]). Note that [Fu] (and [HMI] §3.2) also contains a generalization of the above theorem to totally real fields.

Let us now describe the content of the above theorem in more down-to-earth terms. Let A be a valuation ring finite flat over W. We pick any Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(A)$ which is a p–ordinary deformation with determinant $\phi = \psi\nu_p^{k-1}$ for the p–adic cyclotomic character ν_p and a positive integer $k \geq 2$, where $\psi : \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \to \mathbb{Z}_p^{\times}$ is a character (which could be trivial). Then by the above theorem, we have a unique W–algebra homomorphism $\pi : R^{ord,\phi} = T^{\phi} \to A$ such that $\pi \circ \rho_{T^{\phi}}$ is equivalent to ρ. Under the condition $k \geq 2$, the ring T^{ϕ} is a direct factor of the Hecke algebra $h_k(p, \psi, W)$; so, we may regard π as an W–algebra homomorphism $\pi : h_k(p, \psi, W) \to A$. Since $h_k(p, \psi, W) = h_k(p, \psi, \mathbb{Z}[\psi]) \otimes_{\mathbb{Z}[\psi]} W$, π induces a $\mathbb{C}$–algebra homomorphism $\pi_{\mathbb{C}}$ of $h_k(p, \psi, \mathbb{C}) = h_k(p, \psi, \mathbb{Z}[\psi]) \otimes_{\mathbb{Z}[\psi]} \mathbb{C}$ into

$\mathbb{C}$, which is associated to a Hecke eigenform $f = \sum_{n=1}^{\infty} \pi_{\mathbb{C}}(T(n))q^n$. Thus ρ is isomorphic to the p–adic Galois representation ρ_f associated to the Hecke eigenform f.

Remark 4.1. When $k = 1$, we have a natural homomorphism

$$\pi : T^{\phi} \to h_1^{ord}(p, \phi, W)$$

if ϕ is a finite order character. The homomorphism often has a non-trivial kernel ([H98]) and could have trivial image. A result of Deligne and Serre says that to each weight 1 classical (or equivalently 'true') Hecke eigenform one may associate a two dimensional Artin Galois representation. Thus the image of π is expected to be non-trivial if $\rho_{\mathbb{T}}$ specializes to a Galois representation with finite image at weight 1. This expectation was proved by Langlands [BCG] (and Tunnel) for Artin representations whose image in $\mathrm{PGL}_2(\mathbb{C})$ is a tetrahedral or octahedral group (for example, see [GME] V.1.3). On the other hand, as was shown by Mazur-Wiles [MaW], often the image of the specialization is infinite (so the image of π would have to be trivial in this case). By a recent solution of Serre's mod p modularity conjecture by Khare–Wintenberger and Kisin, all 2-dimensional odd Artin representation is associated to a Hecke eigenform of weight 1 (cf. [KhW] and [Kh1] Theorem 7.1).

Remark 4.2. The argument of Taylor-Wiles (and also the original argument of Wiles in [W1] proving Theorem 3.3 there) actually gives a result covering general $N \geq 1$ when the ramification of the deformations is minimal (see [W1] page 455-8 for a description of the term minimal). Then Wiles analyzed carefully the difference of the Hecke algebra in the minimal case and those without the minimality conditions and reached the following more general (and more convenient) result. To describe it, we need some more notation and conditions: Let Σ be a finite set of primes including the fixed odd prime p and $\mathbb{Q}^{\Sigma}$ be the maximal extension unramified outside Σ and ∞. Let $\mathfrak{G}_{\Sigma} = \mathrm{Gal}(\mathbb{Q}^{\Sigma}/\mathbb{Q})$. We pick an absolutely irreducible *odd* representation $\overline{\rho} : \mathfrak{G} \to GL_2(\mathbb{F})$ for a finite field $\mathbb{F}$ of characteristic p. Hereafter all valuation rings will be finite flat over $\mathbb{Z}_p$. We consider the following conditions:

(Ordinarity) $\overline{\rho}|_{D_p} \cong \left(\begin{smallmatrix} \overline{\varepsilon} & * \\ 0 & \overline{\delta} \end{smallmatrix}\right)$ with $\overline{\delta}$ unramified and $\overline{\delta} \neq \overline{\varepsilon}$ on the decomposition group D_p at p;

(Flatness) $\overline{\rho}$ restricted to the decomposition group at p is isomorphic to a Galois module associated to a locally free group scheme over $\mathbb{Z}_p$ of rank $|\mathbb{F}|^2$;

(Irreducibility) $\overline{\rho}$ restricted to $\mathrm{Gal}(\mathbb{Q}^{\Sigma}/\mathbb{Q})$ is absolutely irreducible;

Theorem 4.8 (Modular Lifting Theorem)**.** *Suppose irreducibility and either ordinarity or flatness of $\overline{\rho}$. Let $\rho : \mathfrak{G}_{\Sigma} \to GL_2(W)$ be a Galois representation for a DVR W such that*

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

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

The above theorem was proven via an $R = T$ theorem in [W1] as Theorem 0.2 under an additional condition on mod p modularity of $\overline{\rho}$, auxiliary ramification outside p and irreducibility over $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}[\mu_p])$. The above statemnet is slightly weaker than $R = T$-theorem as the identification of R and T is not specified. The irreduciblity over $\mathbb{Q}[\mu_p]$ is eased to irreducibility over $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by Skinner–Wiles [SW]. Wiles proved the result assuming the complete intersection property of a certain Hecke algebra in the minimal ramification case, which was in turn proved in [TW]. By the solution of Serre's mod p modularity conjecture by Khare–Wintenberger, we no longer need to assume mod p modularity for $\overline{\rho}$. The flatness condition has now been eased by Kisin [Ki] to potential flatness over an extension of $\mathbb{Z}_p$.

4.5. **Theorem 4.7 + Vertical control ⇒ Theorem 4.5.** It turns out that Theorem 4.7 and the vertical control theorem (Theorem 3.2) imply Wiles' main theorem (Theorem 4.5). To see this we first prove the following lemma:

Lemma 4.9. *$\mathbb{T}$ is a free Λ-module of finite rank.*

Proof. By Theorem 3.2 (for $\chi = \mathbf{1}$), applied with $\phi = \nu^{k-1}$, we see that $\mathbb{T}/P_\phi\mathbb{T}$ sits inside a Hecke algebra of weight k, and so in particular it is W-free, of finite rank, say r. By Nakayama's lemma the minimal number of generators of $\mathbb{T}$ over Λ is r as well. Let $x_1, \ldots, x_r$ be generators of $\mathbb{T}$, and let

$$\begin{array}{rcl} \pi : \Lambda^r & \twoheadrightarrow & \mathbb{T} \\ (\lambda_1, \ldots, \lambda_r) & \mapsto & \displaystyle\sum_{i=1}^{r} \lambda_i x_i. \end{array}$$

Now, by Nakayama's lemma again, $\mathbb{T}/P_{\nu^{j-1}}\mathbb{T}$ must be W-free of finite rank r for each $j \geq 2$. This forces $\ker(\pi) \subset P^r_{\nu^{j-1}}$ for each j, and so

$$\ker(\pi) \subset \cap_{j\geq 2} P^r_{\nu^{j-1}} = 0,$$

as desired. □

Proposition 4.10. *Theorem 4.7 + Vertical control $\Longrightarrow$ Theorem 4.5.*

Proof. Choose $\phi = \nu^{k-1}$ for some $k \geq 2$. Since $R/P_\phi R = \mathbb{T}/P_\phi\mathbb{T}$ by Theorem 4.7, we know that $R/P_\phi R$ is W-free of finite rank r, by Lemma 4.9. By Nakayama's lemma there is a surjective map $\Lambda^r \to R$. On the other hand, by Lemma 4.6, the map $\varphi_{\mathbb{T}} : R \to \mathbb{T}$ is surjective. Since $\mathbb{T} \xrightarrow{\sim} \Lambda^r$ (by Lemma 4.9), $\varphi_{\mathbb{T}} : R \to \mathbb{T}$ is forced to be an isomorphism. □

5. Horizontal control theorems

In this section we will establish horizontal control theorems on both the Galois and Hecke sides. These will be useful in proving Theorem 4.7 above.

5.1. **Galois side.** Recall that $\overline{\rho} := \overline{\rho}_\lambda$ was the reduction of ρ_λ, for fixed $\lambda : h_k^{ord}(p, \psi, W) \to W$. This representation was unramified outside p and was p-ordinary. In addition we had imposed the conditions $(ai_\kappa))$ and (rg_p) on $\overline{\rho}_\lambda$.

Let $Q = \{q_1, \dots q_r\}$ denote a finite set of primes, with $q_i \equiv 1 \bmod p$, for $q_i \in Q$. Let us consider the deformation problem, that allows, in addition, ramification at primes in Q (we also fix a determinant $\phi = \psi\nu_p^{k-1}$). Let $(R_Q^{ord,\phi}, \rho_{R_Q^{ord,\phi}})$ be the universal couple for this deformation problem.

We now impose the following condition: for each $q \in Q$, assume

(rg_q): If

$$\overline{\rho}_\lambda(\mathrm{Frob}_q) = \begin{pmatrix} \bar{\alpha}_q & * \\ 0 & \bar{\beta}_q \end{pmatrix},$$

then $\bar{\alpha}_q \neq \bar{\beta}_q$.

Let D_q denote a decomposition group at q and let I_q denote the corresponding inertia group at q. We have the following theorem on the local behavior of $\rho_{R_Q^{ord,\phi}}$ at q:

Theorem 5.1 (Faltings)**.** *Let $q \in Q$ and assume (rg_q) above. Then*

$$\rho_{R_Q^{ord,\phi}}|_{I_q} \sim \begin{pmatrix} \phi\delta_q^{-1} & 0 \\ 0 & \delta_q \end{pmatrix},$$

for some character $\delta_q : D_q \to R_Q^{ord,\phi\,\times}$.

Recall that local class field theory gives us the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{Q}_q^{ab}/\mathbb{Q}_q) \arrow[r, phantom, "\cong"] & D_q^{ab} \arrow[d, phantom, "\cup"] & \mathbb{Q}_q^\times \arrow[l, hook', "\text{dense}"'] \arrow[d, phantom, "\cup"] & \\
& I_q^{ab} & \mathbb{Z}_q^\times \arrow[l, "\simeq"'] \arrow[r, phantom, "="] & \Delta_q \times \Delta'_q \times 1 + q\mathbb{Z}_q,
\end{tikzcd}$$

where Δ_q, respectively Δ'_q, is the p-Sylow subgroup, respectively prime-to-p part, of $\mathbb{F}_q^\times$.

Now since $\overline{\rho}_\lambda$ is unramified at q, we have

$$\delta_q(I_q^{ab}) \subset 1 + \mathfrak{m}_{R_Q^{ord,\phi}}.$$

Since $1 + \mathfrak{m}_{R_Q^{ord,\phi}}$ is p-profinite, $\delta_q|_{I_q^{ab}}$ factors through Δ_q. Thus we get a map

$$\Delta_Q := \prod_{q \in Q} \Delta_q \xrightarrow{\prod_{q\in Q}\delta_q} R_Q^{\phi\,\times},$$

via which we may consider $R_Q^{ord,\phi}$ as an $W[\Delta_Q]$-algebra.

We note in passing that $W[\Delta_Q]$ is a p-profinite local W-algebra with residue field $\mathbb{F}$.

We denote by $\mathfrak{A}_Q$ the augmentation ideal of the group algebra $W[\Delta_Q]$, that is, $\mathfrak{A}_Q$ is the kernel of the augmentation map $W[\Delta_Q] \to W$, which sends $\sigma \in \Delta_q$ to 1.

The following result establishes horizontal control for the rings R_Q^ϕ:

Proposition 5.2 (Horizontal control: Galois side)**.** *The natural map*

$$R_Q^{\phi} \longrightarrow R^{ord,\phi}$$

induces an isomorphism

$$R_Q^{ord,\phi}/\mathfrak{A}_Q R_Q^{ord,\phi} \xrightarrow{\sim} R^{ord,\phi}.$$

Proof. By the universal property of $R^{ord,\phi}$ it suffices to show that the couple $(R_Q^{ord,\phi}/\mathfrak{A}_Q R_Q^{ord,\phi}, \rho_{R_Q^{ord,\phi}} \bmod \mathfrak{A}_Q)$ is universal for the 'unramified outside p, p-ordinary, det $= \phi$' deformation problem. So say that $\rho_A : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(A)$ is such a deformation. Since, vacuously, ρ_A is unramified outside $Q \cup \{p\}$, there is a unique morphism $\varphi_A : R_Q^{ord,\phi} \to A$ such that

$$\varphi_A \circ \rho_{R_Q^{ord,\phi}} = \rho_A. \tag{5.1}$$

Restricting (5.1) to I_q we see that (cf. Theorem 5.1):

$$\begin{pmatrix} \phi\delta_q^{-1} & 0 \\ 0 & \delta_q \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

on I_q. Thus $\varphi_A(\delta_q(\sigma) - 1) = 0$, for $\sigma \in \Delta_q$. This shows that $\varphi_A(\mathfrak{A}_Q) = 0$, and we may consider φ_A as a map

$$\varphi_A : R_Q^{ord,\phi}/\mathfrak{A}_Q R_Q^{ord,\phi} \to A.$$

If there is another $\phi : R_Q^{ord,\phi}/\mathfrak{A}_Q R_Q^{ord,\phi} \to A$ giving rise to ρ_A, the pull back of ϕ has to coincide with φ_A by the universality of $R_Q^{ord,\phi}$. Thus this φ_A is unique; so, $(R_Q^{ord,\phi}/\mathfrak{A}_Q R_Q^{\phi}, \rho_{R_Q^{ord,\phi}} \bmod \mathfrak{A}_Q)$ is universal for the 'unramified outside p, p-ordinary, det $= \phi$' deformation problem. □

5.2. **Hecke side.** We now establish horizontal control on the Hecke side. This is a much more delicate matter (compared to the Galois side), and the proof will use some algebraic geometry. Since we can choose ϕ congruent to $\det \overline{\rho}_\lambda$ modulo p, we may assume that $\phi = \nu^{k-1}$ with $k \geq 3$ and $\psi = \chi = \mathbf{1}$.

Let $N_Q = \prod_{q \in Q} q$, and consider the space of cusp forms on $\Gamma_1(N_Q) \cap \Gamma_0(p)$. We can define Hecke algebras $h_k^{ord}(p, \Gamma_1(N_Q), \psi, W)$ as the algebra generated by all the Hecke operators inside $\mathrm{End}_W(S_k(\Gamma_1(N_Q) \cap \Gamma_0(p))$. We have the following commutative diagram

$$\begin{tikzcd}
h_k^{ord}(p, \Gamma_1(N_Q), \psi, W) \arrow[r, phantom, "\supset"] \arrow[d] & T_Q^{\phi} \arrow[d] \\
h_k^{ord}(p, \psi, W) \arrow[r, phantom, "\supset"] & T^{\phi},
\end{tikzcd}$$

where the first vertical maps is the natural projection, and T_Q^{ϕ} is defined as a local factor of the pre-image of T^{ϕ} under this projection. The choice of T_Q^{ϕ} depends on the choice of the $\overline{\alpha}_q$ out of the two eigenvalues of $\overline{\rho}_\lambda(\mathrm{Frob}_q)$ for $q \in Q$ as we will see later.

Since the new Hecke algebra is defined with respect to $\Gamma_1(N_Q) \cap \Gamma_0(p)$, the action of $\langle \ell \rangle$ factors through $\mathrm{T}(\mathbb{Z}_p \times (\mathbb{Z}/N_Q\mathbb{Z}))$ instead of $\mathrm{T}(\mathbb{Z}_p)$. We decompose

$$\mathrm{T}(\mathbb{Z}_p \times (\mathbb{Z}/N_Q\mathbb{Z})) = \Gamma \times \mu_{p-1} \times \Delta_Q' \times \Delta_Q$$

so that Δ_Q is the p–Sylow subgroup of $(\mathbb{Z}/N_Q\mathbb{Z})^\times$. The action of the quotient group $\Gamma_0(N_Q)/\Gamma_1(N_Q) = (\mathbb{Z}/N_Q\mathbb{Z})^\times$ gives rise to an action of

$$\Delta_Q \subset \mathrm{T}(\mathbb{Z}_p \times (\mathbb{Z}/N_Q\mathbb{Z}))$$

on the Hecke algebra $h_k^{ord}(p, \Gamma_1(N_Q), \psi, W)$. This action induces a canonical W–algebra homomorphism of the completed group algebra $W[[\mathrm{T}(\mathbb{Z}_p \times (\mathbb{Z}/N_Q\mathbb{Z}))]]$ into T_Q^ϕ. Since T_Q^ϕ is local, this algebra homomorphism factors through a local ring of $W[[\mathrm{T}(\mathbb{Z}_p \times (\mathbb{Z}/N_Q\mathbb{Z}))]]$, which is canonically isomorphic to $\Lambda[\Delta_Q]$ (that is, the quotient of $W[[\mathrm{T}(\mathbb{Z}_p \times (\mathbb{Z}/N_Q\mathbb{Z}))]]$ by the augmentation ideal of the group algebra $W[\mu_{p-1} \times \Delta'_Q]$). For primes $\ell \nmid pN_Q$, we write $\langle \ell \rangle$ for the image of $\ell \in \mathrm{T}(\mathbb{Z}_p \times (\mathbb{Z}/N_Q\mathbb{Z}))]]$ in T_Q^ϕ.

As in Theorem 4.3 we can construct a continuous Galois representation:

$$\rho' = \rho'_{T_Q^\phi} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(T_Q^\phi),$$

with $\det \rho'_{T_Q^\phi}(\mathrm{Frob}_\ell) = \ell^{k-1}\langle \ell \rangle$ and $U(q)|_{T_Q^\phi} \equiv \overline{\alpha}_q \mod \mathfrak{m}$ for the maximal ideal $\mathfrak{m} = \mathfrak{m}_{T_Q^\phi}$ of T_Q^ϕ. Thus the choice of T_Q^ϕ depends on the choice of the root $\overline{\alpha}_q$ for each $q \in Q$, but the isomorphism class of the W–algebra T_Q^ϕ and that of the Galois representation ρ' are independent of the choice, because the algebra is generated by $T(\ell)$ for primes ℓ with $\ell \nmid pN_Q$ and the Galois representation is determined by $\mathrm{Tr}(\rho'(\mathrm{Frob}_\ell)) = T(\ell)$. Since $\det \rho' \equiv \phi \mod \mathfrak{m}$, the ratio $\phi/\det \rho'$ has a p–power order. Since p is odd, we have a unique $\sqrt{\phi/\det \rho'}$. We define

$$\rho_{T_Q^\phi} = \sqrt{\phi/\det \rho'} \otimes \rho'_{T_Q^\phi},$$

which satisfies $\det \rho_{T_Q^\phi} = \phi$ and $\rho_{T_Q^\phi} \equiv \overline{\rho}_\lambda \mod \mathfrak{m}$.

We can now state the horizontal control on the Hecke side:

Theorem 5.3 (Horizontal control: Hecke side)**.** *Fix $\phi = \nu^{k-1}$ for $k \geq 2$. Then*

- *$T_Q^\phi/\mathfrak{A}_Q T_Q^\phi \xrightarrow{\sim} T^\phi$, where $\mathfrak{A}_Q$ is the augmentation ideal inside $W[\Delta_Q]$,*
- *T_Q^ϕ is $W[\Delta_Q]$-free of rank d_Q, say, and,*
- *$d_Q = d$ is independent of Q.*

5.3. **Proof of Theorem 5.3.** In this section, we shall give a brief sketch of the proof of Theorem 5.3, referring the reader to [GME] III.1-2 for more details. For simplicity, we assume an extra condition: $k \geq 3$, in order not to worry about the reduction modulo p of modular curves of level divisible by p.

Let $\mathcal{W}$ be a complete d.v.r. over $\mathbb{Z}_p$ with $p \geq 5$. Let S be a scheme over $\mathcal{W}$. Let $E \xrightarrow{\pi} S$ be an elliptic curve over S. Assume that $\pi_*\Omega_{E/S} = W_S\omega$. Consider the functor

$$\begin{array}{rcl} \mathcal{W} - Schemes & \longrightarrow & Sets \\ S & \mapsto & [(E, \omega)_{/S}], \end{array}$$

where [ ] means the set of isomorphism classes. This functor is represented by the affine scheme $\mathcal{M} = \mathrm{Spec}(\mathcal{A})$ where

$$\mathcal{A} = \mathcal{W}[g_2, g_3, \frac{1}{\Delta}],$$

with $\Delta = 27g_2^3 - g_3^2$. Each $\mathcal{W}$–algebra homomorphism $\phi : \mathcal{A} \to A$ gives rise to the elliptic curve $E_{/A} : y^2 = 4x^3 - \phi(g_2)x - \phi(g_3)$ with differential $\omega = \frac{dx}{y}$.

Now say $S = \mathrm{Spec}(A)$ is affine. Then $\lambda \in \mathbf{G}_m(S) = A^\times$ acts on the above functor via

$$(E, \omega) \mapsto (E, \lambda\omega).$$

It therefore acts on $\mathcal{A}$. Let $\mathcal{A}_j$ denote the corresponding eigenspace under the action of $\mathbf{G}_m$ corresponding to $\lambda \cdot x = \lambda^{-j}x$. Then we may decompose (e.g. [GME] I.6.5)

$$\mathcal{A} = \oplus_{j\in\mathbb{Z}}\mathcal{A}_j.$$

Let $\overline{\mathcal{A}} = \mathcal{W}[g_2, g_3] \subset \mathcal{A}$, and let $\overline{\mathcal{A}}_j$ be the integral closure of $\mathcal{A}_j$ in $\mathcal{A}$. We have

$$\overline{\mathcal{A}} = \oplus_{j\geq 0}\overline{\mathcal{A}}_j$$

Note that $g_2 \in \overline{\mathcal{A}}_4$ and $g_3 \in \overline{\mathcal{A}}_6$.

Definition 5.1. For any $\mathcal{W}$–algebra A, a modular form of weight k integral over A is an element $f \in \overline{\mathcal{A}}_k \otimes_{\mathcal{W}} A$.

This definition agrees with the earlier definition of modular forms of level one, since $G_k(1, \mathbf{1}, \mathcal{W}) = \overline{\mathcal{A}}_k$ is classically known to be spanned over $\mathcal{W}$ by the monomials $g_2^a g_3^b$ for $4a+6b = k$, where g_2 (resp. g_3) is the weight 4 (resp. weight 6) Eisenstein series in $G_k(SL_2(\mathbb{Z}))$ normalized so that its constant term is equal to 1. Polynomials of g_2 and g_3 with this skewed homogeneity condition: $4a+6b = k$ are called isobaric polynomials of weight k. The above definition includes $A = \mathcal{W}/p^n\mathcal{W}$, giving a geometric definition of modular forms (independent of its analytic behavior). We write $G_k(1, \mathbf{1}, A)$ for $\overline{\mathcal{A}}_k \otimes_{\mathcal{W}} A$, which is consistent with our earlier definition.

Let $(\mathbb{E}, \boldsymbol{\omega}) \to \mathcal{M}$ denote the universal elliptic curve, defined over $\mathcal{A}$ by the equation $Y^2 = 4X^3 - g_2X - g_3$ with $\boldsymbol{\omega} = \frac{dX}{Y}$. For each elliptic curve $(E, \omega)_{/S}$, with $S = \mathrm{Spec}(A)$, there is a unique morphism $\iota : S \to \mathcal{M}$ such that

$$(E, \omega) = (S \times_{\iota,\mathcal{M}} \mathbb{E}, \iota^*\boldsymbol{\omega}).$$

We define $f(E, \omega) = i^*(f) \in A$, where $\iota^* : \mathcal{A} \to A$ is the pullback map of ι. Note that this makes f a function on pairs $(E, \omega)_{/S=\mathrm{Spec}(A)}$ such that

- $f(E, \omega) \in A$,
- we have $\phi(f(E, \omega)) = f((E, \omega) \otimes_{A,\phi} B)$ if $\phi : A \to B$ is a $\mathcal{W}$–algebra homomorphism,
- the values of $f(E, \omega)$ only depend on the isomorphism class of (E, ω), and,
- $f(E, \lambda\omega) = \lambda^{-k}f(E, \omega)$, for $\lambda \in A^\times$.

By Fourier expansion, we can embed $\mathcal{A}$ into $\mathcal{W}((q)) = \mathcal{W}[[q]][\frac{1}{q}]$. Then we define $Tate(q) = \mathbb{E}\otimes_{\mathcal{A}}\mathcal{W}((q))$ ([**?**]). We write ω_∞ for the image of $\boldsymbol{\omega}$ on $Tate(q)$. The curve $Tate(q)$ is canonically embedded into the projective space $\mathbf{P}^2_{/\mathcal{W}((q))}$ using the equation $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$. Since the coefficients of the above equation is contained in $\mathcal{W}[[q]]$, the curve $Tate(q)_{/\mathcal{W}((q))}$ canonically extends to a proper flat curve $Tate'(q)_{/\mathcal{W}[[q]]}$ defined by the same equation. Removing singular locus of $Tate'(q)$ concentrated at $q = 0$, we get a flat group scheme $(Tate(q), \omega_\infty)_{/\mathcal{W}[[q]]}$, which is called the Tate curve. Its special fiber at $q = 0$ is isomorphic to $\mathbf{G}_{m/\mathcal{W}}$ as easily seen (by manipulation of the equation; see [GME] II.5); so, $Tate(q)_{/\mathcal{W}[[q]]}$ is no longer an elliptic curve, but, removing the fiber $\mathbf{G}_m$ at $q = 0$, $Tate(q)_{/\mathcal{W}((q))}$ is an elliptic curve. Writing the special fiber $\mathbf{G}_m$ at $q = 0$ as $\mathrm{Spec}(\mathcal{W}[t, t^{-1}])$ (so, t is the local parameter of $\mathbf{G}_m$ at the origin), we find $\omega_\infty = \frac{dt}{t}$. By evaluating $f \in G_k(1, \mathbf{1}, A)$ at $(Tate(q), \omega_\infty)_{/\mathcal{W}((q))}$, we get the q–expansion $f(q) = f(Tate(q), \omega_\infty) \in \mathcal{W}((q))$. Since $G_k(1, \mathbf{1}, A)$ is made up of isobaric polynomials of g_2 and g_3 of weight k, the expansion coincides with the analytic Fourier expansion by substituting $\exp(2\pi iz)$ for q if A is embedded into $\mathbb{C}$, and the q–expansion $f(q)$ actually falls in $A[[q]]$. If it falls further in $qA[[q]]$, we call f a cusp form. We write $S_k(1, \mathbf{1}, A)$ for the subspace of cusp forms.

Now let N be a positive integer prime to p. We introduce a level N structure. Consider the functors

$$\begin{array}{rcl} \wp_N : \mathcal{W}-Schemes & \longrightarrow & Sets \\ S & \mapsto & [(E, \varphi_{\Gamma(N)} : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N], \omega)_{/S}], \\ \wp_{\Gamma_1(N)} : \mathcal{W}-Schemes & \longrightarrow & Sets, \\ S & \mapsto & [(E, \varphi_{\Gamma_1(N)} : \mathbb{Z}/N\mathbb{Z} \hookrightarrow E[N], \omega)_{/S}], \text{and}, \\ \wp_{\Gamma_0(N)} : \mathcal{W}-Schemes & \longrightarrow & Sets \\ S & \mapsto & [(E, C, \omega)_{/S}], \end{array}$$

where $[\quad] = \{\quad\}/\cong$ denotes isomorphims class and C is a subgroup scheme of $E[N]$ defined over S, cyclic of order N (that is, $C \cong \mathbb{Z}/N\mathbb{Z}$ after changing basis to a finite étale extension of S). We often use the symbol: $\phi_{\Gamma_0(N)}$ to indicate the level structure "C" of $\Gamma_0(N)$–type (to make our notation consistent with the other level structures of $\Gamma_1(N)$ and $\Gamma(N)$ type).

These functors are representable by the schemes $\mathcal{M}_N = \mathcal{M}_{\Gamma(N)} = \mathrm{Spec}(\mathcal{A}_N)$, respectively $\mathcal{M}_{\Gamma_1(N)} = \mathrm{Spec}(\mathcal{A}_N^{\Gamma_1(N)})$, $\mathcal{M}_{\Gamma_0(N)} = \mathrm{Spec}(\mathcal{A}_N^{\Gamma_0(N)})$. Here the superscript "$\Gamma$" of $\mathcal{A}_N^{\Gamma}$ indicates symbolically the subring fixed by the modular group Γ. Define the 'bars' of these algebras by the integral closure of $\overline{\mathcal{A}}$ in each algebra, and put $M_\Gamma = \mathrm{Spec}(\mathcal{A}_{N,0})$ and $\overline{M}_\Gamma = \mathrm{Proj}(\overline{\mathcal{A}}_N^{\Gamma})$ for $\Gamma = \Gamma_0(N)$ and $\Gamma_1(N)$. Then $\overline{M}_\Gamma - M_\Gamma$ is the set of cusps of $\overline{M}_\Gamma$.

Now let Q be a finite set of primes as in Section 5.1. Recall that $N_Q = \prod_{q \in Q} q$. To simplify the notation, we write $\mathcal{M}_Q^?$ and $\mathcal{A}_Q^?$, etc. for $\mathcal{M}_{\Gamma_?(N_Q)}$ and $\mathcal{A}_{N_Q}^{\Gamma_?(N_Q)}$ in this section. Note that $\mathcal{M}_Q^1 \to \mathcal{M}_Q^0$ is étale, and moreover that

$$\overline{M}_Q^1 = \mathrm{Proj}(\overline{\mathcal{A}}_Q^1) \to \mathrm{Proj}(\overline{\mathcal{A}}_Q^0) = \overline{M}_Q^0$$

is an étale Galois covering with Galois group $(\mathbb{Z}/N_Q\mathbb{Z})^\times$, the Galois action of $a \in (\mathbb{Z}/N_Q\mathbb{Z})^\times$ being given by $(E, \phi_N^1, \omega) \mapsto (E, \phi_N^1 \circ a, \omega)$. We remark that étaleness at cusps holds because N_Q is square free. This can be easily checked by using the fact that the monodromy group at infinity is given by upper unipotent subgroup of $GL_2(\mathbb{Z}/N_Q\mathbb{Z})$ (and that Bruhat-Tits decomposition holds for $GL_2(\mathbb{F}_q)$ for primes $q \in Q$). This shows that

$$H^0((\mathbb{Z}/N_Q\mathbb{Z})^\times, \overline{\mathcal{A}}_Q^1/p^n\overline{\mathcal{A}}_Q^1) = \overline{\mathcal{A}}_Q^0/p^n\overline{\mathcal{A}}_Q^0$$

for all $0 < n \in \mathbb{Z}$. We now make the following definition:

Definition 5.2. $G_k(\Gamma_?(N_Q), A) = \overline{\mathcal{A}}_{Q,k}^? \otimes_{\mathcal{W}} A = H^0(\overline{M}_Q^?, \underline{\omega}^k)$, where $\underline{\omega}^k$ is the invertible sheaf over $\overline{\mathcal{M}}_Q^?$ generated by degree k homogeneous elements in $\overline{\mathcal{A}}_Q^?$.

The subspace of cusp forms $S_k(\Gamma_?(N_Q), A)$ in $G_k(\Gamma_?(N_Q), A)$ is defined to be made up of modular forms f whose q–expansion $f(Tate(q), \phi_N^?, \omega_\infty)$ is without constant term for any choice of $\phi_N^?$. This definition is again consistent with the earlier one. Note that we have written here $S_k(\Gamma_0(N_Q), A)$ for $S_k(N_Q, \mathbf{1}, A)$ defined in the previous section to emphasize two different level groups $\Gamma_1(N_Q)$ and $\Gamma_0(N_Q)$. Using our new notation, what we have shown is:

$$H^0((\mathbb{Z}/N_Q\mathbb{Z})^\times, G_k(\Gamma_1(N_Q), A)) = G_k(\Gamma_0(N_Q), A),$$
$$H^0((\mathbb{Z}/N_Q\mathbb{Z})^\times, S_k(\Gamma_1(N_Q), A)) = S_k(\Gamma_0(N_Q), A)$$

A variant of this is that if $\xi : (\mathbb{Z}/N_Q\mathbb{Z})^\times \to A$ is a character then

$$S_k(\Gamma_1(N_Q), A)[\xi] = S_k(N_Q, \xi, A).$$

This follows by a similar argument applied to the sheaf $\underline{\omega}^k(\xi)$ obtained from $\underline{\omega}^k_{/\overline{\mathcal{M}}^1_Q}$ by twisting it by the character ξ of $\mathrm{Gal}(\overline{\mathcal{M}}^1_Q/\overline{\mathcal{M}}^0_Q)$. Applying this to $A = \mathcal{W}/p^n\mathcal{W}$ and taking injective limit with respect to n, we get

$$S_k(\Gamma_1(N_Q), \mathcal{W} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)[\xi] = S_k(\Gamma_0(N_Q), \xi, \mathcal{W}) \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p). \tag{5.2}$$

We now take $\mathcal{W}$ to be W to prove the horizontal control theorem on the Hecke side. Writing the q–expansion at ∞ of a cusp form f as $f(q) = \sum_{n=1}^\infty a(n, f)q^n$, it is easy to deduce from (3.1) that the pairing $(f, h) \mapsto a(1, f|h)$ induces a perfect Pontryagin duality between $h_k(\Gamma_1(N_Q), W)$ and $S_k(\Gamma_1(N_Q), W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$. Since $k \geq 3$, we know that the projector e induces an isomorphism of the Hecke algebra $h^{ord}_k(p, \Gamma_1(N_Q), \psi, W)$ onto $h^{ord}_k(\Gamma_1(N_Q), W)$ for $\psi = \mathbf{1}$. By duality, (5.2) may be rephrased as

$$h_k(\Gamma_1(N_Q), W)/\Sigma_{\sigma\in(\mathbb{Z}/N_Q\mathbb{Z})^\times}(\sigma - \xi(\sigma))h_k(\Gamma_1(N_Q), W) = h_k(N_Q, \xi, W). \tag{5.3}$$

Since T^ϕ_Q is local, the algebra homomorphism of $W[\Delta_Q]$ into T^ϕ_Q factors through its augmentation quotient; so, it induces the trivial character on Δ'_Q. Thus on T^ϕ_Q, what matters is only the action of Δ_Q; so, (5.3) yields

$$T^\phi_Q/\Sigma_{\sigma\in\Delta_Q}(\sigma - \xi(\sigma))T^\phi_Q \text{ is a local ring of } h^{ord}_k(N_Q, \xi, W) \tag{5.4}$$

Taking $\xi = \mathbf{1}$ and applying the fact that the local ring T^ϕ_Q of $h_k(N_Q, \mathbf{1}, W)$ with given eigenvalues $\overline{\alpha}_q$ of $\rho'_{T^\phi_Q}(\mathrm{Frob}_q)$ $(q \in Q)$ is isomorphic to T^ϕ in $h_k(1, \mathbf{1}, W)$, we conclude

$$T^\phi_Q/\Sigma_{\sigma\in\Delta_Q}(\sigma - 1)T^\phi_Q \cong T^\phi.$$

Since $W[\Delta_Q]$ is a local ring, by Nakayama's lemma, this shows that the minimal number of generators of T^ϕ_Q over $W[\Delta_Q]$ is $d = \mathrm{rank}_W T^\phi$; so, we have an $W[\Delta_Q]$–linear surjection $\pi : W[\Delta_Q]^d \to T^\phi_Q$. By tensoring

$$W = W[\Delta_Q]/\Sigma_{\sigma\in\Delta_Q}(\sigma - \xi(\sigma))W[\Delta_Q]$$

over $W[\Delta_q]$ with π, the linear map π induces a surjection

$$\pi_\xi : W^d \to T^\phi_Q/\Sigma_{\sigma\in\Delta_Q}(\sigma - \xi(\sigma))T^\phi_Q.$$

Since the right-hand-side is W–free by (5.4) with minimal number of generators d by Nakayama's lemma, it has to be W–free of rank d. Thus π_ξ is an isomorphism. Since $\mathrm{Ker}\,\pi \subset \bigcap_\xi \mathrm{Ker}\,\pi_\xi = 0$ regarding π_ξ as a linear map: $W[\Delta_Q]^d \to T^\phi_Q/\Sigma_{\sigma\in\Delta_Q}(\sigma - \xi(\sigma))T^\phi_Q$, we know that π is an isomorphism. This finishes the proof. □

6. Taylor-Wiles systems

In this section we introduce the commutative algebra machine invented by Taylor and Wiles [TW] (with simplifications due to Faltings, Diamond and Fujiwara) which allows one to deduce the equality of the Hecke algebra and universal deformation ring in Theorem 4.7. We prefer to work axiomatically and a bit more generally here (over arbitrary number fields rather than $\mathbb{Q}$); this section can in fact be read independently of the previous ones. Our treatment follows that of Fujiwara [Fu].

Fix an odd prime p. Let W be an extension of $\mathbb{Z}_p$. Let F be a number field, and let O_F denote the ring of integers of F.

Consider the set $\mathcal{Q}$ defined via

$$\mathcal{Q} = \{\mathfrak{q} \subset O_F \bigm| \mathfrak{q} \text{ prime}, \mathrm{N}\mathfrak{q} \equiv 1 \pmod{p}\}.$$

For each finite subset $Q \subset \mathcal{Q}$, let

- $\Delta_Q =$ the p-Sylow subgroup of $\prod_{\mathfrak{q}\in Q}(O_F/\mathfrak{q})^\times$,
- $W[\Delta_Q] =$ the corresponding group algebra over W, and,
- $\mathfrak{A}_Q$ the augmentation ideal of $W[\Delta_Q]$.

Definition 6.1 (Taylor-Wiles system)**.** For each $m = 1, 2, \ldots$, fix a finite subset $Q_m \subset \mathcal{Q}$. A Taylor-Wiles system is a local W-algebra R, and a collection of tuples (R_m, T_m, M_m), indexed by $m = 1, 2, \ldots$, where

- R_m is a local W-algebras, with a map $R_m \to R$,
- T_m is a local W-algebras, with a map $R_m \to T_m$,
- M_m is a T_m-module,

satisfying:

- R_m (so T_m) is a $W[\Delta_{Q_m}]$-algebra,
- $R_m/\mathfrak{A}_{Q_m}R_m \xrightarrow{\sim} R$,
- As a $W[\Delta_{Q_m}]$-module, M_m is free of finite rank d, which is independent of m.

Theorem 6.1 (Isomorphism Criterion)**.** *Let R, (R_m, T_m, M_m) be a Taylor-Wiles system. Assume that the following conditions hold:*

(TW1): If $\mathfrak{q} \in Q_m$ then $\mathrm{N}\mathfrak{q} \equiv 1 \pmod{p^m}$,
(TW2): $|Q_m|$ is independent of m, say this cardinality is r,
(TW3): R_m is generated by at most r elements as a W-algebra,
(TW4): Assume that the kernel of

$$R \to \mathrm{End}_W(M_m/\mathfrak{A}_{Q_m}M_m)$$

is independent of m, and let $T = R/$kernel.

Then R is a complete intersection, free of finite rank over W. Moreover, the natural map

$$R \twoheadrightarrow T,$$

is an isomorphism.

Proof. Fix m. For each $\mathfrak{q} \in Q_m$, let $\Delta_\mathfrak{q}$, be the p-Sylow subgroup of $(O_F/\mathfrak{q})^\times$. By (TW1) we know that this is cyclic of order at least p^m. Let $\delta_\mathfrak{q}$ be a generator of $\Delta_\mathfrak{q}$. Suppose that $1 \le n \le m$. Note that $\Delta_\mathfrak{q}/ < \delta_\mathfrak{q}^{p^n} >$ is cyclic of order p^n. Thus,

$$\frac{W[\Delta_\mathfrak{q}]}{(\delta_\mathfrak{q}^{p^n} - 1)} \xrightarrow{\sim} \frac{W[[S]]}{(1+S)^{p^n} - 1},$$

via $\delta_{\mathfrak{q}} \mapsto 1 + S$.

By (TW2) we know that the cardinality of Q_m is r (and this number is independent of m). Suppose that $Q_m = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$. Let $I_n \subset W[\Delta_{Q_m}]$ be the ideal generated by $p^n, \delta_{\mathfrak{q}_1}^{p^n} - 1, \ldots, \delta_{\mathfrak{q}_r}^{p^n} - 1$. Then we have

$$\frac{W[\Delta_{Q_m}]}{I_n} \xrightarrow{\sim} \frac{W[[S_1, \ldots, S_r]]}{(p^n, (1+S_1)^{p^n} - 1, \ldots, (1+S_r)^{p^n} - 1)},$$

via $\delta_{\mathfrak{q}_i} \mapsto 1 + S_i$, for $i = 1, \ldots, r$.

Let us set $A_n = W[\Delta_{Q_m}]/I_n$. It is an easy computation to check that $|A_n| = p^{ntp^{nr}}$, where $t = \operatorname{rank}_{\mathbb{Z}_p}(W)$. In particular the cardinality of A_n is independent of m. Now define

$$\begin{aligned} R_{n,m} &= \operatorname{image}\left(\frac{R_m}{I_n R_m} \to \operatorname{End}_{A_n}\left(\frac{M_m}{I_n M_m}\right)\right), \\ \widetilde{R}_{n,m} &= \frac{R_{n,m}}{\mathfrak{A}_{Q_m}}. \end{aligned}$$

Since M_m is free over $W[\Delta_{Q_m}]$ of rank d (independent of m) there are natural maps

$$A_n \xrightarrow{\alpha} R_{n,m} \overset{\beta}{\hookrightarrow} \operatorname{End}_{A_n}\left(\frac{M_m}{I_n M_m}\right) = M_d(A_n).$$

Since β is injective we see that $|R_{n,m}| \leq |A_n|^{d^2}$ is bounded independently of m. Also $\beta \circ \alpha$ is injective, so that α is injective as well. This will be used below.

By (TW3), R_m is generated by r elements over W, and thus, so is $R_{n,m}$. Pick generators $f_1, \ldots, f_r$ of $R_{n,m}$.

Now fix n, and suppose $m, m' \geq n$. We say two triples

$$\Big((R_{n,m}, \alpha, \beta), \widetilde{R}_{n,m}, (f_1, \ldots, f_r)\Big) \text{ and } \Big((R_{n,m'}, \alpha', \beta'), \widetilde{R}_{n,m'}, (f'_1, \ldots, f'_r)\Big)$$

are isomorphic if there is an isomorphism of A_n-algebras

$$\iota : R_{n,m} \xrightarrow{\sim} R_{n,m'}$$

inducing

$$\iota : \widetilde{R}_{n,m} \xrightarrow{\sim} \widetilde{R}_{n,m'},$$

such that $\iota(f_j) = f'_j$ and such that the following two diagrams commute:

$$\begin{tikzcd} A_n \arrow[r, "\alpha"] \arrow[d, equal] & R_{n,m} \arrow[r, hook, "\beta"] \arrow[d, "\iota"] & M_d(A_n) \arrow[d, equal] \\ A_n \arrow[r, "\alpha"] & R_{n,m'} \arrow[r, hook, "\beta'"] & M_d(A_n) \end{tikzcd}$$

and

$$\begin{tikzcd} R_{n,m} \arrow[r] \arrow[d, "\iota"] & \widetilde{R}_{n,m} \arrow[d, "\iota"] \\ R_{n,m'} \arrow[r] & \widetilde{R}_{n,m'}. \end{tikzcd}$$

Since the cardinality of $R_{n,m}$ is bounded independently of m, we see that for $n = 1$, there exists infinitely $m \geq 1$ (call this set $\mathbb{N}_1 \subset \mathbb{N}$) such that the

$$\Big((R_{1,m}, \alpha, \beta), \widetilde{R}_{1,m}, (f_1, \ldots, f_r)\Big),$$

are mutually isomorphic.

Suppose, for purposes of induction, that we have constructed $\mathbb{N}_n \subset \mathbb{N}_{n-1} \subset \cdots \subset \mathbb{N}_1 \subset \mathbb{N}$ such that

$$\left((R_{n,m}, \alpha, \beta), \widetilde{R}_{n,m}, (f_1, \ldots, f_r)\right),$$

are mutually isomorphic for all $n \in \mathbb{N}_n$. Then, again, by varying $m \geq n+1$ in $\mathbb{N}_n$ we may pick an infinite subset $\mathbb{N}_{n+1} \subset \mathbb{N}_n$, such that

$$\left((R_{n+1,m}, \alpha, \beta), \widetilde{R}_{n+1,m}, (f_1^{(n)}, \ldots, f_r^{(n)})\right),$$

are mutually isomorphic for $m \in \mathbb{N}_{n+1}$.

Now, for each n, let $m(n)$ denote the minimal element in $\mathbb{N}_n$, and let the corresponding triple be

$$\left((R_{n,m(n)}, \alpha, \beta), \widetilde{R}_{n,m(n)}, (f_1, \ldots, f_r)\right).$$

Note that the following diagram commutes:

$$\begin{tikzcd}
\frac{R_{m(n+1)}}{I_{n+1}R_m(n+1)} \arrow[r] \arrow[d, "\bmod I_n"] & \mathrm{End}_{A_{n+1}}\left(\frac{M_{m(n+1)}}{I_{n+1}M_{m(n+1)}}\right) \arrow[d] \\
\frac{R_{m(n+1)}}{I_nR_m(n+1)} \arrow[r] & \mathrm{End}_{A_n}\left(\frac{M_{m(n+1)}}{I_nM_{m(n+1)}}\right).
\end{tikzcd}$$

Moreover $R_{n,m(n+1)}$ (and its tuple) is isomorphic to $R_{n,m(n)}$ (and its tuple) since both $m(n+1)$ and $m(n) \in \mathbb{N}_n$. This shows that the process of going modulo I_n yields a projective system of tuples

$$\left((R_{n,m(n)}, \alpha, \beta), \widetilde{R}_{n,m(n)}, (f_1^{(n)}, \ldots, f_r^{(n)})\right),$$

as n varies. Denote the projective limit by

$$\left((R_\infty, \alpha_\infty, \beta_\infty), \widetilde{R}_\infty, (f_1^{(\infty)}, \ldots, f_r^{(\infty)})\right).$$

Let us now set

$$A := \varprojlim A_n = W[[S_1, \ldots S_r]], \text{ and } B := W[[T_1, \ldots T_r]].$$

By the injectivity of the α and β at each level, we have maps

$$A \overset{\alpha_\infty}{\hookrightarrow} R_\infty \overset{\beta_\infty}{\hookrightarrow} M_d(A). \tag{6.1}$$

Also we have a map

$$\begin{array}{ccc} B & \twoheadrightarrow & R_\infty \\ T_i & \mapsto & f_i^{(\infty)}. \end{array} \tag{6.2}$$

The maps (6.1) show that R_∞ is a torsion free A-module of finite type, and so by the going-up and going-down theorems, the Krull dimension of R_∞ is given by $\dim(R_\infty) = r+1$. This shows that the map (6.2) must be injective. For if it were not, we could always choose some $0 \neq f$ in its kernel K, and a height 1 prime P of B containing f, and we would get the absurdity:

$$r+1 = \dim R_\infty = \dim B/K \leq \dim B/(f) = \dim B/P = r.$$

This shows that R_∞ is isomorphic to the power series ring $B = W[[T_1, \ldots T_r]]$.

We now claim that $\widetilde{R}_\infty$ is a complete intersection, free of finite rank over W. To see this note that we have an exact sequence

$$\begin{array}{ccc} R_\infty^r & \longrightarrow & R_\infty \longrightarrow \widetilde{R}_\infty \\ (x_i) & \mapsto & \sum S_i x_i \end{array}$$

This shows that $\widetilde{R}_\infty$ is the homomorphic image of a power series ring over W in r variables, with kernel generated by r elements, i.e. that $\widetilde{R}_\infty$ is a complete intersection. The fact that $\widetilde{R}_\infty$ is free of finite rank over W follows from the following lemma:

Lemma 6.2. *Let $A \hookrightarrow B$ be power series rings over W in the same number of variables. Assume that as an A-module B is of finite type. Then B is A-free.*

Indeed, in our situation, since $A \hookrightarrow B \hookrightarrow M_d(A)$, B is indeed an A-module of finite type. Thus R_∞ is A-free (of finite rank), and so $\widetilde{R}_\infty$ is W-free (of the same rank). This proves the claim.

We now claim that $\widetilde{R}_\infty = T$. For this we need one more general lemma, (which follows the Auslander-Buchsbaum formula):

Lemma 6.3. *Say $A \hookrightarrow B$ are power series rings over W in the same number of variables. Say L is a B-module. Then L is A-free $\iff$ L is B-free.*

Let $L = \lim_{\leftarrow n} M_{m(n)}/I_n M_{m(n)} = \lim_{\leftarrow n} A_n^d = A^d$. By Lemma 6.3 L is a free B-module (of finite rank), and so consequently $L/I_n L = M_{m(n)}/I_n M_{m(n)}$ is $R_\infty/I_n R_\infty = R_{n,m(n)}$-free. Now note that generally, for a C-module X, which is free of finite rank, and an idea $\mathfrak{A} \subset C$, $C/\mathfrak{A}$ acts *faithfully* on $X/\mathfrak{A}X$, and so we may consider $C/\mathfrak{A} \subset \mathrm{End}(X/\mathfrak{A}X)$. Applying this to our situation we see

$$\widetilde{R}_{n,m(n)} \subset \mathrm{End}_W \left(M_{m(n)}/(I_n + \mathfrak{A}_{Q_{m(n)}}) M_{m(n)} \right).$$

Now note that the following diagram is commutative (see (TW4)):

$$\begin{tikzcd}
R_{m(n)} \arrow[r, two heads] \arrow[d, equal] & R_{n,m(n)} \arrow[r, two heads] & \widetilde{R}_{n,m(n)} \arrow[r, phantom, "\subset"] & \mathrm{End}_W \left(M_{m(n)}/(I_n + \mathfrak{A}_{Q_{m(n)}}) M_{m(n)} \right) \\
R_{m(n)} \arrow[r, two heads] & T \arrow[rr, phantom, "\subset"] & & \mathrm{End}_W \left(M_{m(n)}/\mathfrak{A}_{Q_{m(n)}} M_{m(n)} \right) \arrow[u]
\end{tikzcd}$$

Letting $n \to \infty$, we see that the map $R_\infty \twoheadrightarrow \widetilde{R}_\infty$ factors through T:

$$R_\infty \twoheadrightarrow T \twoheadrightarrow \widetilde{R}_\infty. \tag{6.3}$$

On the other hand we see that under the map $R_\infty \twoheadrightarrow T$, the ideal $(S_1, \dots, S_r)$ maps to 0, so that we have a map from $\widetilde{R}_\infty = R_\infty/(S_1, \dots, S_r) \twoheadrightarrow T$. Along with (6.3) this says that $\widetilde{R}_\infty \xrightarrow{\sim} T$.

We now claim that in fact $R \xrightarrow{\sim} T$. Let

$$K_n = \ker(R_\infty \twoheadrightarrow R_{n,m(n)}),$$

and $\mathfrak{m}_\infty$ the maximal ideal of R_∞. Then for each $N > 0$, there exists $n(N) >> 0$, such that $K_{n(N)} \subset \mathfrak{m}_\infty^N$. Consider the following commutative diagram with exact rows:

$$\begin{tikzcd}
R^r_{m(n(N))} \arrow[r] \arrow[d] & R_{m(n(N))} \arrow[r] \arrow[d] & R \arrow[r] \arrow[d] & 0 \\
R^r_{n(N),m(n(N))} \arrow[r] & R_{n(N),m(n(N))} \arrow[r] & \widetilde{R}_{n(N),m(n(N))} \arrow[r] \arrow[d, equal] & 0 \\
& & T/p^{n(N)}T &
\end{tikzcd}$$

Tensoring this with $R_\infty/\mathfrak{m}_\infty^N$ (over R_∞) we get another commutative diagram with exact rows:

$$\begin{tikzcd}
(R^r_{m(n(N))}/\mathfrak{m}_\infty^N)^r \arrow[r] \arrow[d] & R_{m(n(N))}/\mathfrak{m}_\infty^N \arrow[r] \arrow[d] & R/\mathfrak{m}_\infty^N \arrow[r] \arrow[d] & 0 \\
(R^r_{n(N),m(n(N))}/\mathfrak{m}_\infty^N)^r \arrow[r] & R_{n(N),m(n(N))}/\mathfrak{m}_\infty^N \arrow[r] & T/\mathfrak{m}_T^N \arrow[r] & 0,
\end{tikzcd}$$

where $\mathfrak{m}_T$ is the maximal ideal of T. By our choice of $n(N)$ the first two vertical maps are isomorphisms, so that

$$R/\mathfrak{m}_R^N \xrightarrow{\sim} T/\mathfrak{m}_T^N,$$

for all $N > 0$. Taking limits, we see that $R \xrightarrow{\sim} T$, and this finishes the proof of the Theorem 6.1. □

Theorem 6.4 (Freeness Criterion)**.** *Let the hypothesis and assumptions be as in Theorem 6.1. Assume in addition that*

(TW5): There is an R-module M, such that $M_m/\mathfrak{A}_{Q_m}M_m \cong M$, as R-modules for each $m = 1, 2, \ldots$.

Then M is a free T-module.

Proof. We have

$$M = \varprojlim M/p^nM = \varprojlim_n M_{m(n)}/(I_n + \mathfrak{A}_{Q_{m(n)}})M_{m(n)} = L/(S_1, \ldots S_r)L.$$

But L is a free R_∞-module (of finite rank) and $\widetilde{R}_\infty = R_\infty/(S_1, \ldots S_r)R_\infty = T$. So M is a free T-module (of finite rank). □

7. Proof of Theorem 4.7

We use the isomorphism criterion of Theorem 6.1 to give a proof of Theorem 4.7.

In our proof, the Galois cohomological argument is a version of the argument of Wiles in [W1] Chapters 1 and 3. In [TW], this type of argument is applied to the Taylor-Wiles system obtained from the topological cohomology groups $M_Q = H^1(X_1(pN_Q), \mathbb{Z}_p)$; so, a new aspect of the proof here is the use of the Hecke algebra T_Q^ϕ in place of the cohomology groups.

We refer the reader to [MFG] 3.2.7-8 for further details of the argument and to [MFG] 4 for the Tate duality theorem, Poitou-Tate exact sequence, local and global Euler characteristic formulas etc. that we use below.

Let $F = \mathbb{Q}$. Let $p \geq 5$ and $W/\mathbb{Z}_p$ be as in previous sections. Let

$$\mathcal{Q}_m = \{q \in \mathcal{Q} \mid q \equiv 1 \pmod{p^m} \text{ and } \overline{\rho}_\lambda(\mathrm{Frob}_q) \text{ has distinct eigenvalues}\}.$$

It is a fact (shown by Wiles) that under the condition $(ai_\kappa))$, there are infinitely many primes in $\mathcal{Q}_m$.

We now show that there exist sets $Q_m \subset \mathcal{Q}_m$ for $m = 1, 2, 3, \ldots$, satisfying (TW1), (TW2) and (TW3), such that, if, in the notation of Sections 4.4 and 5,

$$R := R^{ord,\phi},\ \ R_m := R^{ord,\phi}_{Q_m} \text{ and } T_m := M_m := T^{\phi}_{Q_m},$$

with $\phi = \nu^{k-1}$, then, $\{R,\ (R_m, T_m, M_m)_{m\in\mathbb{N}}\}$ is a Taylor-Wiles system in the sense of Definition 6.1. In fact many of the requirements of the definition have already been checked (see in particular Proposition 5.2 and Theorem 5.3). Indeed Theorem 5.3 shows that (TW5), and therefore (TW4), holds.

As a result we will get, by Theorem 6.1, that:

$$R^{ord,\phi} \xrightarrow{\sim} T^{\phi}$$

which is the desired conclusion of Theorem 4.7.

Fix m, and fix a finite set $Q \subset \mathcal{Q}_m$ of arbitrary cardinality. Denote by $\mathbb{Q}^{Q\cup\{p\}}$ the maximal extension of $\mathbb{Q}$ unramified outside p, ∞ and the primes in Q. Let $\mathfrak{G}_Q = \mathrm{Gal}(\mathbb{Q}^{Q\cup p}/\mathbb{Q})$. Let $Ad = Ad(\overline{\rho}_\lambda)$ be the three dimensional $\mathfrak{G}_Q$-module over $\mathbb{F}$, arising from the adjoint representation on the 2 by 2 matrices over $\mathbb{F}$ of trace 0.

For each $q \in Q \cup \{p\}$, let B_q be an $\mathbb{F}$-subspace of $H^1(D_q, Ad)$. We define the *Selmer group* attached to the data

- the $\mathfrak{G}_Q$-module Ad, and,
- the local conditions B_q, for $q \in Q \cup \{p\}$,

as follows. Set

$$\mathrm{Sel}_Q(Ad) := \beta_Q^{-1}\left(\prod_{q\in Q\cup\{p\}} B_q\right),$$

where β_Q is the natural restriction map:

$$\beta_Q : H^1(\mathfrak{G}_Q, Ad) \longrightarrow \prod_{q\in Q\cup\{p\}} H^1(D_q, Ad).$$

Eventually we will choose the following local conditions in the definition of the Selmer group. We will assume that

- $B_q = H^1(D_q, Ad)$, for each $q \in Q$, and,
- B_p is given by
$$B_p = \ker\left(H^1(D_p, Ad) \to H^1(I_p, Ad/Ad_0)\right),$$
where Ad_0 is the sub-representation of Ad consisting of matrices of the form $\left(\begin{smallmatrix} 0 & * \\ 0 & 0 \end{smallmatrix}\right)$.

This is because of the following lemma.

Lemma 7.1. *Let R_Q denote the universal deformation ring (with fixed determinant) as above. Let $t_Q = \mathfrak{m}_{R_Q}/\mathfrak{m}^2_{R_Q} + \mathfrak{m}_W$ be the cotangent space of R_Q. Then with the choice of local conditions B_q as above, we have*

$$\mathrm{Hom}_{\mathbb{F}}(t_Q, \mathbb{F}) \xrightarrow{\sim} \mathrm{Sel}_Q(Ad),$$

and the number of generators of R_Q as a W-algebra is equal to $\dim \mathrm{Sel}_Q(Ad)$.

This is a standard formula for the tangent space of a universal deformation ring. One can find a proof of this fact and related topics in [MFG] 2.3.4, 3.2.4 and 5.2.4.

Now let us consider the Selmer group attached to the dual representation of Ad. Set $Ad^* = \mathrm{Hom}_{\mathbb{F}}(Ad, \mathbb{F})$ and set $Ad^*(1) = Ad^* \otimes_{\mathbb{F}} \mu_p$. (In our case since

$Ad \subset M_2(\mathbb{F})$, the non-degenerate pairing $(X, Y) \mapsto \mathrm{Tr}(XY)$ shows that $Ad^* \xrightarrow{\sim} Ad$. Thus we have $Ad^*(1) \xrightarrow{\sim} Ad(1)$).

Theorem 7.2 (Local Tate duality)**.** *For $r = 0, 1, 2$, there is a natural duality between $H^{2-r}(D_q, Ad)$ and $H^r(D_q, Ad^*(1)) = H^r(D_q, Ad(1))$.*

For an arbitrary subspace $B_q \subset H^1(D_q, Ad)$, with $q \in Q \cup \{p\}$, let $B_q^\perp \subset H^1(D_q, Ad^*(1))$ denote the orthogonal compliment of B_q under the pairing of Theorem 7.2. Define the Selmer group $\mathrm{Sel}_Q(Ad^*(1))$ with respect to the subspaces $B_q^\perp$ as follows. For the restriction map

$$\beta_Q^* : H^1(\mathfrak{G}_Q, Ad^*(1)) \longrightarrow \prod_{q \in Q \cup \{p\}} H^1(D_q, Ad^*(1)),$$

$$\mathrm{Sel}_Q(Ad^*(1)) := {\beta_Q^*}^{-1} \left(\prod_{q \in Q \cup \{p\}} B_q^\perp \right).$$

Note that for the eventual choice of B_q that we have mentioned above, we have $B_q^\perp = 0$ for $q \in Q$.

Theorem 7.3 (Poitou-Tate exact sequence)**.** *Let B_q be arbitrary subspaces of $H^1(D_q, Ad)$, for $q \in Q \cup \{p\}$. Then, there is an exact sequence*

$$\begin{aligned} 0 \to \mathrm{Sel}_Q(Ad) \to H^1(\mathfrak{G}_Q, Ad) \to \prod_{q \in Q \cup \{p\}} \frac{H^1(D_q, Ad)}{B_q} \to \mathrm{Sel}_Q(Ad^*(1)) \\ \to H^2(\mathfrak{G}_Q, Ad) \to \prod_{q \in Q \cup \{p\}} H^2(D_q, Ad) \to H^0(\mathfrak{G}_Q, Ad^*(1))^* \to 0. \end{aligned}$$

Note that the condition (ai_κ)) holds $\iff$ Ad is an absolutely irreducible $\mathfrak{G}_Q$-module. Consequently

$$H^0(\mathfrak{G}_Q, Ad) = 0 = H^0(\mathfrak{G}_Q, Ad^*(1))^*. \tag{7.1}$$

We need another formula:

Theorem 7.4 (Global Euler characteristic formula)**.**

$$\begin{aligned} \dim H^0(\mathfrak{G}_Q, Ad) - \dim H^1(\mathfrak{G}_Q, Ad) + \dim H^2(\mathfrak{G}_Q, Ad) \\ = \dim H^0(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), Ad) - \dim Ad. \end{aligned}$$

Let c denote complex conjugation. Since $\det \overline{\rho}_\lambda(c) = -1$, we have $\overline{\rho}_\lambda(c) \sim \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, so that the eigenvalues of c on Ad are $-1, +1, -1$. This means that the value of the expression on the RHS of Theorem 7.4 is $= 1 - 3 = -2$.

Now let us assume that we have made the choice of the local conditions at $q \in Q \cup \{p\}$, as mentioned above. We set

$$d_Q = \dim \mathrm{Sel}_Q(Ad) - \dim \mathrm{Sel}_Q(Ad^*(1)).$$

By the Poitou-Tate exact sequence, the global Euler characteristic formula, local Tate duality, and (7.1), we have:

$$d_Q = h_p + 2 + \sum_{q \in Q} \dim H^0(D_q, Ad^*(1)), \tag{7.2}$$

where

$$h_p = \dim H^0(D_p, Ad^*(1)) - \dim \frac{H^1(D_p, Ad)}{B_p}$$

depends only on p. We now impose an additional condition:

(Sel) Assume that $\phi = \nu^{k-1}$ with $k \not\equiv 2 \pmod{p-1}$.

Proposition 7.5. *Recall that $Q \subset \mathcal{Q}_m$. Assume that (Sel) holds. We have*

(1) $h_p + 2 \leq 0$,
(2) $\dim H^0(D_q, Ad^*(1)) = 1$, *for all $q \in Q$.*

Proof. Since the cohomological dimension of D_p is 2, the exact sequence

$$0 \to Ad_0 \to Ad \to Ad/Ad_0 \to 0,$$

yields the following long exact sequence in cohomology:

$$\begin{aligned} 0 \to \mathrm{image}(u) \to H^1(D_p, Ad/Ad_0) \to H^2(D_p, Ad_0) \\ \to H^2(D_p, Ad) \to H^2(D_p, Ad/Ad_0) \to 0 \end{aligned}$$

where u is the map defined by

$$u : H^1(D_p, Ad) \to H^1(D_p, Ad/Ad_0).$$

Thus we have,

$\dim \mathrm{image}(u) =$

$$\dim H^1(D_p, \frac{Ad}{Ad_0}) - \dim H^2(D_p, Ad_0) + \dim H^2(D_p, Ad) - \dim H^2(D_p, \frac{Ad}{Ad_0}).$$

Now consider the following commutative diagram

$$\begin{tikzcd} & & H^1(D_p, Ad) \arrow[d, "u"] \arrow[dr, "\delta"] & & \\ 0 \arrow[r] & H^1(D_p/I_p, \frac{Ad}{Ad_0})^{I_p} \arrow[r] & H^1(D_p, \frac{Ad}{Ad_0}) \arrow[r] & H^1(I_p, \frac{Ad}{Ad_0})^{D_p} \arrow[r] & 0, \end{tikzcd}$$

where the bottom row comes from the inflation-restriction sequence, and the map δ is defined by the triangle above. Note that by the definition of the Selmer group,

$$h_p = \dim H^0(D_p, Ad^*(1)) - \dim \mathrm{image}(\delta).$$

In any case we see that

$$\dim \mathrm{image}(\delta) \geq \dim \mathrm{image}(u) - \dim H^1(D_p/I_p, Ad/Ad_0)^{I_p}.$$

But

$$H^1(D_p/I_p, Ad/Ad_0)^{I_p} \xrightarrow{\sim} (Ad/Ad_0)^{I_p}/(\mathrm{Frob}_p - 1)(Ad/Ad_0)^{I_p}.$$

Moreover there is an exact sequence

$$\begin{aligned} 0 \to H^0(D_p/I_p, Ad/Ad_0)^{I_p} \to (Ad/Ad_0)^{I_p} \xrightarrow{\mathrm{Frob}_p - 1} \\ (Ad/Ad_0)^{I_p} \to H^1(D_p/I_p, Ad/Ad_0)^{I_p} \to 0. \end{aligned}$$

This shows that

$$\dim H^1(D_p/I_p, Ad/Ad_0)^{I_p} = \dim H^0(D_p/I_p, Ad/Ad_0)^{I_p} = H^0(D_p, Ad/Ad_0).$$

Putting things together we get:

$$\begin{aligned} \dim \mathrm{image}(\delta) \geq \dim H^1(D_p, Ad/Ad_0) - \dim H^2(D_p, Ad_0) \\ + \dim H^2(D_p, Ad) - \dim H^2(D_p, Ad/Ad_0) - \dim H^0(D_p, Ad/Ad_0). \end{aligned}$$

Proposition 7.6 (Local Euler characteristic formula)**.**

$$\dim H^0(D_p, \frac{Ad}{Ad_0}) - \dim H^1(D_p, \frac{Ad}{Ad_0}) + \dim H^2(D_p, \frac{Ad}{Ad_0}) = \dim(\frac{Ad}{Ad_0}) = 2.$$

Consequently we have:

$$\begin{aligned} h_p &= \dim H^0(D_p, Ad^*(1)) - \dim \operatorname{image}(\delta) \\ &\leq \dim H^0(D_p, Ad^*(1)) - 2 + \dim H^2(D_p, Ad_0) - \dim H^2(D_p, Ad) \\ &= -2 + \dim H^0(D_p, Ad_0^*(1)), \end{aligned}$$

where the last equality follows by local Tate-duality (applied twice!)

We now claim that when (Sel) holds, $H^0(D_p, Ad_0^*(1)) = 0$. Note that part (1) of the proposition then follows immediately. To see this note that by (Sel) we may write

$$\overline{\rho}_{\lambda|I_p} = \begin{pmatrix} \psi & * \\ 0 & 1 \end{pmatrix},$$

where ψ is a non-trivial power of the Teichmüller character. Thus we see that $H^0(D_p, Ad_0^*(1)) = 0$.

As for part (2), note that $q \in Q \implies q \equiv 1 \pmod{p}$, so $Ad^*(1) = Ad(1) = Ad$. Consequently since the eigenvalues of Frob_q on Ad are $\bar{\alpha}_q/\bar{\beta}_q$, 1, and $\bar{\beta}_q/\bar{\alpha}_q$, we see that $\dim H^0(D_q, Ad^*(1)) = 1$ by (rg_q). □

Remark 7.1. *The condition* (Sel) *is not necessary in the sense that the Proposition also holds under other hypothesis.*

Corollary 7.7.

$$d_Q \leq |Q|.$$

Proof. This follows immediately from (7.2) and Proposition 7.5. □

Let

$$r := \dim \mathrm{Sel}_\emptyset(Ad^*(1))$$

be the dimension of the Selmer group when $Q = \emptyset$. Our next objective is to show that for each m, we may choose $Q \in \mathcal{Q}_m$ above such that $|Q| = r$, and so that $\mathrm{Sel}_Q(Ad^*(1)) = 0$. Lemma 7.1 and Corollary 7.7 will then show that these choices of Q will satisfy (TW1 - 3). Indeed, since $\mathrm{Sel}_Q(Ad^*(1)) = 0$, we see that $d_Q = \dim t_Q$, and so each R_Q will be generated by at most r elements as a W-algebra.

Proposition 7.8. *There are infinitely many sets* $Q \in \mathcal{Q}_m$ *such that*

(1) $|Q| = r = \dim \mathrm{Sel}_\emptyset(Ad^*(1))$*, and,*
(2) $\mathrm{Sel}_Q(Ad^*(1)) = 0$.

Proof. Let $Q \in \mathcal{Q}_m$ be arbitrary. Since $B_q^\perp = 0$ for all $q \in Q$, we have

$$\mathrm{Sel}_Q(Ad^*(1)) \subset \ker \beta_Q'$$

where

$$\beta_Q' : H^1(\mathfrak{G}_Q, Ad^*(1)) \longrightarrow \prod_{q \in Q} H^1(D_q, Ad^*(1))$$

is the map obtained from β_Q^* by ignoring the restriction at p. In fact one may check that $\ker \beta'_Q \subset \ker \beta_Q^\dagger$, where

$$\beta_Q^\dagger : H^1(\mathfrak{G}_\emptyset, Ad^*(1)) \longrightarrow \prod_{q \in Q} H^1(D_q, Ad^*(1))$$

We now show that when the cardinality of $|Q|$ is sufficiently large, $\beta_Q^\dagger$ is injective. This will force the vanishing of $\mathrm{Sel}_Q(Ad^*(1))$ when $|Q|$ is sufficiently large.

First let us introduce some notation. Let $\mathfrak{h}_Q = \mathrm{Gal}(\mathbb{Q}^{Q \cup p}/K(\mu_p)) \subset \mathfrak{G}_Q$. When $Q = \emptyset$, we write $\mathfrak{G}$ (respectively $\mathfrak{h}$) for $\mathfrak{G}_Q$ (respectively $\mathfrak{h}_Q$). Let K be the fixed field of $\ker \overline{\rho}_\lambda$, and let $G = \mathrm{Gal}(K(\mu_p)/\mathbb{Q})$.

It is a fact that

$$H^1(G, Ad(1)) = 0.$$

Consequently, the inflation-restriction sequence yields:

$$0 = H^1(G, Ad(1)) \to H^1(\mathfrak{G}, Ad(1)) \xrightarrow{\iota} H^1(\mathfrak{h}, Ad(1))^G = \mathrm{Hom}_G(\mathfrak{h}, Ad(1)).$$

Now fix $0 \neq x \in \ker \beta_Q^\dagger$, and let $f = f_x : \mathfrak{h} \to Ad(1)$ be the image of x under the map ι.

Since $\overline{\rho}_\lambda$ satisfies $(ai_\kappa))$, we see that $\overline{\rho}_\lambda$ is not induced from κ. Consequently the image of $\overline{\rho}_\lambda$ in $\mathrm{PGL}_2(\mathbb{F})$ has cardinality divisible by p or is isomorphic to one of the groups A_4, S_4 or A_5. A lemma of Wiles then shows that there is an element $\sigma \in \mathfrak{G}$ such that

(1) $\overline{\rho}_\lambda(\sigma)$ has order ℓ, where $\ell \geq 3$ is a prime different from p, and,
(2) σ fixes $\mathbb{Q}(\mu_{p^m})$ (so $\det \overline{\rho}_\lambda(\sigma) = 1$).

We claim that we may additionally assume that

(3) $f(\sigma^\ell) \neq 0$.

To see this, let L be the fixed field of the kernel of f. Then $X = \mathrm{Gal}(L/K(\mu_p))$ is an abelian extension of exponent p. We have the exact sequence

$$0 \to X \to \mathrm{Gal}(L/\mathbb{Q}) \to G \to 0.$$

Note that G acts on X via conjugation, and $f : X \to Ad(1) = Ad$ is an isomorphism of G modules (note that $f \neq 0$, f is injective, and Ad is irreducible, so f is surjective as well). Now let σ' satisfy the conditions (1) and (2) above. Then $\mathrm{Ad}(\overline{\rho}_\lambda)(\sigma')$ has three distinct eigenvalues on Ad and therefore on X, and one of them is equal to 1. Write

$$X = X[1] \oplus X',$$

where $X[1]$, $X' \neq 0$, $\sigma' = 1$ on $X[1]$ and $\sigma' - 1$ is an automorphism of X'. Since f is an isomorphism, we see that $f(X[1]) \neq 0$. Thus we may choose an element $\tau \in X[1]$ such that $f(\tau) \neq 0$.

Since $\mathrm{Gal}(K(\mu_{p^m})/K(\mu_p))$ is abelian on which $\mathrm{Im}(\overline{\rho})$ acts trivially by conjugation and on $\mathrm{Gal}(L/K)$, $\mathrm{Im}(\overline{\rho})$ acts by irreducible representation, we see that L and $K(\mu_{p^m})$ are linearly disjoint over $K(\mu_p)$. We now set

$$\tau' := 1 \times \tau \in \mathrm{Gal}(K(\mu_{p^m})/K(\mu_p)) \times \mathrm{Gal}(L/K(\mu_p)) = \mathrm{Gal}(L(\mu_{p^m})/K(\mu_p)).$$

Since $\tau \in X[1]$, τ' commutes with σ' in $\mathrm{Gal}(L(\mu_{p^m})/\mathbb{Q})$. Then, noting that ${\sigma'}^\ell \in X$, we have

$$f((\tau'\sigma')^\ell) = f({\tau'}^\ell {\sigma'}^\ell) = \ell f(\tau') + f({\sigma'}^\ell).$$

Since $\ell \neq p$, $\ell f(\tau') \neq 0$, and so one of $\tau'\sigma'$ or σ' satisfies (1), (2) and (3) above. This proves the claim.

Now choose a prime $q \notin Q$ such that $\mathrm{Frob}_q = \sigma$ in $\mathrm{Gal}(L(\mu_{p^m})/\mathbb{Q})$. Then the fact that $f(\mathrm{Frob}_q^{\ell}) \neq 0$ implies that $\beta_{Q\cup\{q\}}(x) \neq 0$. By (2) we see that $q \equiv 1 \bmod p^m$. Further (1) and (2) imply that the characteristic roots α and β of $\overline{\rho}_\lambda(\sigma)$ satisfy $\alpha\beta = 1$ and hence are primitive ℓ^{th} roots of unity. Since $\ell \geq 3$, we have $\alpha \neq \beta$. This shows that

$$Q \cup \{q\} \in \mathcal{Q}_m.$$

We have shown that for $0 \neq x \in \ker \beta_Q$, there is a prime $q \notin Q$, such that $Q \cup \{q\} \in \mathcal{Q}_m$, and $\beta_{Q\cup\{q\}}(x) \neq 0$. Iterating this statement, we may assume that $Q \in \mathcal{Q}_m$ is such that $\beta_Q^{\dagger}$ is injective.

Now, by the local Euler characteristic formula, $\dim H^1(D_q, Ad^*(1)) = 2$. So we may now remove primes from Q, one at a time, preserving the injectivity of $\beta_Q^{\dagger}$, at least until we reach $|Q| = r$. This finishes the proof of the proposition. □

Since we have proved Proposition 7.8 we have in fact completed the proof of Theorem 4.7 as well. □

References

Books

[BCM] N. Bourbaki, *Algèbre Commutative*, Hermann, Paris, 1961–83

[BCG] R. P. Langlands, *Base Change for $GL(2)$*, Annals of Math. Studies **96**, Princeton University Press, 1980

[CGP] K. S. Brown, *Cohomology of Groups*, Graduate texts in Math. **87**, Springer, 1982

[CPI] K. Iwasawa, *Collected Papers*, Vol. 1-2, Springer, 2001

[CRT] H. Matsumura, *Commutative Ring Theory*, Cambridge studies in advanced mathematics **8**, Cambridge Univ. Press, 1986

[FAN] D. Ramakrishnan and R. J. Valenza, *Fourier Analysis on Number Fields*, GTM **186**, 1999, Springer

[GME] H. Hida, *Geometric Modular Forms and Elliptic Curves*, 2000, World Scientific Publishing Co., Singapore (a list of errata downloadable at www.math.ucla.edu/~hida)

[HMI] H. Hida, *Hilbert Modular Forms and Iwasawa Theory*, forthcoming

[IAT] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press and Iwanami Shoten, 1971, Princeton-Tokyo

[ICF] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Text in Mathematics, **83**, Springer, 1980

[LFE] H. Hida, *Elementary Theory of L–functions and Eisenstein Series*, LMSST **26**, Cambridge University Press, Cambridge, 1993

[MFM] T. Miyake, *Modular Forms*, Springer, Berlin-Heiderberg-New York-Tokyo, 1989

[MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, 2000, Cambridge University Press

Articles

[BDGP] K. Barré-Sirieix, G. Diaz, F. Gramain and G. Philibert, Une preuve de la conjecture de Mahler-Manin, Inventiones Math **124** (1996), 1-9

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

[D] P. Deligne, Valeurs des fonctions L et périodes dintégrales, Proc. Symp. Pure Math. **33** (1979), part 2, 313–346

[Di] F. Diamond, On deformation rings and Hecke rings, Ann. of Math. **144** (1996), 137–166

[Di1] F. Diamond, The Taylor-Wiles construction and multiplicity one, Inventiones Math. **128** (1997), 379-391

[Fu] K. Fujiwara, Deformation rings and Hecke algebras in totally real case, preprint, 1996

[G] R. Greenberg, On the structure of certain Galois groups, Inventiones Math. **47** (1978), 85–99

[G1] R. Greenberg, Trivial zeros of p-adic L-functions, Contemporary Math. **165** (1994), 149–174

[GS] R. Greenberg and G. Stevens, p-adic L-functions and p-adic periods of modular forms, Inventiones Math. **111** (1993), 407–447

[H86a] H. Hida, Iwasawa modules attached to congruences of cusp forms, Ann. Sci. Ec. Norm. Sup. 4-th series **19** (1986), 231–273

[H86b] H. Hida, Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, Inventiones Math. **85** (1986), 545–613

[H88] H. Hida, Modules of congruence of Hecke algebras and L-functions associated with cusp forms, Amer. J. Math. **110** (1988) 323–382

[H90] H. Hida, p-adic L-functions for base change lifts of GL_2 to GL_3, in Proc. of Conference on "Automorphic forms, Shimura varieties, and L-functions", Perspectives in Math. **11** (1990), 93–142

[H96] H. Hida, On the search of genuine p-adic modular L-functions for $GL(n)$, Mémoire SMF **67**, 1996

[H98] H. Hida, Global quadratic units and Hecke algebras, Documenta Math. **3** (1998), 273–284

[H00] H. Hida, Adjoint Selmer groups as Iwasawa modules, Israel Journal of Math. **120** (2000), 361–427

[H04] H. Hida, Greenberg's $\mathcal{L}$-invariants of adjoint square Galois representations, 2004, (preprint downloadable at www.math.ucla.edu/~hida)

[HT] H. Hida and J. Tilouine, On the anticyclotomic main conjecture for CM fields, Inventiones Math. **117** (1994), 89–147

[Kh1] C. Khare, Serre's conjecture and its consequences. Jpn. J. Math. **5** (2010), 103–125.

[KhW] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture. I, II. I: Invent. Math. **178** (2009), 485–504; II. Invent. Math. **178** (2009), 505–586

[Ki] M. Kisin, Moduli of finite flat group schemes, and modularity, Annals of Math. **170** (2009), 1085–1180

[M] B. Mazur, Deforming Galois representations, MSRI Publications **16** (1989), 385–437

[MaW] B. Mazur and A. Wiles, On p–adic analytic families of Galois representations, Compositio Math. **59** (1986), 231–264

[S] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, Publ. IHES. **54** (1981), 323–401

[SW] C. Skinner and A. Wiles, Nearly ordinary deformations of irreducible residual representations, Ann. Fac. Sc. Toulouse Math. **10** (2001), 185–215

[T] R. Taylor, On Galois representations associated to Hilbert modular forms II, in Series in Number Thory **1** (1995): "Elliptic curves, Modular forms, & Fermat's last theorem", pp.185–191

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

[U] E. Urban, Selmer groups and the Eisenstein-Klingen ideal. Duke Math. J. **106** (2001), 485–525

[W] A. Wiles, The Iwasawa conjecture for totally real fields, Ann. of Math. **131** (1990), 493–540

[W1] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. **141** (1995), 443–551