

7.4 Wiles' Main Theorem and Isomorphism Criteria for Local Rings

7.4.1 Strategy of the proof of the Main Theorem 7.33

Let us consider again a local \mathcal{O} -algebra A with maximal ideal \mathfrak{m}_A , where $\mathcal{O} \supset \mathbb{Z}_p$ denotes (as in section 7.2) the ring of integers of a finite extension $K \supset \mathbb{Q}_p$; \mathcal{O} is a discrete valuation ring (DVR), and λ denotes the maximal ideal of \mathcal{O} . We always assume that

$$A/\mathfrak{m}_A \cong \mathcal{O}/\lambda = k \supset \mathbb{F}_p,$$

and we fix a two-dimensional representation $\rho_0 : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(k)$ over the finite field k , together with sets S and Σ as described above.

Recall that Ribet's modular Galois representation

$$\tilde{\rho} = \rho_{f,\lambda} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathcal{O})$$

of minimal level N_0 given by Theorem 7.30 belongs to the (non-empty) set $DM_{\emptyset}(\mathcal{O})$. This gives a distinguished element of each of the sets $DM_{\Sigma}(A) \subset DA_{\Sigma}(A)$. This representation $\tilde{\rho}$ is used in an explicit construction of the modular universal deformation ring \mathbb{T}_{Σ} , see [CSS95].

Surjectivity of the map $\varphi_{\Sigma} : R_{\Sigma} \rightarrow \mathbb{T}_{\Sigma}$ (7.3.2) can be easily deduced from the fact (see 7.32) that the universal deformation rings R_{Σ} and \mathbb{T}_{Σ} are topologically generated by the elements $\mathrm{tr}(\rho_{\Sigma}^{univ}(\mathrm{Frob}_l)) \in R_{\Sigma}$ for primes $l \notin \Sigma_S$, see below §7.4.2.

Injectivity of $\varphi_{\Sigma} : R_{\Sigma} \rightarrow \mathbb{T}_{\Sigma}$ was proved by A.Wiles by an induction argument on Σ . For a prime l not in Σ_S , we let $\Sigma' = \Sigma \cup \{l\}$. Wiles deduced the bijectivity of $\varphi_{\Sigma'}$ from the bijectivity of φ_{Σ} using an isomorphism criterion for local rings. This criterion was formulated in terms of certain invariants (discovered by Wiles earlier, in spring 1991, see the introduction of his paper [Wi]). However, in order to start the induction one needed the case $\Sigma = \emptyset$ (the base of induction). This was the point which caused a problem in 1993, after the announcement of a complete proof of FLT, and which was repaired in 1994 by A.Wiles and R.Taylor using a horizontal version of Iwasawa theory together with a second isomorphism criterion for local rings. In this section we describe these criteria and give explicit constructions (due to H.Lenstra and B.Mazur) of the universal deformation ring R_{Σ} .

7.4.2 Surjectivity of φ_{Σ}

In order to prove the surjectivity, we assume the existence of the universal deformation rings $R_{\Sigma}, \mathbb{T}_{\Sigma} \in \mathcal{C}_{\mathcal{O}}$. Thus for any $A \in \mathcal{C}_{\mathcal{O}}$ we have

$$DA_{\Sigma}(A) = \mathrm{Hom}_{\mathcal{C}_{\mathcal{O}}}(R_{\Sigma}, A) \supset DM_{\Sigma}(A) = \mathrm{Hom}_{\mathcal{C}_{\mathcal{O}}}(\mathbb{T}_{\Sigma}, A),$$

implying the existence of a canonical morphism (7.3.2)

$$\varphi_\Sigma : R_\Sigma \rightarrow \mathbb{T}_\Sigma.$$

Lemma 7.34. *Let $A = R_\Sigma$ (resp. $A = \mathbb{T}_\Sigma$), and denote by A^0 subring of A which is the topological closure of the \mathcal{O} -subalgebra in A generated by all elements $\mathrm{tr}(\rho_\Sigma^{\mathrm{univ}}(\mathrm{Frob}_l)) \in R_\Sigma$ (resp. $\mathrm{tr}(\rho_\Sigma^{\mathrm{univ.mod.}}(\mathrm{Frob}_l)) \in \mathbb{T}_\Sigma$). Then $A^0 = A$.*

This lemma can be deduced from the following:

Proposition 7.35. *Let $A^0 \subset A$ be two local rings with maximal ideals satisfying*

$$\mathfrak{m}_{A^0} = \mathfrak{m}_A \cap A^0$$

and with the same finite residue field k . Suppose

$$\rho : G \rightarrow \mathrm{GL}_m(A)$$

is a representation of a group over A such that

- 1) $\bar{\rho} = \rho \bmod \mathfrak{m}_A$ *is absolutely irreducible;*
- 2) $\mathrm{tr}\rho(\sigma) \in A^0$ *for all $\sigma \in G$.*

Then ρ is conjugate over A to a representation

$$\rho^0 : G \rightarrow \mathrm{GL}_m(A^0)$$

Proof of Proposition 7.35.

Let B denote the A^0 -subalgebra in $M_m(A)$ generated by $\rho(G)$. The image of B in $M_m(k)$ is a central simple algebra over the finite field k . It follows from the triviality of the Brauer group (see §5.5.5) of the finite field k that the image of B in $M_m(k)$ is the whole of $M_m(k)$. Let e_1, \dots, e_{m^2} be elements of B whose reductions modulo \mathfrak{m}_A form the standard basis of $M_m(k) = B \bmod \mathfrak{m}_A$. We shall show that e_1, \dots, e_{m^2} is a basis for B over A^0 . By Nakayama's lemma elements of B may be expressed in the form:

$$b = \sum_{i=1}^{m^2} a_i e_i, \text{ with } a_i \in A.$$

Hence

$$\mathrm{tr}(b \cdot {}^t e_j) = \sum_{i=1}^{m^2} a_i \mathrm{tr}(e_i \cdot {}^t e_j), \text{ with } j = 1, \dots, m^2. \quad (7.4.1)$$

Let us define

$$c_{ij} = \mathrm{tr}(e_i {}^t e_j) \in A \Rightarrow (c_{ij}) \equiv I_{m^2} \bmod \mathfrak{m}_A.$$

Hence the system (7.4.1) is solvable over the local ring A^0 . One defines $V \subset A^m$ to be the submodule generated by the columns of elements in B . Thus $V \cong (A^0)^m$ is free, and we deduce that $B \xrightarrow{\sim} \mathrm{End}(V) \cong M_m(A^0)$ by Nakayama's lemma.

7.4.3 Constructions of the universal deformation ring R_Σ

We assume that ρ_0 is absolutely irreducible.

To prove the existence of R_Σ one can either appeal to a general criterion of Schlessinger (cf. Mazur's paper in [CSS95]), or instead use a more explicit method of H.Lenstra (cf. the paper of Bart de Smit and H.W.Lenstra in [CSS95]).

Consider first a finite group G , and let us define an \mathcal{O} -algebra $\mathcal{O}[G, m]$ with generators:

$$\{X_{ij}^g \mid i, j = 1, \dots, m; g \in G\},$$

and the following relations:

$$X_{ij}^e = \delta_{ij}, \quad X_{ij}^{gh} = \sum_{l=1}^m X_{il}^g X_{lj}^h \quad i, j = 1, \dots, m; g, h \in G$$

As these relations mimic the relations satisfied by matrix coefficients of a representation of G , it follows that for any $A \in \mathcal{C}_{\mathcal{O}}$ there is a canonical identification

$$\mathrm{Hom}_{\mathcal{O}\text{-alg}}(\mathcal{O}[G, m], A) = \mathrm{Hom}(G, \mathrm{GL}_m(A)). \quad (7.4.2)$$

Substituting $A = \mathcal{O}/\lambda = k$ in the above formula, we obtain a homomorphism π_0 of \mathcal{O} -algebras corresponding to ρ_0 :

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{O}\text{-alg}}(\mathcal{O}[G, m], k) & = & \mathrm{Hom}(G, \mathrm{GL}_m(k)) \\ \Downarrow & & \Downarrow \\ \pi_0 & \longleftarrow & \rho_0. \end{array}$$

Let $\mathfrak{m}_0 = \mathrm{Ker} \pi_0$; we define the \mathcal{O} -algebra R_G to be the completion of $\mathcal{O}[G, m]$ with respect to \mathfrak{m}_0 :

$$R_G = \varprojlim_n \mathcal{O}[G, m]/\mathfrak{m}_0^n.$$

Now suppose we have a profinite group:

$$G_\Sigma = \varprojlim_j G_j.$$

Then we put

$$R_j = R_{G_j}, \quad R_\Sigma = \varprojlim_j R_j.$$

It may be verified that

a)

$$\mathrm{Hom}_{\rho_0}(G, \mathrm{GL}_m(A)) = \mathrm{Hom}_{\mathcal{O}\text{-alg}}(R_\Sigma, A). \quad (7.4.3)$$

b) R_Σ is a local Noetherian \mathcal{O} -algebra (to show this, one uses a universal bound for the dimension of the tangent space of R_j , and the absolute irreducibility of ρ_0).

7.4.4 A sketch of a construction of the universal modular deformation ring \mathbb{T}_Σ

Let us again fix a two-dimensional modular representation $\rho_0 : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(k)$ over the finite field k , together with sets S and Σ as above.

We shall consider a slightly different Hecke algebra than in 7.3, Definition 7.24, namely,

$$\mathbb{T}(\Sigma) = \mathcal{O}[T_l, U_q, \langle d \rangle \mid l \nmid N_\Sigma, d \in (\mathbb{Z}/N\mathbb{Z})^\times, q \in S \cup \Sigma].$$

We shall regard $\mathbb{T}(N_\Sigma)$ as a subalgebra of $\mathrm{End}_{\mathcal{O}} S_2(N_\Sigma, \mathcal{O})$. In the above we have

$$N_\Sigma = p \prod_{\tilde{q} \in S} \tilde{q} \prod_{\tilde{l} \in \Sigma} \tilde{l}^2.$$

Furthermore $S_2(N_\Sigma, \mathcal{O})$ denotes the \mathcal{O} -submodule of $\mathcal{O}[[q]]$, generated by all formal q -expansions of the form

$$\sum_{n \geq 1} i_p(a_n) q^n \in \mathcal{O}[[q]],$$

such that

$$f = \sum_{n \geq 1} a_n q^n \in S_2(N_\Sigma; \overline{\mathbb{Q}})$$

is a cusp form with coefficients $a_n \in \overline{\mathbb{Q}} \cup i_p^{-1}(\mathcal{O})$.

Let

$$\tilde{f} = f_\emptyset = \sum_{n \geq 1} \tilde{a}_n q^n$$

denote Ribet's modular form of Theorem 7.30, attached to a two-dimensional modular representation $\rho_0 : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(k)$ over the finite field k .

Recall that Ribet's modular Galois representation

$$\tilde{\rho} = \rho_{f, \lambda} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathcal{O})$$

of minimal level N_0 given by Theorem 7.30 belongs to the (non-empty) set $DM_\emptyset(\mathcal{O})$. For any Σ as above, we define

$$f_\Sigma = \sum_{n \geq 1} \tilde{a}_n(f_\Sigma) q^n$$

by removing from the Mellin transform of \tilde{f} the Euler factors at $\tilde{l} \in \Sigma$:

$$\begin{aligned} L(f_\Sigma, s) &= \sum_{n \geq 1} \tilde{a}_n(f_\Sigma) n^{-s} \\ &= \prod_{\tilde{q} \in S} (1 - \tilde{a}_{\tilde{q}} \tilde{q}^{-s})^{-1} \prod_{\tilde{l} \nmid N_\Sigma} (1 - \tilde{a}_{\tilde{l}} \tilde{l}^{-s} + \tilde{l}^{1-2s})^{-1}. \end{aligned} \tag{7.4.4}$$

Now consider the following ideal of the Hecke algebra:

$$\mathcal{M}_\Sigma = (\lambda, T_l - \tilde{a}_l, U_{\tilde{q}} - \tilde{a}_{\tilde{q}}, T_{\tilde{l}})_{l \notin \Sigma \cup S \cup \{p\}, \tilde{q} \in S, \tilde{l} \in \Sigma}. \quad (7.4.5)$$

This ideal is actually prime, since

$$\begin{aligned} \mathcal{M}_\Sigma &= \text{Ker}(\mathbb{T}(\Sigma) \xrightarrow{\pi_{f_\Sigma}} k[[q]]), \\ T_l &\mapsto a_l \bmod \lambda, \\ U_{\tilde{q}} &\mapsto a_{\tilde{q}} \bmod \lambda, \\ T_{\tilde{l}} &\mapsto 0 \\ &\quad (l \notin \Sigma \cup S \cup \{p\}, \tilde{q} \in S, \tilde{l} \in \Sigma), \end{aligned} \quad (7.4.6)$$

and the ring $k[[q]]$ is an integral domain.

We define \mathbb{T}_Σ to be the completion of $\mathbb{T}(\Sigma)$ with respect to the ideal \mathcal{M}_Σ :

$$\mathbb{T}_\Sigma = \varprojlim_n \mathbb{T}(\Sigma) / \mathcal{M}_\Sigma^n.$$

One can check that \mathbb{T}_Σ is a finite flat local Noetherian \mathcal{O} -algebra (i.e. it is a free \mathcal{O} -module of finite rank), and one defines an augmentation map $\mathbb{T}_\Sigma \rightarrow \mathcal{O}$ using \tilde{f} .

Theorem 7.36. *There exists, up to isomorphism, a unique admissible Galois representation*

$$\rho_\Sigma^{\text{univ.mod.}} : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{T}_\Sigma), \quad (7.4.7)$$

with the following properties:

$$\begin{aligned} \text{tr}(\rho_\Sigma^{\text{univ.mod.}}(\text{Frob}_l)) &= T_l, \\ \det(\rho_\Sigma^{\text{univ.mod.}}(\text{Frob}_l)) &= l(l \notin \Sigma \cup S \cup \{p\}). \end{aligned} \quad (7.4.8)$$

The construction by A.Wiles of the universal representation $\rho_\Sigma^{\text{univ.mod.}}$ was obtained from the Eichler–Shimura Theorem 7.26 by patching together all the modular deformations of type \mathcal{D}_Σ . To achieve this he used of the theory of pseudo-representations. The strong absolute irreducibility condition of theorem 7.28, concerning the restriction

$$\rho_0|_{G_{\mathbb{Q}}\left(\sqrt{\frac{p-1}{(-1)^{\frac{p-1}{2}}p}}\right)},$$

was essential in this construction.

7.4.5 Universality and the Chebotarev density theorem

Let us recall Theorem 4.22 in the following form:

Theorem 7.37 (Chebotarev density theorem). *Let L/K be a finite extension of number fields, and let X be a non-empty subset of $G(L/K)$, invariant under conjugation. Denote by P_X the set of places $v \in \Sigma_K^0$, unramified in L , such that the classes of Frobenius elements of these places belong to X : $F_{L/K}(P_X) \subset X$. Then the set P_X is infinite and has a density, which is equal to $\text{Card } X / \text{Card } G(L/K)$.*

Corollary 7.38. *The canonical morphism (7.3.2) is compatible with the augmentation maps π_{R_Σ} and $\pi_{\mathbb{T}_\Sigma}$*

$$\varphi_\Sigma : R_\Sigma \rightarrow \mathbb{T}_\Sigma \quad (7.4.9)$$

In fact, the traces of representations π_{R_Σ} and $\pi_{\mathbb{T}_\Sigma} \circ \varphi_\Sigma$ coincide on the subset of elements $\text{Frob}_l (l \notin \Sigma_S)$ (which is dense in the group G_{Σ_S}). It follows that the corresponding universal deformations are equivalent, hence they coincide by their universal property.

7.4.6 Isomorphism Criteria for local rings

To prove that the canonical morphism (7.3.2)

$$\varphi_\Sigma : R_\Sigma \rightarrow \mathbb{T}_\Sigma$$

of universal deformation rings is an isomorphism (in the category $\mathcal{C}_\mathcal{O}$), one argues by induction on Σ . Let $\Sigma' = \Sigma \cup \{l\}$ for some prime l not in Σ_S . Wiles deduced the bijectivity of $\varphi_{\Sigma'}$ from the bijectivity of φ_Σ using an isomorphism criterion for local rings. This criterion is formulated in terms of certain invariants, which will be described next. In order to start the induction, one needs to prove the case $\Sigma = \emptyset$; this is achieved by a second isomorphism criterion for local rings.

Definition 7.39. *A local Noetherian \mathcal{O} -algebra A is called a complete intersection if:*

- a) *A is a free \mathcal{O} -module of finite rank;*
- b) *$A \cong \mathcal{O}[[X_1, \dots, X_n]]/(f_1, \dots, f_n)$.*

(cf. [Mats70]).

We shall use the following invariants of a local \mathcal{O} -algebra A :

$$I_A = \text{Ker } \pi_A, \quad \Phi_A = I_A/I_A^2, \quad \eta_A = \pi_A(\text{Ann } I_A) \subset \mathcal{O} \quad (7.4.10)$$

These are called respectively the *kernel of augmentation*, the *tangent space* and the *congruence module*.

Example 7.40. a) $A = \mathcal{O} = \mathbb{Z}_p$, $\Phi_A = I_A/I_A^2 = \{0\}$

- b) $A = \mathbb{Z}_p[[X, Y]]/(X(X - p), Y(Y - p))$, $\Phi_A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, $\eta_A = (p^2)$.
The augmentation map in this case is given by

$$\pi_A(f) = f(0, 0) \in \mathbb{Z}_p, \quad A \text{ is a complete intersection ring.}$$

The ring A is a complete intersection.

- c) $A = \mathbb{Z}_p[[X, Y]]/(X(X - p), Y(Y - p), XY)$, $\Phi_A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, $\eta_A = (p)$.
The augmentation is given by

$$\pi_A(f) = f(0, 0) \in \mathbb{Z}_p.$$

In this case A is not a complete intersection.

Theorem 7.41 (Criterion I). *Let $\varphi : A \rightarrow B$ be a surjective morphism in the category $\mathcal{C}_{\mathcal{O}}$. Then the following are equivalent:*

- (i) φ is an isomorphism of two local complete intersection \mathcal{O} -algebras;
- (ii) $\#\Phi_A \leq \#\mathcal{O}/\eta_B < \infty$;
- (iii) $\#\Phi_A = \#\mathcal{O}/\eta_B < \infty$.

Remark 7.42. In the first version of his proof A.Wiles had made the assumption that the ring B is *Gorenstein* (i.e. $\tilde{B} = \text{Hom}(B, \mathcal{O})$ is a free B -module of rank 1). This restriction was later removed by H.Lenstra.

Corollary 7.43. *An \mathcal{O} -algebra $A \in \mathcal{C}_{\mathcal{O}}$ is a complete intersection ring if and only if*

$$\#\Phi_A = \#\mathcal{O}/\eta_A < \infty.$$

This is proved by applying Criterion I to the identity map $\text{id}_A : A \rightarrow A$.

7.4.7 J -structures and the second criterion of isomorphism of local rings

Let us consider the distinguished ideals

$$J_m = (\omega_m(S_1), \dots, \omega_m(S_n)) \subset \mathcal{O}[[S_1, \dots, S_n]],$$

where

$$\omega_m(S_1) = (1 + S_1)^{p^m} - 1, \quad \omega_m(S_n) = (1 + S_n)^{p^m} - 1, \quad J_0 = (S_1, \dots, S_n).$$

Definition 7.44. *Let $\varphi : A \rightarrow B$ be a surjective morphism in $\mathcal{C}_{\mathcal{O}}$. One says that φ admits a J -structure, if there is a family of commutative diagrams, indexed by $m \in \mathbb{N}$:*

$$\begin{array}{ccccc} & & \mathcal{O}[[S_1, \dots, S_n]] & & \\ & & \downarrow \sigma_m & & \\ \mathcal{O}[[T_1, \dots, T_n]] & \xrightarrow{\xi_m} & A_m & \xrightarrow{\varphi_m} & B_m \\ & & \downarrow & & \downarrow \\ & & A & \xrightarrow{\varphi} & B \end{array}$$

with the following properties for each m :

- i) ξ_m is surjective;
- ii) φ_m is surjective;
- iii) $A_m/J_0A_m \cong A$ and $B_m/J_0B_m \cong B$.
- iv) B_m/J_mB_m is a torsion free module of finite rank over the \mathcal{O} -algebra $\mathcal{O}[[S_1, \dots, S_n]]/J_m$.

Theorem 7.45 (Criterion II).

Let $\varphi : A \rightarrow B$ be a surjective morphism in the category $\mathcal{C}_{\mathcal{O}}$.

If φ admits a J -structure then φ is an isomorphism of two local complete intersection \mathcal{O} -algebras.

Proof of both criteria belong to commutative algebra. We refer therefore the reader to [CSS95], [Ta-Wi].



<http://www.springer.com/978-3-540-20364-3>

Introduction to Modern Number Theory
Fundamental Problems, Ideas and Theories

Manin, Y.I.; Panchishkin, A.A.

2005, XVI, 514 p., Hardcover

ISBN: 978-3-540-20364-3