* Anti-cyclotomic Cyclicity and Gorenstein-ness of Hecke algebras

Haruzo Hida
Department of Mathematics, UCLA,
Los Angeles, CA 90095-1555, U.S.A.

A talk in June, 2016
at Rubinfest at Harvard.

*The author is partially supported by the NSF grant: DMS 1464106.

Under mild conditions, we prove certain Gorenstein property is equivalent to cyclicity of the Iwasawa module for the anticyclotomic $\mathbb{Z}_p$-extension over an imaginary quadratic field with an anti-cyclotomic branch character. If such ring theoretic result holds, the characteristic ideal of the Iwasawa module determines the isomorphism class of the Iwasawa module, as expected by Iwasawa.

§**1. Cyclotomic cyclicity, a conjecture of Iwasawa:** Fix a prime $p > 3$. We have the following conjecture due to Iwasawa (cf. No.62 and U3 in his collected papers):

Cyclotomic cyclicity conjecture: *Let X be the Galois group of the maximal p-abelian extension everywhere unramified over $\mathbb{Q}(\mu_{p^\infty})$. Let $X(\omega^k)$ be the ω^k-branch on which complex conjugation acts by -1. Identifying* $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \mathbb{Z}_p^\times = \mu_{p-1} \times \Gamma$ *and regarding $X(\omega^k)$ as $\mathbb{Z}_p[[\Gamma]]$-module naturally, $X(\omega^k)$ is pseudo isomorphic to $\mathbb{Z}_p[[\Gamma]]/(f)$ for a power series f prime to $p\mathbb{Z}_p[[\Gamma]]$.*

Here ω is the Teichmüller character. Iwasawa wrote this conjecture in 1987 in a paper in Japanese (No.62) without much theoretical evidence (though he verified it under the Kummer–Vandiever conjecture, which now known to hold for primes up to 163 million). Iwasawa wrote at the end of No.62: "a most interesting point of number theory is that authentic conjectures often fail! This is an excuse for presenting outrageous predictions."

§2. **Setting over an imaginary quadratic field.** Let F be an imaginary quadratic field with discriminant $-D$ and integer ring O. Assume that the prime (p) **splits** into $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in O with $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Let L/F be a $\mathbb{Z}_p$-extension with group $\mathbf{\Gamma}_L := \mathrm{Gal}(L/F) \cong \mathbb{Z}_p$. Take a branch character $\overline{\phi} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathbb{F}^\times$ (for $\mathbb{F} = \mathbb{F}_{p^f}$) with its Teichmüller lift ϕ with values in $W = W(\mathbb{F})$. Regard it as an idele character $\phi : F_{\mathbb{A}}^\times/F^\times \to \overline{\mathbb{Q}}_p^\times$ with

$$W = \mathbb{Z}_p[\phi] := \mathbb{Z}_p[\phi(x)|x \in F_{\mathbb{A}}^\times] \subset \overline{\mathbb{Q}}_p.$$

Consider the Iwasawa algebra $W[[\mathbf{\Gamma}_L]] = \varprojlim_n W[\mathbf{\Gamma}_L/\mathbf{\Gamma}_L^{p^n}]$.

Let $F(\phi)/F$ be the extension cut out by ϕ (i.e., $F(\phi) = \overline{\mathbb{Q}}^{\mathrm{Ker}(\phi)}$). Let Y_L be the Galois group of the maximal p-abelian extension over the composite $L(\phi) := L \cdot F(\phi)$ **unramified outside** $\mathfrak{p}$. By the splitting: $\mathrm{Gal}(L(\phi)/F) = \mathrm{Gal}(F(\phi)/F) \times \mathbf{\Gamma}_L$, we have

$$Y_L(\phi) := Y_L \otimes_{W[\mathrm{Gal}(F(\phi)/F)],\phi} W \ \textbf{(the } \phi\textbf{-eigenspace)}.$$

This is a **torsion** module over $W[[\mathbf{\Gamma}_L]]$ of finite type by Rubin.

§3. Cyclicity conjecture for an anti-cyclotomic branch. Let c be a generator of Gal$(F/\mathbb{Q})$. Suppose that $\phi(x) = \varphi(x)\varphi(x^{-c}) := \varphi^-(x)$ for a finite order character $\varphi : F_{\mathbb{A}}^\times/F^\times \to \overline{\mathbb{Q}}_p^\times$.

Conjecture for L: *Assume $\varphi^- \neq 1$ and that the conductor φ is a product of split primes over $\mathbb{Q}$. If the class number h_F of F is prime to p, then $Y_L(\varphi^-)$ is pseudo isomorphic to $W[[\mathbf{\Gamma}_L]]/(f_L)$ as $W[[\mathbf{\Gamma}_L]]$-modules for an element $f_L \in W[[\mathbf{\Gamma}_L]]$.*

We know $f_L \neq 0$ by Rubin. For some specific $\mathbb{Z}_p$-extension (e.g., the anticyclotomic $\mathbb{Z}_p$-extension), we know that (f_L) is prime to $pW[[\mathbf{\Gamma}_L]]$ (vanishing of the μ-invariant).

The anti-cyclotomic cyclicity conjecture is the one for the anticyclotomic $\mathbb{Z}_p$-extension $L = F_\infty^-$ such that on $\mathbf{\Gamma}_- := \mathbf{\Gamma}_{F_\infty^-}$, we have $c\sigma c^{-1} = \sigma^{-1}$. Write $Y^-(\varphi^-)$ for the $W[[\mathbf{\Gamma}_-]]$-module $Y_{F_\infty^-}(\varphi^-)$.

§4. By Rubin, anti-cyclotomic cyclicity $\Rightarrow$ L-cyclicity.

In this talk, hereafter, we suppose

(H1) We have $\phi = \varphi^-$ for a character φ of conductor $\mathfrak{c}\mathfrak{p}$ with $\mathfrak{c} + (p) = O$ and of order prime to p,
(H2) $N = DN_{F/\mathbb{Q}}(\mathfrak{c})$ for an O-ideal $\mathfrak{c}$ prime to D with square-free $N_{F/\mathbb{Q}}(\mathfrak{c})$ (so, N is cube-free),
(H3) p is prime to $N\prod_{l|N}(l-1)$ for prime factors l of N,
(H4) the character φ^- has order at least 3,
(H5) the class number of F is prime to p.

We prove

Theorem A: *Under* (H1–5), *The anticyclotomic pure cyclicity implies pure cyclicity for* $Y_L(\varphi^-)$. (**Note that the branch character is anti-cyclotomic.**)

§**5. Rubin's control theorem.** Let K_∞/F be the unique $\mathbb{Z}_p^2$-extension with $\mathbf{\Gamma} = \mathrm{Gal}(K_\infty F(\phi)/F(\phi)) \cong \mathbb{Z}_p^2$. Let Y be the Galois group of the maximal p-abelian extension over $K_\infty F(\phi)$ unramified outside $\mathfrak{p}$, and put $Y(\phi) = Y \otimes_{W[[\mathbf{\Gamma}]],\phi} W$. Let $\mathfrak{a}_L :=$ $\mathrm{Ker}(W[[\mathbf{\Gamma}]] \to W[[\mathbf{\Gamma}_L]]$ and $\mathfrak{a}_- := \mathrm{Ker}(W[[\mathbf{\Gamma}]] \to W[[\mathbf{\Gamma}_-]]$.

Theorem 1 (Rubin)**.** *Assume that $\phi \neq 1$. As long as K_∞/L is unramified outside $\mathfrak{p}$, we have*

$$Y(\phi)/\mathfrak{a}_- Y(\phi) \cong Y^-(\phi) \quad \textit{and} \quad Y(\phi)/\mathfrak{a}_L Y(\phi) \cong Y_L(\phi)$$

as $W[[\mathbf{\Gamma}_F]]$-modules. If L is the Coates–Wiles tower unramified outside $\mathfrak{p}$, the natural map $Y(\phi)/\mathfrak{a}_L Y(\phi) \to Y_L(\phi)$ is surjective.

If one can show the **cyclicity without pseudo-null error** for $Y^-(\varphi^-)$, by Rubin's control theorem, $Y(\varphi^-)$ is cyclic by Nakayama's lemma, and hence $Y_L(\varphi^-)$ has to be cyclic.

§6. Anti-cyclotomic Cyclicity and Hecke algebra. Anti-cyclotomic cyclicity follows from a **ring theoretic assertion** on the big ordinary Hecke algebra $\mathbf{h}$. We identify the Iwasawa algebra $\Lambda = W[[\Gamma]]$ with the one variable power series ring $W[[T]]$ by $\Gamma \ni \gamma = (1+p) \mapsto t = 1+T \in \Lambda$. Take a Dirichlet character $\psi : (\mathbb{Z}/Np\mathbb{Z})^\times \to W^\times$, and consider the big ordinary Hecke algebra $\mathbf{h}$ (over Λ) of prime-to-p level N and the character ψ. We just mention here the following three facts about $\mathbf{h}$:

- $\mathbf{h}$ is an algebra flat over the Iwasawa (weight) algebra $\Lambda := W[[T]]$ **interpolating** p-ordinary Hecke algebras of level Np^{r+1}, of weight $k+1 \geq 2$ and of character $\epsilon\psi\omega^{1-k}$, where $\epsilon : \mathbb{Z}_p^\times \to \mu_{p^r}$ ($r \geq 0$) and $k \geq 1$ vary. If N is cube-free, $\mathbf{h}$ is a **reduced** algebra;
- Each prime $P \in \mathrm{Spec}(\mathbf{h})$ has a unique Galois representation

$$\rho_P : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\kappa(P)),\ \mathrm{Tr}\rho_P(\mathrm{Frob}_l) = T(l) \bmod P (l \nmid Np)$$

for the residue field $\kappa(P)$ of P;
- $\rho_P|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \cong \begin{pmatrix} \epsilon_P & * \\ 0 & \delta_P \end{pmatrix}$ with unramified quotient character δ_P.

§7. **Hypothesis for the ring theoretic conjecture.** We study a local ring $\mathbb{T}$ of $\mathbf{h}$ with maximal ideal $\mathfrak{m} = \mathfrak{m}_{\mathbb{T}}$. Suppose

(h0) p is prime to $N\prod_{l|N}(l-1)$ for prime factors l of N,
(h1) $N = DN_{F/\mathbb{Q}}(\mathfrak{c})$ for an O-ideal $\mathfrak{c}$ prime to D with square-free $N_{F/\mathbb{Q}}(\mathfrak{c})$ (so, N is cube-free; so, $\mathbb{T}$ is **reduced**),
(h2) $\overline{\rho} = \rho_{\mathfrak{m}}$ is the absolutely irreducible induced representation $\mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}$ for a Galois character $\overline{\varphi} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathbb{F}^\times = \varphi \mod p$ unramified outside $\mathfrak{c}\mathfrak{p}$,
(h3) Np is the conductor of $\det(\overline{\rho})$ ($\overline{\epsilon} := \epsilon_{\mathfrak{m}}$ ramifies at p),
(h4) writing $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)} = \overline{\varphi} \oplus \overline{\varphi}'$, the ratio $\overline{\varphi'}^{-1}\overline{\varphi} = \overline{\varphi}^-$ has order **at least** 3.

Write ψ for the Teichmüller lift of $\det(\overline{\rho})$. Let K be the ray class field over F of conductor $\mathfrak{C}p^\infty$ for $\mathfrak{C} := \mathfrak{c} \cap \mathfrak{c}^c$ and $H := \mathrm{Gal}(K^-/F)$ for the maximal p-abelian anticyclotomic sub-extension K^-/F of K/F. Note $H = \mathbf{\Gamma}_-$ if $p \nmid h_F$.

§8. Ring theoretic conjecture.

Conjecture B: *Let* Spec($\mathbb{T}$) *be the connected component of* Spec($\mathbf{h}$) *as above. Then* $\mathbb{T}$ *has an* **algebra involution** σ *over* Λ *with the following two properties:*

(i) *For the ideal* I *of* $\mathbb{T}$ *generated by* $\mathbb{T}^- = \{\sigma(x) - x | x \in \mathbb{T}\}$ *(the "$-$" eigenspace), we have a canonical isomorphism* $\mathbb{T}/I \cong W[[H]]$ *as* Λ*-algebras, where the* Λ*-algebra structure is given by sending* $u \in \Gamma$ *naturally into* $u \in O_{\mathfrak{p}}^{\times} = \mathbb{Z}_p^{\times}$ *and then projecting the local Artin symbol* $\tau = [u, F_{\mathfrak{p}}] \in \Gamma$ *to* $\sqrt{\tau c \tau^{-1} c^{-1}} = \tau^{(1-c)/2} \in H$*.*
(ii) I *is a* **principal** *ideal of* $\mathbb{T}$*.*

By irreducibility of $\overline{\rho}$, we have a Galois representation $\rho_{\mathbb{T}}$: Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) $\rightarrow$ GL$_2$($\mathbb{T}$) with Tr($\rho_{\mathbb{T}}$(Frob$_l$)) $= T(l)$ for all primes $l \nmid Np$.

§9. Conjecture B $\Rightarrow$ Pure anti-cyclotomic cyclicity, Involution σ. By the celebrated $R = \mathbb{T}$ theorem of Taylor–Wiles, the couple $(\mathbb{T}, \rho_{\mathbb{T}})$ is universal among deformations $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(A)$ satisfying

(D1) $\rho \mod \mathfrak{m}_A \cong \overline{\rho}$.

(D2) $\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \cong \left(\begin{smallmatrix} \epsilon & * \\ 0 & \delta \end{smallmatrix}\right)$ with δ unramified.

(D3) $\det(\rho)|_{I_l} = \psi_l$ for the l-part ψ_l of ψ for each prime $l|N$.

(D4) $\det(\rho)|_{I_p} \equiv \psi|_{I_p} \mod \mathfrak{m}_A$ ($\Leftrightarrow \epsilon|_{I_p} \equiv \psi|_{I_p} \mod \mathfrak{m}_A$).

For $\chi = \left(\frac{F/\mathbb{Q}}{}\right)$, if ρ satisfies (D1–4), $\rho \otimes \chi$ satisfies (D1–4); so, by universality, we have $\sigma \in \mathrm{Aut}(\mathbb{T})$ such that

$$\sigma \circ \rho_{\mathbb{T}} \cong \rho_{\mathbb{T}} \otimes \chi.$$

By the $R = \mathbb{T}$ theorem and a theorem of Mazur, if $p \nmid h_F$,

$$I/I^2 = \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} W[[H]] = \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} W[[\boldsymbol{\Gamma}_-]] \cong Y^-(\varphi^-),$$

and principality of I implies cyclicity.

§**10. A key duality lemma** from the theory of dualizing modules by Grothendieck, Hartshorne and Kleiman in a simplest case:

Lemma 1. *Let S be a p-profinite* **Gorenstein integral domain** *and A be a* **reduced Gorenstein local S-algebra** *free of finite rank over S. Suppose*

- *A has a ring involution σ with $A_+ := \{a \in A | \sigma(a) = a\}$,*
- *A_+ is Gorenstein,*
- $\mathrm{Frac}(A)/\mathrm{Frac}(A_+)$ *is étale quadratic extension.*
- $\mathfrak{d}^{-1}_{A/A_+} := \{x \in \mathrm{Frac}(A) | \mathrm{Tr}_{A/A_+}(xA) \subset A_+\} \supsetneq A$,

Then A is free of rank 2 over A_+ and $A = A_+ \oplus A_+\delta$ for an element $\delta \in A$ with $\sigma(\delta) = -\delta$.

Lemma 2. *Let S be a* **Gorenstein local ring***. Let A be a local Cohen–Macaulay ring and is an S-algebra with $\dim A = \dim S$. If A is an S-module of finite type, the following conditions are equivalent:*

- *The local ring A is Gorenstein;*
- *$A^\dagger := \mathrm{Hom}_S(A, S) \cong A$ as A-modules.*

§11. Almost we can apply the key lemmas to $\mathbb{T}$.

1st Step: $\mathbb{T}$ is a local complete intersection by Taylor–Wiles; so, Gorenstein ($\Leftrightarrow \mathbb{T}^\vee := \mathrm{Hom}_\Lambda(\mathbb{T},\Lambda) \cong \mathbb{T}$).

2nd Step: Decompose $\mathbb{T} = \mathbb{T}^+ \oplus \mathbb{T}^-$ for the $\pm$-eigenspace $\mathbb{T}^\pm$ of σ; so, $\mathbb{T}^- = (\sigma-1)\mathbb{T}$ and $I = \mathbb{T}\cdot\mathbb{T}^-$. The quotient $\mathbb{T}/I$ is the maximal quotient on which σ acts trivially; so, $\rho_\mathbb{T} \mod I \cong \mathrm{Ind}_F^\mathbb{Q}\Phi$ and hence $\mathbb{T}/I \cong W[[H]]$. Note $\mathrm{Frac}(\mathbb{T}) = \mathrm{Frac}(W[[H]]) \oplus X$ as algebra direct sum. Let $\mathbb{T}^{\mathrm{ncm}}$ be the image of $\mathbb{T}$ in X.

3rd Step: Since $\mathrm{rank}_\Lambda \mathbb{T}^+ = \mathrm{rank}_\Lambda W[[H]] + \mathrm{rank}_\Lambda \mathbb{T}^- > \mathrm{rank}_\Lambda \mathbb{T}^-$, $\mathbb{T}^+$ is Gorenstein. Indeed, by Step 1, $\mathbb{T}^+$ has to be isomorphic to $\mathbb{T}^{+,\vee}$ (Krull-Schmidt Theorem).

If $\mathbb{T}$ were a domain and $\mathfrak{d}_{\mathbb{T}/\mathbb{T}_+} \subset \mathfrak{m}_\mathbb{T}$, applying Lemma 1, $I = \mathbb{T}\cdot\mathbb{T}^- = (\delta)$ with $\delta \in \mathbb{T}^-$, we get the result. But $\mathbb{T}$ is not a domain as $\mathrm{Frac}(\mathbb{T}) = \mathrm{Frac}(W[[H]]) \oplus \mathrm{Frac}(\mathbb{T}^{\mathrm{ncm}})$ if $\mathbb{T}^{\mathrm{ncm}} \neq 0$ (the case where $Y^-(\varphi^-) \neq 0$ we are interested in).

§12. Presentation of $\mathbb{T}$.

A way-out could be to find a power series ring $\mathcal{R} = \Lambda[[T_1, \ldots, T_r]]$ with an involution σ_∞ such that $\mathcal{R}^+ := \{r \in \mathcal{R} | \sigma_\infty(r) = -r\}$ is Gorenstein and that $(\mathcal{R}/\mathfrak{A}, \sigma_\infty \bmod \mathfrak{A}) \cong (\mathbb{T}, \sigma)$ for an ideal $\mathfrak{A}$ stable under σ_∞.

Taylor and Wiles (with a later idea of Diamond and Fujiwara) find a pair $(\mathcal{R} := \Lambda[[T_1, \ldots, T_r]], (S_1, \ldots, S_r))$ with a regular sequence $(S_1, \ldots, S_r) \subset \Lambda[[T_1, \ldots, T_r]])$ such that

$$\Lambda[[T_1, \ldots, T_r]]/(S_1, \ldots, S_r) \cong \mathbb{T}$$

by their Taylor–Wiles system argument.

We need to lift σ somehow to an involution $\sigma_\infty \in \mathrm{Aut}(\mathcal{R})$ and show also that $\mathcal{R}^+$ is Gorenstein. If further $\mathfrak{d}_{\mathcal{R}/\mathcal{R}^-} \subset \mathfrak{m}_\mathcal{R}$, $\mathcal{R} \cdot \mathcal{R}^- = (\delta_\infty)$ and the image $\delta \in \mathbb{T}^-$ of δ_∞ in $\mathbb{T}$ generates I as desired.

§**13. Taylor–Wiles method.** Taylor–Wiles found an integer $r > 0$ and an infinite sequence of r-sets $\mathcal{Q} := \{Q_m | m = 1, 2, \dots\}$ of primes $q \equiv 1 \mod p^m$ such that for **the local ring** $\mathbb{T}^{Q_m}$ of $\overline{\rho}$ of the Hecke algebra $\mathbf{h}^{Q_m}$ of tame-level $N_m = N \prod_{q \in Q_m} q$. The pair $(\mathbb{T}^{Q_m}, \rho_{\mathbb{T}^{Q_m}})$ is universal among deformation satisfying (D1–4) but ramification at $q \in Q_m$ is allowed. Then $\rho \mapsto \rho \otimes \chi$ induces an involution σ_{Q_m} and $\mathbb{T}^{Q_m}_{+} := \{x \in \mathbb{T}^{Q_m} | \sigma_{Q_m}(x) = x\}$ is Gorenstein.

Actually they work with $\mathbb{T}_{Q_m} = \mathbb{T}^{Q_m}/(t - \gamma^{k-1})\mathbb{T}^{Q_m}$ ($t = 1 + T$, $\gamma = 1 + p \in \Gamma$; the weight k Hecke algebra of weight $k \geq 2$ fixed). The product inertia group $I_{Q_m} = \prod_{q \in Q_m} I_q$ acts on $\mathbb{T}_{Q_m}$ by the p-abelian quotient Δ_{Q_m} of $\prod_{q \in Q_m} (\mathbb{Z}/q\mathbb{Z})^{\times}$. We choose an ordering of primes $Q_m = \{q_1, \dots, q_r\}$ and a generator $\delta_{i,m(n)}$ of the p-Sylow group of $(\mathbb{Z}/q_i\mathbb{Z})^{\times}$. The sequence $\mathcal{Q}$ is chosen so that for a given integer $n > 0$, we can find $m = m(n) > n$ so that we have ring projection maps $R_{n+1} := \mathbb{T}_{Q_{m(n+1)}}/(p^{n+1}, \delta_{i,m(n+1)}^{p^{n+1}} - 1)_i \to R_n$, and $R_\infty = \varprojlim_n R_n \cong W[[T_1, \dots, T_r]]$ and $S_i = \varprojlim_n (\delta_{i,m(n)} - 1)$.

§14. Lifting involution.

Write $\overline{\mathcal{S}}_n$ for the image of $W[[S_1,\dots,S_r]]$ in R_n ($\overline{\mathcal{S}}_n$ is a Gorenstein local ring). We can add the involution to this projective system and an R_n-**linear isomorphism** $\phi_n : R_n^\dagger := \mathrm{Hom}_{\overline{\mathcal{S}}_n}(R_n,\overline{\mathcal{S}}_n) \cong R_n$ commuting with the involution σ_n of R_n induced by $\sigma_{Q_{m(n)}}$ to the Taylor-Wiles system, and get the lifting

$$\sigma_\infty \in \mathrm{Aut}(R_\infty)$$

$$\text{with}\quad \phi_\infty : R_\infty^\dagger := \mathrm{Hom}_{W[[S_1,\dots,S_r]]}(R_\infty, W[[S_1,\dots,S_r]]) \cong R_\infty$$

compatible with σ_∞; i.e., $\phi_\infty \circ \sigma_\infty = \sigma_\infty \circ \phi_\infty$. This shows

$$R_\infty^{+,\dagger} \cong R_\infty^+$$

as R_∞^+-modules, as desired. Then we can further lift involution to $\mathcal{R} = \Lambda[[T_1,\dots,T_r]]$ as $\mathcal{R}/(t-\gamma^{k-1}) = R_\infty$ for $t = 1+T$.

The remaining point I have not done is to show

$$\mathfrak{d}_{\mathcal{R}/\mathcal{R}^+} \subset \mathfrak{m}_{\mathcal{R}}?$$

§**15. Taylor–Wiles projective system.** Taylor and Wiles/Fujiwara found an infinite sequence $\mathcal{Q} = \{Q_m | m = 1, 2, \dots\}$ of ordered finite sets $Q = Q_m$ which produces a projective system:

$$\{((R_{n,m(n)}, \alpha = \alpha_n), \widetilde{R}_{n,m(n)}, (f_1 = f_1^{(n)}, \dots, f_r = f_r^{(n)}))\}_n \quad (1)$$

made of the following objects:

• $R_{n,m} := \mathbb{T}_{Q_m}/(p^n, \delta_q^{p^n} - 1)_{q \in Q_m}\mathbb{T}_{Q_m}$ for each $0 < n \le m$. Since the integer m in the system (1) is determined by n, we have written it as $m(n)$. An important point is that $R_{n,m}$ is a finite ring whose order is bounded independent of m (by (Q0) below).

• $\widetilde{R}_{n,m} := R_{n,m}/(\delta_q - 1)_{q \in Q_m}$, $\Delta_{n,Q_m} = \Delta_n := \Delta_{Q_m}/\Delta_{Q_m}^{p^n}$,

• $\alpha_n : W_n[\Delta_n] \to R_{n,m}$ for $W_n := W/p^nW$ is a $W[\Delta_n]$-algebra homomorphism for $\Delta_n = \Delta_{n,Q_m}$ induced by the $W[\Delta_{Q_m}]$-algebra structure of $\mathbb{T}_{Q_m}$ (making $R_{n,m}$ finite $W[\Delta_n]$-algebras).

• $(f_1 = f_1^{(n)}, \dots, f_r = f_r^{(n)})$ is an ordered subset of the maximal ideal of $R_{n,m}$.

§16. Properties satisfied by Q_m.

(Q0) $\mathbb{T}_{Q_m}$ is of rank d over $W[\Delta_{Q_m}]$ with d independent of m.

(Q1) $|Q_m| = r \geq \dim_{\mathbb{F}} \mathcal{D}_{Q_m}(\mathbb{F}[\epsilon])$ for r independent of m, where ϵ is the dual number with $\epsilon^2 = 0$.

(Q2) $q \equiv 1 \mod p^m$ and $\overline{\rho}(\mathrm{Frob}_q) \sim \begin{pmatrix} \overline{\alpha}_q & 0 \\ 0 & \overline{\beta}_q \end{pmatrix}$ with $\overline{\alpha}_q \neq \overline{\beta}_q \in \mathbb{F}$.

(Q3) The set $Q_m = \{q_1, \ldots, q_r\}$ is ordered so that

- $\Delta_{q_j} \subset \Delta_{Q_m}$ is identified with $\mathbb{Z}/p^{|\Delta_{q_j}|}\mathbb{Z}$ by $\delta_{q_j} \mapsto 1$; so, $\Delta_n = \Delta_{n,Q_{m(n)}} = (\mathbb{Z}/p^n\mathbb{Z})^{Q_{m(n)}}$,
- $\Delta_n = (\mathbb{Z}/p^n\mathbb{Z})^{Q_{m(n)}}$ is identified with $\Delta_{n+1}/\Delta_{n+1}^{p^n}$,
- the diagram

$$\begin{tikzcd} W_{n+1}[\Delta_{n+1}] \arrow[r, "\alpha_{n+1}"] \arrow[d] & R_{n+1,m(n+1)} \arrow[d, "\pi_n^{n+1}"] \\ W_n[\Delta_n] \arrow[r, "\alpha_n"] & R_{n,m(n)} \end{tikzcd}$$

is commutative for all $n > 0$ (α_n is injective for all n).

§17. Properties satisfied by Q_m, continued.

(Q4) There exists an ordered set of generators $\{f_1^{(n)}, \dots, f_r^{(n)}\} \subset \mathfrak{m}_{R_{n,m(n)}}$ of $R_{n,m(n)}$ over W for the integer r in (Q1) such that $\pi_n^{n+1}(f_j^{(n+1)}) = f_j^{(n)}$ for each $j = 1, 2, \dots, r$.

(Q5) $R_\infty := \varprojlim_n R_{n,m(n)}$ is isomorphic to $W[[T_1, \dots, T_r]]$ by sending T_j to $f_j^{(\infty)} := \varprojlim_n f_j^{(n)}$ for each j.

(Q6) Inside R_∞, $\varprojlim_n W_n[\Delta_n]$ is isomorphic to $W[[S_1, \dots, S_r]]$ so that $s_j := (1 + S_j)$ is sent to the generator $\delta_{q_j}\Delta_{q_j}^{p^n}$ of $\Delta_{q_j}/\Delta_{q_j}^{p^n}$ for the ordering $q_1, \dots, q_r$ of primes in Q_m in (Q3).

(Q7) $R_\infty/(S_1, \dots, S_r) \cong \varprojlim_n \widetilde{R}_{n,m(n)} \cong R_\emptyset \cong \mathbb{T}_\emptyset$, where $R_\emptyset$ is the universal deformation ring for the deformation functor $\mathcal{D}_\emptyset$ and $\mathbb{T}_\emptyset = \mathbb{T}/(t - \gamma^k)\mathbb{T}$.

(Q8) The pair $(\mathbb{T}_{Q_m}, \rho_{Q_m})$ is isomorphic to the universal pair for $\mathcal{D}_{Q_m}$, and $\mathbb{T}_{Q_m} \cong R_\infty/\mathfrak{A}_{Q_m}R_\infty$ for the ideal

$$\mathfrak{A}_{Q_m} := ((1 + S_j)^{|\Delta_{q_j}|} - 1)_{j=1,2,\dots r}$$

of $W[[S_1, \dots, S_r]]$ is a local complete intersection.

§**18. Compatibility with the involution σ_Q.** The involution $\sigma_{Q_{m(n)}}$ induces an involution σ_n on R_n. Write $\pi^n_{n+1} : R_{n+1} \twoheadrightarrow R_n$ for the projection. We claim to be able to add the compatibility:

(Q9) $\pi^{n+1}_n \circ \sigma_{n+1} = \sigma_n \circ \pi^{n+1}_n$, and the set $\{f^{(n)}_1, \ldots, f^{(n)}_r\}$ is made of eigenvectors of σ_n for all n (i.e., $\sigma_n(f^{(n)}_j) = \pm f^{(n)}_j$).

Here is a proof of the claim. The second point is just to replace f_j by $f_j \pm \sigma(f_j)$. If $m(n) = m(n+1)$, $R_j = \mathbb{T}_Q/(p^j, \delta_q^{p^j} - 1)_{q\in Q}$ $(j = n, n+1)$ for the same $Q = Q_{m(n)}$, and hence satisfies (Q9). Since we can find an isomorphism class containing infinitely many

$$\mathcal{I}_n := \{((R_{n,m}, \alpha = \alpha_n), \widetilde{R}_{n,m}, (f_1 = f^{(n)}_1, \ldots, f_r = f^{(n)}_r))\}_{n<m},$$

we can always find $m > n$ with an isomorphism class $\mathcal{I}_{n+1} := \{((R_{n+1,m}, \alpha = \alpha_{n+1}), \widetilde{R}_{n+1,m}, (f_1 = f^{(n+1)}_1, \ldots, f_r = f^{(n+1)}_r))\}_{n<m}$ of infinite cardinality whose reduction modulo $(p^j, \delta_q^{p^j} - 1)_{q\in Q}$ falls in $\mathcal{I}_n$. By keep repeating this process, we achieve (Q9).