ANTICYCLOTOMIC CYCLICITY CONJECTURE

HARUZO HIDA

Abstract. Let $F$ be an imaginary quadratic field. We formulate certain Gorenstein/local complete intersection property of subrings of the universal deformation ring $\mathcal{R}$ of a mod $p$ induced representation of a character of $\text{Gal}(\overline{\mathbb{Q}}/F)$. These conditions provide a base to prove pseudocyclicity of the Iwasawa module over $\mathbb{Z}_p$-extensions of $F$. Under mild conditions, we realize this scheme and prove anticyclotomic pseudocyclicity.

Fix a prime $p > 3$ throughout the paper. We have the following conjecture due to Iwasawa (cf. [CPI, No.62 and U3]):

Cyclotomic cyclicity conjecture: Let $X$ be the Galois group of the maximal $p$-abelian extension everywhere unramified over $\mathbb{Q}(\mu_{p^n})$. Let $X_{\pm}$ be the minus part on which complex conjugation acts by $\pm 1$. Then identifying $\text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) = \mathbb{Z}_p^\times = \mu_{p-1} \times \Gamma$ and regarding $X_{\pm}$ as $\mathbb{Z}_p[[\Gamma]]$-module naturally, $X_-$ is pseudo isomorphic to $\mathbb{Z}_p[[\Gamma]]/(f)$ for a power series $f$ prime to $p\mathbb{Z}_p[[\Gamma]]$.

This conjecture asserts the cyclicity (up to finite error) of $X_-$ as an Iwasawa module (i.e., having a single generator over the Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$). Under the assumption that $X_+ = 0$ (the Kummer–Vandieuvre conjecture), in [CPI, No.48], Iwasawa proved (along with his main conjecture) pure cyclicity without finite pseudo-null error. The fact $p \nmid f$ is a combination of the vanishing of the $\mu$-invariant of the Kubota–Leopoldt $p$-adic L-function (proven by Ferrero–Washington) and the proof of Iwasawa’s main conjecture by Mazur–Wiles. There are some positive results towards this conjecture via Galois deformation theory (e.g. [Ku93], [003], [Wa15] and [WE15]), relating it to Ribet’s proof of the converse of Herbrand’s theorem, Iwasawa main conjecture, Sharifi’s conjecture, a generalized version of the Kummer–Vandieuvre conjecture (which sometimes fails) and a conjecture of Greenberg.

Let $F$ be an imaginary quadratic field with discriminant $-D$ and integer ring $O$. Assume that the prime $(p)$ splits into $(p) = p\mathfrak{p}$ in $O$ with $p \neq \mathfrak{p}$. Let $F_\infty / F$ be the anti-cyclotomic $\mathbb{Z}_p$-extension with Galois group $\Gamma_- := \text{Gal}(F_\infty / F)$; so, $c \sigma c = \sigma^{-1}$ for complex conjugation $c$ and $\sigma \in \Gamma_- \cong \mathbb{Z}_p$. Take a branch character $\phi : \text{Gal}(\overline{\mathbb{Q}}/F) \to \overline{\mathbb{Q}}_p^\times$, fixing an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Regard it as a finite order idele character $\phi : F_\infty^\times / F^\times \to \overline{\mathbb{Q}}_p^\times$. Most of the time, we suppose that $\phi$ is anticyclotomic; so, $\phi(x^c) = \phi^{-1}(x)$. Although we always choose a finite order character $\varphi$ of $F_\infty^\times / F^\times$ such that $\phi = \varphi^\prime$ for $\varphi^\prime$ given by $\varphi^\prime(x) = \varphi(x)\varphi(x^-)^{-1}$ (e.g., [HMI, Lemma 5.31]), controlling the conductor of $\varphi$ is a difficult task. We write $\mathbb{Z}_p[\phi]$ for the subring of $\overline{\mathbb{Q}}_p$ generated by the values of $\phi$ over $\mathbb{Z}_p$. Consider the anticyclotomic Iwasawa algebra $\mathbb{Z}_p[\phi][[\Gamma_-]] = \lim_n \mathbb{Z}_p[\phi][\Gamma_- / \Gamma_-^n]$. Let $F(\phi)/F$ be the abelian extension cut out by $\phi$ (i.e., $F(\phi) = \overline{\mathbb{Q}}^{\text{Ker}(\phi)}$). Let $Y^-$ be the Galois group of the maximal $p$-ramified $p$-abelian extension over the composite $F_\infty^- := F_\infty^- F(\phi)$. The word: "$p$-ramified" means that it is unramified outside the prime $p$. Since $\text{Gal}(F(\phi)/F)$ acts on $Y^-$ naturally as a factor of $\text{Gal}(F(\phi)/F)$, we have the $\phi$-eigenspace $Y^- \phi = Y^- \otimes_{\mathbb{Z}_p[\text{Gal}(F(\phi)/F),\phi]} \mathbb{Z}_p[\phi]$, where $\mathbb{Z}_p[\phi]$ is the $\mathbb{Z}_p[\phi]$-free module of rank 1 on which $\text{Gal}(F(\phi)/F)$ acts via $\phi$.

Anticyclotomic cyclicity conjecture: Assume $\phi \neq 1$ and that the conductor $\phi$ is a product of split primes over $\mathbb{Q}$. If the class number of $F$ is prime to $p$, then the $\mathbb{Z}_p[\phi][[\Gamma_-]]$-module $Y^- \phi$ is pseudo isomorphic to $\mathbb{Z}_p[\phi][[\Gamma_-]]/(f^-)$ as $\mathbb{Z}_p[\phi][[\Gamma_-]]$-modules for an element $f^- \in \mathbb{Z}_p[\phi][[\Gamma_-]]$ prime to $p\mathbb{Z}_p[\phi][[\Gamma_-]]$.

We prove in this paper:

\[\text{Date: November 13, 2016.}\]
\[1991\ Mathematics Subject Classification.\ primary 11R23, 11F25, 11F33, 11F80; secondary 11F11, 11G18, 11F27.\]
\[The\ author\ is\ partially\ supported\ by\ the\ NSF\ grant:\ DMS\ 1464106.\]
Theorem A: Let the notation be as above. Assume that ϕ = φ into the Teichmüller lift φ of a mod p Galois character ϕ of conductor ℓ and let N = DN_{F/Q}(c). Suppose

(1) p is prime to N \prod \prod_{i=1}^{\infty} (l - 1) for prime factors l of N,
(2) ϕ is prime to D, and N_{F/Q}(c) is square-free (so, N is cube-free),
(3) \rho is the conductor of det(\rho) for \rho = \text{Ind}_F^Q \phi,
(4) \rho has order at least 3.

If the class number of F is prime to p, the anticyclotomic cyclicity conjecture holds.

The proof of this theorem is technical ring theoretic tools applied to a local ring of the big Hecke algebra of tame level N. In this introduction, to give a short outline of our argument without going into technicality, let us state a typical theorem which describes ring theoretic properties of the Hecke pure algebra of tame level a base ring, we take a (sufficiently large) complete discrete valuation ring F. If the class number of F is prime to p, let h be a finite set of rational primes in F, Q = \mathbb{Q}((h2), (h4), (h0), (h3), (h1)) be a set of rational primes in Z. Let T be the ring of integers of F. By (2), each local ring W \subset C is complete, and W_{\mathfrak{p}} is a complete discrete valuation ring W \subset \mathfrak{p} over the p-adic integer ring \mathbb{Z}_p. Here C_{\mathfrak{p}} is the p-adic completion of a fixed algebraic closure \overline{\mathbb{Q}}_{\mathfrak{p}} of \mathbb{Q}_{\mathfrak{p}} under its norm \| \cdot \|_{\mathfrak{p}} normalized so that \| p \|_{\mathfrak{p}} = 1/2. We identify the Iwasawa algebra A = W[\Gamma] with the one variable power series ring W[[T]] by \Gamma \ni \gamma = (1 + p) \rightarrow t = 1 + T \in \Lambda. Take a Dirichlet character \psi : (\mathbb{Z}/Np) \rightarrow W^*, and consider the big ordinary Hecke algebra h (over A) of prime-to-p level N and the character \psi whose definition (including its CM components) will be recalled in the following section. We just mention here the following three facts

1. h is an algebra flat over A interpolating p-ordinary Hecke algebras of level Np^{r+1}, of weight k + 1 \geq 2 and of character \psi^{1-k}\phi for the Teichmüller character \phi, where \phi : \mathbb{Z}_p^* \rightarrow \mu_{p^r}(r \geq 0) and k \geq 1 vary. If N is cube-free, h is a reduced algebra [H13, Corollary 1.3];
2. Each prime P \in \text{Spec}(h) has a unique (continuous) Galois representation \rho_{P} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(K(P)) for the residue field K(P) of P;
3. \rho_{P} restricted to \text{Gal}(\overline{\mathbb{Q}}_{\mathfrak{p}}/\mathbb{Q}_{\mathfrak{p}}) (the p-decomposition group) is isomorphic to an upper triangular representation whose quotient character is unramified.

By (2), each local ring \mathbb{T} has a mod p representation \overline{\rho}_{\mathfrak{m}} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathbb{F}) for the residue field \mathbb{F} = \mathbb{T}/\mathfrak{m}. If \overline{\rho} = \text{Ind}_F^Q \overline{\rho}_{\mathfrak{m}} for the reduction \overline{\rho} modulo p of \phi, we have an involution \sigma \in \text{Aut}(\mathbb{T}/\Lambda) such that \sigma \circ \rho_{P} \cong \rho_{P} \oplus \chi for \chi := (\mathbb{F}/\mathbb{Q}). For a subscheme \text{Spec}(A) \subset \text{Spec}(\mathbb{T}) stable under \sigma, we put A_{\pm} := \{ x \in A | \sigma(x) = \pm x \}. Then A_{\pm} \subset A is a subring and A_{-} is an A_{+}-module.

Let Q be a finite set of rational primes in \mathbb{F}/\mathbb{Q} prime to Np. Let Q^+ be the subset of primes in Q split in F. Write KQ for the ray class field over F of conductor \mathfrak{c} such that \sigma \circ \rho_{P} \cong \rho_{P} \oplus \chi for \chi := (\mathbb{F}/\mathbb{Q}). For a subscheme \text{Spec}(A) \subset \text{Spec}(\mathbb{T}) stable under \sigma, we put A_{\pm} := \{ x \in A | \sigma(x) = \pm x \}. Then A_{\pm} \subset A is a subring and A_{-} is an A_{+}-module.

Theorem B: Let \text{Spec}(\mathbb{T}) be a connected component of \text{Spec}(h) associated to the induced Galois representation \overline{\rho} = \text{Ind}_F^Q \overline{\rho}_{\mathfrak{m}} for the reduction \overline{\rho} modulo p of \phi. Suppose (h0–4) as in Theorem A. Then if the class number of F is prime to p, then, the following four statements are equivalent:

1. The rings \mathbb{T} and \mathbb{T}^+ are both local complete intersections free of finite rank over A.
2. The \mathbb{T}^+ ideal I = \mathbb{T}(\sigma - 1)A \subset \mathbb{T}^+ is principal and generated by a non-zero-divisor \theta \in \mathbb{T}^+ with \theta^2 \in \mathbb{T}^+ \mathbb{T}^+. The element \theta generates a free \mathbb{T}^+ module \mathbb{T}^+ and \mathbb{T}^+=\mathbb{T}^+ is free of rank 2 over \mathbb{T}^+.
3. The Iwasawa module Y^-(\overline{\rho}) is cyclic over W[\Gamma^-].
4. The Iwasawa module Y^-(\overline{\rho} \circ \overline{\chi}) is cyclic over W[\Gamma^-].
The condition \( p \nmid h_F \) could be an analogue of Iwasawa’s assumption \( X_+ = 0 \), and the cyclotomic cyclicity and anti-cyclotomic cyclicity could be closely related (as pointed out to the author by P. Wake). We actually do not assume \( p \nmid h_F \) in the main text and prove a result equivalent (under \( p \nmid h_F \)) to the above theorem (see Theorem 5.4) replacing the assertions (3) and (4) by suitably modified statements, and if the statements for \( T \) fail in this general setting, \( Y^- (\phi) \) for \( \phi = \varphi^-, \varphi^- \omega \) may not be cyclic over \( W[[\Gamma_-]] \). The fact that \( f^- \) in the conjecture is prime to \( p \mathbb{Z}_p [\bar{\phi}][[\Gamma_-]] \) follows from the vanishing of the \( \mu \)-invariant of the anti-cyclotomic Katz \( p \)-adic \( L \)-function \([H10] \) (and \([EAI, \text{Theorem 3.37}] \)) and the proof of the main conjecture by Rubin \([R88] \), \([R91] \), Tilouine \([T89] \), Mazur \([MT90] \) (and the author \([H06] \)).

A slightly stronger and detailed version of Theorem B will be proven as Theorem 5.4 (and Corollary 2.5). The proof of equivalence of the assertion (4) and the rest of Theorem 5.4 relies on a new type of the Taylor–Wiles system argument proving Theorem 4.10 in Section 4 (and on the theory of relative dualizing modules of Grothendieck–Hartshorne–Kleiman recalled in Section 11). The Taylor–Wiles system is made of the deformation rings \( R_Q \) of \( \mathfrak{p} \) and the corresponding local rings \( T_Q \) of the Hecke algebras (of level \( N_Q := N \prod_{q \in Q} q \) ) allowing ramification at primes in \( Q \) (for a suitably chosen finite sequence of sets \( \{ q \} \) the conditions \( q \equiv 1 \mod p ; \) see Section 4 and \([TW95] \)).

Here is a sketch of the proof of the equivalence of \((2) \iff (3)\) in Theorem B. For any commutative ring \( A \), we write \( \text{Frac}(A) \) for the total quotient ring of \( A \) (i.e., \( \text{Frac}(A) \) is the ring of fractions inverting all non-zero-divisors of \( A \)). We simply write \( \mathbb{K} \) for \( \text{Frac}(\mathbb{K}) \) as is well known, under \((h_1)\), \( \text{Frac}(\mathbb{T}) \) can be decomposed as an algebra direct sum \( \text{Frac}(W[[H]]) \oplus X \) in a unique way. Write \( \mathbb{T}_{\text{ncm}} \) for the projected image of \( \mathbb{T} \) in \( X \). Then we have \( I \hookrightarrow \mathbb{T}_{\text{ncm}} \), and via the deformation theoretic technique of Mazur–Tilouine \([MT90] \) (see also \([H16, \text{6.3.6}] \)), we show that \( Y^- (\varphi^-) \otimes_{\mathbb{Z}_p [\bar{\phi}]} W \) is isomorphic to \( J / J^2 \) (by an old formula in \([H86c, \text{Lemma 1.1}] \)). Assume that the class number \( h_F \) of \( F \) is prime to \( p \). Then the projection of \( H \) to \( \Gamma_- \) is an isomorphism. By the proof of the anticyclotomic main conjecture in \([T89] \), \([MT90] \) and \([H06] \), for the Katz \( p \)-adic \( L \)-function \( L_p^- (\varphi^-) \) with branch character \( \varphi^- \) giving the characteristic ideal of \( Y^- (\varphi^-) \), we have \( W[[\Gamma_-]] / (L_p^- (\varphi^-)) \cong \mathbb{T}_{\text{ncm}} / I \) (which also shows that the generator of \( I \) is a non-zero-divisor of \( \mathbb{T}_{\text{ncm}} \)). Since \( I \) is principal generated by a non-zero divisor, we have \( I / I^2 \cong \mathbb{T}_{\text{ncm}} / I \cong W[[\Gamma_-]] / (L_p^- (\varphi^-)) \), getting the anticyclotomic cyclicity conjecture. If \( H \twoheadrightarrow \Gamma_- \) has non-trivial kernel (which implies \( p | h_F \)), Theorem 5.4 tells us that \( Y^- (\varphi^-) \otimes_{\mathbb{Z}_p [\bar{\phi}]} W \) is not cyclic over \( W[[\Gamma_-]] \).

To reach \((2) \iff (4)\) in Theorem B, following the techniques of \([H98] \) and \([CV03] \), we construct an involution \( \sigma \) of \( \mathbb{T} \) (Corollary 2.3). By Taylor–Wiles \([TW95] \), \( \mathbb{T} \) is known to be a local complete intersection over \( \Lambda \) (so, is Gorenstein over \( \Lambda \)). Adding to the data of the Taylor–Wiles system the involution \( \sigma \) coming from the twist by \( \chi = \left( \frac{2 \omega}{\mathfrak{p}} \right) \), we argue in the same way as Taylor and Wiles did. The limit ring \( \mathcal{R} \) (the system produced) is a power series ring over \( \Lambda \) with the induced involution \( \sigma \), and the ring \( \mathcal{R}_+ \) fixed by involution is proven to be Gorenstein. By the theory of dualizing modules/sheaves for Gorenstein covering \( X \twoheadrightarrow Y \) (studied by A. Grothendieck \([SGA 2. VI–V]\), R. Hartshorne \([RDD] \) and S. Kleiman \([K80] \)), this is close to the cyclicity of \( \mathcal{R}_- = \{ x \in \mathcal{R} | \sigma(x) = -x \} \) over \( \mathcal{R}_+ \) (see Lemma 11.4), but we are bit short of proving it. Instead, we prove that the number of generator of \( \mathcal{R}_- \) over \( \mathcal{R}_+ \) is actually given by the number of generators of \( Y^- (\varphi^- \omega) \) over \( W[[\Gamma_-]] \) via a refinement of the original Taylor–Wiles argument. Since \( \mathcal{R}_- = \{ x \in \mathcal{T} | \sigma(x) = -x \} \) is the surjective image of \( \mathcal{R}_- \), it is generated over \( \mathbb{T}_+ = \{ x \in \mathbb{T} | \sigma(x) = x \} \) by a single element which is a generator of \( I \), and essentially \((4) \iff (2)\).

The Gorenstein-ness of the rings \( \mathbb{T}_{\text{ncm}} \) and \( \mathbb{T}_{\text{ncp}} \) (i.e., \((1)\)) implies \((2)\) by Lemma 11.4 in the theory of dualizing modules. The identity \( \mathbb{T}_{\text{ncp}} / (\theta^2) \cong \mathbb{T}_{\text{ncf}} / (\theta^2) \cong W[[H]] / (L_p^- (\varphi^-)) \) tells us that \( \mathbb{T}_{\text{ncp}} \) and \( \mathbb{T}_{\text{ncf}} \) are actually local complete intersections; so, \((2) \Rightarrow (1)\).

The same ring theoretic analysis can be also done for a real quadratic field \( F \), as the conditions \((h_0–4)\) do make sense for real \( F \). We hope to come back to this problem for real quadratic fields in our future work. An example of \( T \neq \Lambda \) given in \([H85] \) is for \( F = \mathbb{Q} (\sqrt{-3}) \), \( p = 13 \) and \( N = 3 \). This prime 13 is an irregular prime for \( \mathbb{Q} (\sqrt{-3}) \) in the sense of \([H82] \) and in the list \([H81, \text{8.11}] \). Of course, as easily checked (from the numerical values given in \([H85] \)) the equivalent conditions of the theorem, and actually (the distinguished factor of) \( L_p^- (\varphi^-) \) is a linear polynomial in this case. The condition \((h_4)\) implies an assumption for “\( R = T \)” theorems of Wiles et al \([Wi95] \) and \([TW95] \):
(W) \( \mathfrak{p} \) restricted to \( \text{Gal}(\overline{Q}/M) \) for \( M = Q[\sqrt{(-1)^{(p-1)/2}p}] \) is absolutely irreducible, and the main reason for us to assume (h4) is the use of the “\( R = T \)” theorem for the minimal deformation ring \( R \) of \( \mathfrak{p} \) (see Theorem 2.1), which we might be able to avoid by scrutinizing our proof more. The condition (W) is equivalent to the condition that the representation \( \mathfrak{p} \) is not of the form \( \text{Ind}^G_{\xi} \) for a character \( \xi : \text{Gal}(\overline{Q}/Q) \to \mathbb{F}^\times \) by Frobenius reciprocity. The implication: (h4) \( \Rightarrow \) (W) follows from [H15, Proposition 5.2]. Actually (W) also follows from the following condition:

(h5) \( \mathfrak{p}^{-1}\mathfrak{p} \) ramifies at a prime factor \( l | N \).

Indeed, if \( \mathfrak{p} = \text{Ind}^G_{\xi} \) for another quadratic field \( K \neq F \), by [H15, Proposition 5.2 (2)], \( KF \) is uniquely determined degree 4 extension of \( Q \) by \( \mathfrak{p} \), and the prime \( l \) in (h5) ramifies in \( KF/F \) as \( \mathfrak{p}|l = \mathfrak{p} \oplus \mathfrak{p} \) for the inertia group \( I_l \subset \text{Gal}(\overline{Q}/Q) \) with unramified \( \mathfrak{p} \). This is impossible if \( K = M \) as only \( p \) ramifies in \( M/Q \). Because of this, in near future, we hope to prove Theorem A assuming (h5) (i.e., \( \epsilon \neq O \)) in place of assuming the order of \( \varphi^- \) has at least 3 (though this latter assumption is used for some other reason than (W) in this paper).

Since \( \mathfrak{p}_{\text{Gal}(\overline{Q}/O_p)} \cong \mathfrak{p} \oplus \mathfrak{p} \) with \( \mathfrak{p} \) unramified, by (h2–3), \( \mathfrak{p} \) has to ramify at \( p \) (as \( F/Q \) is unramified at \( p \)), and hence we conclude

(Rg) \( \mathfrak{p} \neq \mathfrak{p} \),

(Rm) \( \varphi^- \) in Theorems A and B ramifies at \( p \).

Without (Rm), the choice of the \( p \)-unramified quotient \( \mathfrak{p} \) of \( \mathfrak{p} \) is not uniquely determined; so, we have two different universal Hecke rings \( T = T_\tau \) for \( ? = \mathfrak{p} \) or \( \mathfrak{p}^- \) insisting \( \mathfrak{p} \neq ? \) (the problem coming from the existence of companion forms giving rise to the same \( \mathfrak{p} \) but a different unramified quotient \( ? \) assigned). So, \( Y^-(\varphi^-) \otimes \mathbb{Z}_p[\varphi^-] \) \( W \) is not exactly isomorphic to \( I_\tau/I_\tau^2 \) for the ideal \( I_\tau \subset T_\tau \). Here \( I_\tau = I \) as above depends on the choice \( T = T_\tau \). We hope to study this more complicated case carefully in a future article. We freely therefore use (Rg) and (Rm) as we assume (h1–3) and (W) throughout the paper.

Here is a brief outline of the paper. In Section 1, we recall the theory of big ordinary Hecke algebras, paying particular attention to the Hecke algebra \( hQ \) of auxiliary \( Q \)-level used to construct Taylor–Wiles systems and its CM components \( W[\mathbb{H}_Q] \) as their residue rings. In Section 2, we recall the original \( R = T \) theorem proved by Taylor–Wiles, and in Section 3, we recall some technical details of the Taylor–Wiles argument and describe the relation of \( Y^-(\varphi^-) \) and \( R_- \). In Section 4, we prove a sufficient condition for the local intersection property of the subring \( T_\tau \) of \( R = T \) fixed by the involution \( \sigma \), employing the method of Taylor–Wiles adding the datum of the involutions. In the following Section 5, we prove a finer version of Theorem B, applying the result of Section 4 to a residual representation induced from an imaginary quadratic field. In Section 6, we show that the minus part of the cotangent space of \( Q \)-ramified Hecke algebra \( T_Q \) is generated by \( T(q) \) for primes \( q \) in \( Q \) inert in \( F/Q \). By a Selmer group computation, we show that the number \( r_- \) of such inert primes in \( Q \) is equal to the minimum number of generators of \( Y^-(\varphi^-) \) over the Iwasawa algebra. In Section 7, we prove Theorem A, introducing more \( r_- \)-local involutions acting on \( T \). To have such involutions, the choice of generators given in Section 6 (Theorem 6.4) is crucial. These extra involutions fix subring smaller than \( T_\tau \) if \( r_- > 1 \), and studying intricate relations among eigenspaces of the involutions of \( \Omega T/A \), we reach the proof of Theorem A. In Section 8, we show by a control theorem of Rubin that cyclicity (not pseudo cyclic) of \( Y^-(\varphi^-) \) implies cyclicality of the corresponding Iwasawa module for any \( \mathbb{Z}_p \)-extension \( K/F \). In Section 9, we study CM irreducible components when the class number of the CM imaginary quadratic field is divisible by \( p \) and shows that the component is often far larger than the weight Iwasawa algebra \( A \). In Section 10, we explore the close relation of a generator of the ideal \( I \) and the adjoint \( p \)-adic \( L \)-function. In the final section, we gather purely ring theoretic results on Gorenstein local rings and their duality theory used in the proofs of our main results.

Throughout this paper, we write \( \overline{Q} \) (resp. \( \overline{Q}_p \)) for an algebraic closure of \( Q \) (resp. \( Q_p \)) and fix embeddings \( \overline{Q}_p \xrightarrow{\iota_p} \overline{Q} \xrightarrow{\iota_p} \mathbb{C} \). We write \( C_p \) for the \( p \)-adic completion of \( \overline{Q}_p \). A number field is a subfield of \( \overline{Q} \) by a fixed embedding. For each local ring \( A \), we write \( m \) for the maximal ideal of \( A \). For any profinite abelian group \( G \), we write \( W[G] \) for its group algebra, and put \( W[\mathbb{G}] = \varprojlim H W[\mathbb{G}/H] \) for \( H \) running over all open subgroups of \( G \); so, \( W[\mathbb{G}] = W[G] \) is \( G \) is finite.
The author would like to thank R. Greenberg and R. Sharifi. Greenberg pointed out the missing hidden assumption (Rm) of Theorem A in the first draft of this paper by counter-examples presumably exist.Sharifi read the paper carefully and suggested many improvements. The author also appreciates the comments on the results of the paper made by P. Wake.

### Contents

1. Big Hecke algebra  
2. The $R = \mathbb{T}$ theorem and an involution of $R$  
3. The Taylor–Wiles system and Taylor–Wiles primes  
4. A sufficient condition for complete intersection property for $R_+$  
5. Proof of Theorem B  
6. A good choice of generators of $R_Q$ over $W$  
7. Proof of Theorem A and local involutions  
8. Cyclicity for a $\mathbb{Z}_p$-extension $K/F$  
9. Degree of CM components over the Iwasawa algebra  
10. Divisibility of the adjoint $p$-adic L-function  
11. Dualizing modules  
References

### 1. Big Hecke algebra

We recall the theory of $h$ to the extent we need. We assume that the starting prime-to-$p$ level $N$ is as in (h1); in particular, $N$ is cube-free and its odd part is square-free. We assume that the base discrete valuation ring $W$ flat over $\mathbb{Z}_p$ is sufficiently large so that its residue field $\mathbb{F}$ is equal to $\mathbb{T}/m_\mathbb{T}$ for the maximal ideal of the connected component $\text{Spec}(\mathbb{T})$ (of our interest) in $\text{Spec}(h)$.

The base ring $W$ may not be finite over $\mathbb{Z}_p$. For example, if we deal with Katz $p$-adic L-functions, the natural ring of definition is the Witt vector ring $W(\mathbb{F}_p)$ of an algebraic closure $\overline{\mathbb{F}}_p$ (realized in $\mathbb{C}_p$), though the principal ideal generated by a branch of the Katz $p$-adic L-function descends to an Iwasawa algebra over a finite extension $W$ of $\mathbb{Z}_p$ (and in this sense, the reader may assume finiteness over $\mathbb{Z}_p$ of $W$ just to understand our statement as it only depends on the ideal in the Iwasawa algebra over $W$).

We consider the following traditional congruence subgroups

\begin{equation}
\begin{aligned}
\Gamma_0(Np^r) &:= \{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod{Np^r} \}, \\
\Gamma_1(Np^r) &:= \{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(Np^r) \mid d \equiv 1 \pmod{Np^r} \}.
\end{aligned}
\end{equation}

A $p$-adic analytic family $\mathcal{F}$ of modular forms is defined with respect to the fixed embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. We write $|\alpha|_p$ ($\alpha \in \overline{\mathbb{Q}}$) for the $p$-adic absolute value (with $|p|_p = 1/p$) induced by $i_p$. Take a Dirichlet character $\psi : (\mathbb{Z}/Np^r\mathbb{Z})^\times \to W^\times$ with $(p \nmid N, r \geq 0)$, and consider the space of elliptic cusp forms $S_{k+1}(\Gamma_0(Np^{r+1}), \psi)$ with character $\psi$ as defined in [IAT, (3.5.4)].

For our later use, we pick a finite set of primes $Q$ outside $Np$. We define

\begin{equation}
\begin{aligned}
\Gamma_0(Q) &:= \{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod{q} \text{ for all } q \in Q \}, \\
\Gamma_1(Q) &:= \{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(Q) \mid d \equiv 1 \pmod{q} \text{ for all } q \in Q \}.
\end{aligned}
\end{equation}

Let $\Gamma_{Q}^{(p)}$ be the subgroup of $\Gamma_0(Q)$ containing $\Gamma_1(Q)$ such that $\Gamma_0(Q)/\Gamma_{Q}^{(p)}$ is the maximal $p$-abelian quotient of $\Gamma_0(Q)/\Gamma_1(Q) \cong \prod_{q \in Q} (\mathbb{Z}/q\mathbb{Z})^\times$. We put

\begin{equation}
\Gamma_{Q,r} := \Gamma_{Q}^{(p)} \cap \Gamma_0(Np^r),
\end{equation}

and we often write $\Gamma_Q$ for $\Gamma_{Q,r}$ when $r$ is well understood (mostly when $r = 0, 1$). Then we put

\begin{equation}
\Delta_Q := (\Gamma_0(Np^r) \cap \Gamma_0(Q))/\Gamma_{Q,r},
\end{equation}
which is canonically isomorphic to the maximal $p$-abelian quotient of $\Gamma_0(Q)/\Gamma_1(Q)$ independent of the exponent $r$. If $Q = \emptyset$, we have $\Gamma_{Q,r} = \Gamma_0(Np^r)$, and if $q \neq 1 \mod p$ for all $q \in Q$, we have $\Gamma_1(Nq_{p^r}) \subset \Gamma_{Q,r} = \Gamma_0(Nq_{p^r})$ for $N_Q := N \prod_{q \in Q} q$.

Let the ring $\mathbb{Z}[\psi] \subset \mathbb{C}$ and $\mathbb{Z}_p[\psi] \subset \mathbb{Q}_p$ be generated by the values $\psi$ over $\mathbb{Z}$ and $\mathbb{Z}_p$, respectively. The Hecke algebra over $\mathbb{Z}[\psi]$ is the subalgebra of the $\mathbb{C}$-linear endomorphism algebra of $S_{k+1}(\Gamma_{Q,r}, \psi)$ generated over $\mathbb{Z}[\psi]$ by Hecke operators $T(n)$:

$$h = \mathbb{Z}[\psi][T(n)|n| = 1, 2, \ldots] \subset \text{End}_\mathbb{C}(S_{k+1}(\Gamma_{Q,r}, \psi)),$$

where $T(n)$ is the Hecke operator as in [IAT, §3.5]. We put

$$h_{Q,k,\psi/W} = h_{k}(\Gamma_{Q,r}, \psi; W) := h \otimes_{\mathbb{Z}[\psi]} W.$$

Here $h_{k}(\Gamma_{Q,r}, \psi; W)$ acts on $S_{k+1}(\Gamma_{Q,r}, \psi; W)$ which is the space of cusp forms defined over $W$ (under the rational structure induced from the $q$-expansion at the infinity cusp; see, [MFG, §3.1.8]). More generally for a congruence subgroup $\Gamma$ containing $\Gamma_1(Np^r)$, we write $h_k(\Gamma, \psi; W)$ for the Hecke algebra on $\Gamma$ with coefficients in $W$ acting on $S_{k+1}(\Gamma, \psi; W)$. The algebra $h_k(\Gamma, \psi; W)$ can be also realized as $W[T(n)|n| = 1, 2, \ldots] \subset \text{End}_W(S_{k+1}(\Gamma, \psi; W))$. When we need to indicate that our $T(l)$ is the Hecke operator of a prime factor $l$ of $Np^r$, we write it as $U(l)$, since $T(l)$ acting on a subspace $S_{k+1}(\Gamma_{0}(N'), \psi) \subset S_{k+1}(\Gamma_{0}(Np^r), \psi)$ of level $N' | Np$ prime to $l$ does not coincide with $U(l)$ on $S_{k+1}(\Gamma_{0}(Np^r), \psi)$. The ordinary part $h_{Q,k,\psi/W} \subset h_{Q,k,\psi/W}$ is the maximal ring direct summand on which $U(p)$ is invertible. If $Q = \emptyset$, we simply write $h_{k,\psi/W}$ for $h_{Q,k,\psi/W}$. We write $e$ for the idempotent of $h_{Q,k,\psi/W}$, and hence $e = \lim_{n \to \infty} U(p)^n$ under the $p$-adic topology of $h_{Q,k,\psi/W}$. The idempotent $e$ not only acts on the space of modular forms with coefficients in $W$ but also on the classical space $S_{k+1}(\Gamma_{1}, \psi)$ (as $e$ descends from $S_{k+1}(\Gamma_{0}(\psi), \psi_{\mathbb{Q}_p})$ to $S_{k+1}(\Gamma_{1}, \psi, \mathbb{Q}_p)$). We write the image $M_{\text{ord}} := e(M)$ of the idempotent attaching the superscript “ord” (e.g., $S_{k,\text{ord}}$).

Fix a character $\psi_0$ modulo $Np$, and assume now $\psi_0(-1) = -1$. Let $\omega$ be the modulo $p$ Teichmüller character. Recall the multiplicative group $\Gamma := 1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ and its topological generator $\gamma = 1 + p$. Then the Iwasawa algebra $\Lambda = W[[\Gamma]] = \lim_{n \to \infty} W[T/T^{p^n}]$ is identified with the power series ring $W[[T]]$ by a $W$-algebra isomorphism sending $\gamma \in \Gamma$ to $t := 1 + T$. As constructed in [H86a], [H86b] and [GME], we have a unique ‘big’ ordinary Hecke algebra $h^\Omega$ (of level $\Gamma_{1,\infty}$). We write $h$ for $h^\Omega$.

Since $Np = DN_{F/Q}(\epsilon)p \geq Dp > 4$, the algebra $h^\Omega$ is characterized by the following two properties (called Control theorems; see [H86a] Theorem 3.1, Corollary 3.2 and [H86b, Theorem 1.2] for $p \geq 5$ and [GME, Corollary 3.2.22] for general $p$):

(C1) $h^\Omega$ is free of finite rank over $\Lambda$ equipped with $T(n) \in h^\Omega$ for all $1 \leq n \in \mathbb{Z}$ prime to $Np$ and $U(l)$ for prime factors $l$ of $Np$,

(C2) if $k \geq 1$ and $\epsilon : \mathbb{Z}_p^\times \to \mu_{p^\infty}$ is a finite order character,

$$h^\Omega/(t - \epsilon(\gamma)\gamma^k)h^\Omega \cong h_{Q,k,\psi_{\omega^k}}(\gamma = 1 + p)$$

for $\psi_k := \psi_0\omega^{-k}$, sending $T(n)$ to $T(n)$ (and $U(l)$ to $U(l)$ for $l | Np$).

Actually a slightly stronger fact than (C1) is known:

**Lemma 1.1.** The Hecke algebra $h^\Omega$ is flat over $\Lambda[\Delta_Q]$ with $h^\Omega/\mathfrak{a}_{\Delta_Q}h^\Omega \cong h^\Omega$ for the augmentation ideal $\mathfrak{a}_{\Delta_Q} \subset \Lambda[\Delta_Q]$.

See [H89, Lemma 3.10] and [MFG, Corollary 3.20] for a proof. Hereafter, even if $k \leq 0$, abusing the notation, we put $h_{Q,k,\psi_{\omega^k}} := h^\Omega/(t - \epsilon(\gamma)\gamma^k)h^\Omega$ which acts on $p$-ordinary $p$-adic cusp forms of weight $k$ and of Neben character $\psi_{\omega^k}$. By the above lemma, $h_{Q,k,\psi_{\omega^k}}$ is free of finite rank $d$ over $W[\Delta_Q]$ whose rank over $W[\Delta_Q]$ is equal to rank$_k h_{Q,k,\psi_{\omega^k}}$ (independent of $Q$).

Since $N_Q$ is cube-free, by [H13, Corollary 1.3], $h^\Omega$ is reduced. Let $\text{Spec}(\mathbb{I})$ be an irreducible component of $\text{Spec}(h^\Omega)$. Write $a(n)$ for the image of $T(n)$ in $\mathbb{I}$ (so, $a(p)$ is the image of $U(p)$). If a point $P$ of $\text{Spec}(\mathbb{I})$ kills $(t - \epsilon(\gamma)\gamma^k)$ with $1 \leq k \in \mathbb{Z}$ (i.e., $P((t - \epsilon(\gamma)\gamma^k)) = 0$), we call $P$ an arithmetic point, and we write $\epsilon_P := \epsilon$, $k(P) := k \geq 1$ and $p^{r(P)}$ for the order of $\epsilon_P$. If $P$ is arithmetic, by (C2), we have a Hecke eigenform $f_P \in S_{k+1}(\Gamma_{Q,r}, \omega^k)$ such that its eigenvalue for $T(n)$ is given by $a_P(n) := P(a(n)) \in \mathbb{Q}$ for all $n$. Thus $\mathbb{I}$ gives rise to a family $\mathcal{F} = \{f_P|\text{arithmetic } P \in \text{Spec}(\mathbb{I})\}$ of Hecke eigenforms. We define a $p$-adic analytic family of slope
0 (with coefficients in $\mathbb{L}$) to be the family as above of Hecke eigenforms associated to an irreducible component $\text{Spec}(\mathbb{L}) \subset \text{Spec}(\mathbb{H}_Q)$. We call this family slope 0 because $|a_p(p)| = 1$ for the $p$-adic absolute value $|\cdot|_p$ of $\mathbb{Q}_p$ (it is also often called an ordinary family). This family is said to be analytic because the Hecke eigenvalue $a_p(n)$ for $T(n)$ is given by an analytic function $a(n)$ on (the rigid analytic space associated to) the $p$-profinite formal spectrum $\Spf(\mathbb{L})$. Identify $\text{Spec}(\mathbb{L})(\mathbb{Q}_p)$ with $\text{Hom}_W(\mathbb{L}, \mathbb{Q}_p)$ so that each element $a \in \mathbb{L}$ gives rise to a “function” $a : \text{Spec}(\mathbb{L})(\mathbb{Q}_p) \to \mathbb{Q}_p$ whose value at $(P : \mathbb{L} \to \mathbb{Q}_p) \in \text{Spec}(\mathbb{L})(\mathbb{Q}_p)$ is $a_{P} := a(P) \in \mathbb{Q}_p$. Then $a$ is an analytic function of the rigid analytic space associated to $\Spf(\mathbb{L})$. Taking a finite covering $\text{Spec}(\overline{\mathbb{L}})$ of $\text{Spec}(\mathbb{L})$ with surjection $\text{Spec}(\overline{\mathbb{L}})(\mathbb{Q}_p) \to \text{Spec}(\mathbb{L})(\mathbb{Q}_p)$, abusing slightly the definition, we may regard the family $\mathcal{F}$ as being indexed by arithmetic points of $\text{Spec}(\overline{\mathbb{L}})(\mathbb{Q}_p)$, where arithmetic points of $\text{Spec}(\overline{\mathbb{L}})(\mathbb{Q}_p)$ are made up of the points above arithmetic points of $\text{Spec}(\mathbb{L})(\mathbb{Q}_p)$. The choice of $\overline{\mathbb{L}}$ is often the normalization of $\mathbb{L}$ or the integral closure of $\mathbb{L}$ in a finite extension of the quotient field of $\mathbb{L}$.

Each irreducible component $\text{Spec}(\mathbb{L}) \subset \text{Spec}(\mathbb{H}_Q)$ has a 2-dimensional semi-simple (actually absolutely irreducible) continuous representation $\rho_{\ell}$ of $\text{Gal}(\mathbb{Q}/\mathbb{Q})$ with coefficients in the quotient field of $\mathbb{L}$ (see [H86b]). The representation $\rho_{\ell}$ restricted to the $p$-decomposition group $D_p$ is reducible with unramified quotient character (e.g., [GME, §4.2]). As is well known now (e.g., [GME, §4.2]), $\rho_{\ell}$ is unramified outside $N_{Q\mathbb{P}}$ and satisfies

$$\text{Tr}(\rho_{\ell}(\text{Frob}_l)) = a(l) (l \not\equiv 1 \pmod{N_{Q\mathbb{P}}}) \quad \rho_{\ell}([p, Q_p]) \sim \left( \begin{array}{cc} p^s & 0 \\ 0 & \bar{\nu}_l \end{array} \right) \left( \begin{array}{cc} \alpha & 0 \\ 0 & \beta \end{array} \right),$$

where $p^s = (1 + p)^s = \prod_{n=0}^{\infty} (s_n p^n) \in \mathbb{Z}_p^\times$ for $s \in \mathbb{Z}_p$ and $[x, Q_p]$ is the local Artin symbol. As for primes in $q \in \mathbb{Q}$, if $q \equiv 1 \pmod{p}$ and $\mathfrak{p} \supseteq q \mathbb{P}$ has two distinct eigenvalues, we have

$$\rho_{\ell}([z, Q_q]) \sim \left( \begin{array}{cc} \alpha & 0 \\ 0 & \beta \end{array} \right)$$

with characters $\alpha_q$ and $\beta_q$ of $Q_q^\times$ for $z \in Q_q^\times$, where one of $\alpha_q$ and $\beta_q$ is unramified (e.g., [MFG, Theorem 3.32 (2)] or [HMI, Theorem 3.75]). For each prime ideal $P$ of $\text{Spec}(\mathbb{L})$, writing $\kappa(P)$ for the residue field of $P$, we also have a semi-simple Galois representation $\rho_{\ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\kappa(P))$ unramified outside $N_{Q\mathbb{P}}$ such that $\text{Tr}(\rho_{\ell}(\text{Frob}_l))$ is given by $a(l)_{P}$ for all primes $l \not\equiv 1 \pmod{N_{Q\mathbb{P}}}$. If $P$ is the maximal ideal $\mathfrak{m}_1$, we write $\overline{\mathfrak{m}}$ for $\rho_{\ell}$ which is called the residual representation of $\rho_{\ell}$. The residual representation $\overline{\mathfrak{m}}$ is independent of $\mathfrak{m}$ as long as $\mathfrak{m}$ belongs to a given connected component $\text{Spec}(\mathfrak{m})$ of $\text{Spec}(\mathbb{H}_Q)$. Indeed, $\text{Tr}(\rho_{\ell}) \mod \mathfrak{m}_1 = \text{Tr}(\overline{\mathfrak{m}})$ for any $\mathfrak{m} \in \text{Spec}(\mathfrak{m})$. If $P$ is an arithmetic prime, we have $\det(\rho_{\ell}) = \epsilon_P \psi_P \epsilon_P^{k}$ for the $p$-adic cyclotomic character $\psi_P$ (regarding $\epsilon_P$ and $\psi_P$ as Galois characters by class field theory). This is the Galois representation associated to the Hecke eigenform $f_P$ (constructed earlier by Shimura and Deligne) if $P$ is arithmetic (e.g., [GME, §4.2]).

A component $\mathfrak{L}$ is called a CM component if there exists a nontrivial character $\chi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times$ such that $\rho_{\ell} \cong \rho_{\ell} \otimes \chi$. We also say that $\mathfrak{L}$ has complex multiplication if $\mathfrak{L}$ is a CM component. In this case, we call the corresponding family $\mathcal{F}$ a CM family (or we say that $\mathcal{F}$ has complex multiplication). If $\mathcal{F}$ is a CM family associated to $\mathfrak{L}$ with $\rho_{\ell} \cong \rho_{\ell} \otimes \chi$, then $\chi$ is a quadratic character of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which cuts out an imaginary quadratic field $F$, i.e., $\chi = \left( \frac{F/\mathbb{Q}}{\cdot} \right)$. Write $\overline{\mathfrak{L}}$ for the integral closure of $\Lambda$ inside the quotient field of $\mathfrak{L}$. The following three conditions are known to be equivalent:

(CM1) $\mathcal{F}$ has CM with $\rho_{\ell} \cong \rho_{\ell} \otimes \left( \frac{\overline{\mathfrak{L}}/\mathbb{L}}{\cdot} \right)$ (\(\Leftrightarrow \rho_{\ell} \cong \text{Ind}_{\mathfrak{L}}^{\overline{\mathfrak{L}}} \lambda \) for a character $\lambda : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times$);

(CM2) For all arithmetic $P$ of $\text{Spec}(\overline{\mathfrak{L}})(\mathbb{Q}_p)$, $f_P$ is a binary theta series of the norm form of $F/\mathbb{Q}$;

(CM3) For some arithmetic $P$ of $\text{Spec}(\overline{\mathfrak{L}})(\mathbb{Q}_p)$, $f_P$ is a binary theta series of the norm form of $F/\mathbb{Q}$. Indeed, (CM1) is equivalent to $\rho_{\ell} \cong \text{Ind}_{\mathfrak{L}}^{\overline{\mathfrak{L}}} \lambda$ for a character $\lambda : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Frac}(\mathbb{L})^\times$ unramified outside $N_{\mathbb{P}}$ (e.g., [DH98, Lemma 3.2] or [MFG, Lemma 2.15]). Since the characteristic polynomial of $\rho_{\ell}(\sigma)$ has coefficients in $\mathfrak{L}$, its eigenvalues fall in $\overline{\mathfrak{L}}$; so, the character $\lambda$ has values in $\overline{\mathfrak{L}}$ (see, [H86c, Corollary 4.2]). Then by (Gal), $\lambda_P = P \circ \lambda : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Q}_p$ for an arithmetic $P$ in $\text{Spec}(\overline{\mathfrak{L}})(\mathbb{Q}_p)$ is a locally algebraic $p$-adic character, which is the $p$-adic avatar of a Hecke character $\lambda_P : F_\mathfrak{L}^\times/F_\mathfrak{L}^\times \to \mathbb{C}^\times$ of type $A_0$ of the quadratic field $F_\mathfrak{L}$. Then by the characterization (Gal) of $\rho_{\ell}$, $f_P$ is the theta series with $q$-expansion $\sum a \lambda_P(a) q^{N(a)}$, where $a$ runs over all integral ideals of $F$. By $k(P) \geq 1$ (and (Gal)), $F$ has to be an imaginary quadratic field in which $p$ is split (as holomorphic binary theta series of real quadratic field are limited to weight $1 \Rightarrow k = 0$; cf.,
This shows (CM1) ⇒ (CM2) ⇒ (CM3). If (CM2) is satisfied, we have an identity 
\[ \text{Tr}(\rho_l(Frob_l)) = a(l) = (l)(\chi(l)) = \text{Tr}(\rho_l \otimes \chi(Frob_l)) \]
with \( \chi = \left( F/Q \right) \) for all primes \( l \) except \( Np \). By Chebotarev density, we have \( \text{Tr}(\rho_l) = \text{Tr}(\rho_l \otimes \chi) \), and we get (CM1) from (CM2) as \( \rho_l \) is semi-simple.

If a component \( \text{Spec}(\mathcal{I}) \) contains an arithmetic point \( P \) with theta series \( \varphi_p \) as above of \( F/Q \), either \( \mathcal{I} \) is a CM component or otherwise \( P \) is in the intersection in \( \text{Spec}(h^Q) \) of a component \( \text{Spec}(\mathcal{I}) \) not having CM by \( F \) and another component having CM by \( F \) (as all families with CM by \( F \) are made up of theta series of \( F \) by the construction of CM components in [HS6a, §7]). The latter case cannot happen as two distinct components never cross at an arithmetic point in \( \text{Spec}(h^Q) \) (i.e., the reduced part of the localization \( h^Q \) is étale over \( \Lambda_p \) for any arithmetic point \( P \in \text{Spec}(\Lambda)(\overline{\mathbb{Q}}_p) \); see [HMI, Proposition 3.78]). Thus (CM3) implies (CM2). We call a binary theta series of the norm form of an imaginary quadratic field a CM theta series.

We describe how to construct residue rings of \( h^Q \) whose Galois representations are induced from a quadratic field \( F \) (see [LFE, §7.6] and [HMI, §2.5.4]). Here \( F \) is either real or imaginary. We write \( c \) for the generator of \( \text{Gal}(F/Q) \) (even if \( F \) is real). Let \( c \) be the prime-to-\( p \) conductor of a character \( \varphi \) as in Theorem B in the introduction (allowing real \( F \)). Put \( c = \mathfrak{c} \cap c' \). By (h1), \( c \) is a square free integral of \( F \) with \( c + c' = O \) (for complex conjugation \( c \)). Since \( Q \) is outside \( N \), \( Q \) is a finite set of rational primes unramified in \( F/Q \) prime to \( \mathfrak{c}p \). Let \( Q^+ \) be the subset in \( Q \) made up of primes split in \( F \). We choose a prime factor \( q \) of \( q \) for each \( q \in Q^+ \) (once and for all), and put \( \Omega^+ := \prod_{q \in Q^+} q \). We study some ray class groups isomorphic to \( h \). We put \( \mathfrak{e}Q := \mathfrak{e} \prod_{q \in Q^+} q \). We simply write \( \mathfrak{e} \mathfrak{c} \) for \( \mathfrak{c} \mathfrak{e} \mathfrak{c} \). Consider the ray class group \( Cl(\mathfrak{a}) \) (of \( F \)) modulo \( \mathfrak{a} \) for an integral ideal \( \mathfrak{a} \) of \( O \), and put

\[
Cl(c\Omega^+p^\infty) = \lim_{\mathfrak{a}} Cl(c\Omega^+p^\infty), \quad \text{and} \quad Cl(\mathfrak{c}Q^+p^\infty) = \lim_{\mathfrak{a}} Cl(\mathfrak{c}Q^+p^\infty).
\]

On \( Cl(\mathfrak{c}Q^+p^\infty) \), complex conjugation \( c \) acts as an involution.

Let \( Z_{Q^+} \) (resp. \( 3_{Q^+} \)) be the maximal \( p \)-profinite subgroup (and hence quotient) of \( Cl(c\Omega^+p^\infty) \) (resp. \( Cl(\mathfrak{c}Q^+p^\infty) \)). We write \( Z \) (resp. \( 3 \)) for \( Z_{Q^+} \) (resp. \( 3_{Q^+} \)). We have the finite level analogue \( C_{Q^+} \), which is the maximal \( p \)-profinite subgroup (and hence quotient) of \( Cl(c\Omega^+p^\infty) \). We have a natural map of \( (O_{cQ}^\times \times O_{cQ}^\times) \) into \( Cl(\mathfrak{c}Q^+p^\infty) = \lim_{\mathfrak{a}} Cl(\mathfrak{c}Q^+p^\infty) \) (with finite kernel). Let \( Z_{Q^+} = 3_{Q^+}/3_{Q^+}^1 \) (the maximal quotient on which \( c \) acts by \( -1 \)). We have the projections

\[
\pi : 3_{Q^+} \to Z_{Q^+} \quad \text{and} \quad \pi^{-} : 3_{Q^+} \to Z_{Q^+}^-
\]

Recall \( p > 3 \); so, the projection \( \pi^- \) induces an isomorphism \( 3_{Q^+}^{-} = \{ z^{-1}z \mid z \in 3_{Q^+} \} \to Z_{Q^+}^- \). Thus \( \pi^- \) induces an isomorphism between the \( p \)-profinite groups \( Z_{Q^+} \) and \( 3_{Q^+}^{-} \). Similarly, \( \pi \) induces

\[
\pi : 3_{Q^+}^{-} \cong Z_{Q^+}^{-}
\]

Thus we have for the Galois group \( H \) as in the introduction

\[
i : Z_{Q^+}^{-} \cong Z_{Q^+}^{-} \cong H
\]

by first lifting \( z \in Z_{Q^+} \) to \( \bar{z} \in 3_{Q^+}^{-} \) and taking its square root and then project down to \( \pi^- \left( \bar{z}^{1/2} \right) = \bar{z}^{-1} \). Here the second isomorphism \( Z_{Q^+}^- \cong H \) is by Artin symbol of class field theory. The isomorphism \( \iota \) identifies the maximal torsion free quotients of the two groups \( Z_{Q^+} \) and \( Z_{Q^+}^- \) which we have written as \( \Gamma_- \). This \( \iota \) also induces \( W \)-algebra isomorphism \( W[[Z_{Q^+}]] \cong W[[Z_{Q^+}^-]] \) which is again written by \( \iota \).

Let \( \varphi \) be the Teichmüller lift of \( \varphi \) as in Theorem B. Recall \( N = N_{F/Q}(\varphi)D \). Then we have a unique continuous character \( \Phi : \text{Gal}(\overline{\mathbb{Q}}/F) \to W[[Z_{Q^+}]] \) characterized by the following two properties:

1. \( \Phi \) is unramified outside \( e\Omega^+p \),
2. \( \Phi(Frob_p) = \varphi(Frob_p)[l] \) for each prime \( l \) outside \( Np \) and \( \Omega^+ \), where \( [l] \) is the projection to \( Z_{Q^+} \) of the class of \( l \) in \( Cl(c\Omega^+p^\infty) \).

When \( F \) is real, all groups \( Z_{Q^+} \), \( Z_{Q^+}^- \) and \( H \) are finite groups; so, \( W[[Z_{Q^+}]] = W[[Z_{Q^+}^-]] \) for example. The character \( \Phi \) is uniquely determined by the above two properties because of Chebotarev density. We can prove the following result in the same manner as in [H86c, Corollary 4.2]:

**Theorem 1.2.** Suppose that \( \varphi(Frob_q) \neq \varphi(Frob_{q'}) \) for all \( q|\Omega^+ \). Then we have a surjective \( \Lambda \)-

\[ h^Q : W[[Z_{Q^+}]] \to W[[Z_{Q^+}]] \quad \text{such that} \]
If \( F \) is real, the above homomorphism factors through the weight 1 Hecke algebra \( h^{Q^+}/(p^m - 1)h^{Q^+} \) for a sufficiently large \( m \geq 0 \).

The last point of the morphism factoring through the weight 1 Hecke algebra is because theta series of a real quadratic field are limited to weight 1.

Note that out of a Hecke eigenform \( f(z) \in S_{k+1}(\Gamma_0(N_{Q^+}p^r),\phi) \) with \( f(T)(q) = a_f q \) for \( q \notin Q^+ \) and two roots \( \alpha, \beta \) of \( X^2 - a_q X + \phi(q)q^k = 0 \), we can create two Hecke eigenforms \( f_\alpha = f(z) - \beta f(qz) \) and \( f_\beta = f(z) - \alpha f(qz) \) of level \( N_{Q^+}q \) with \( f_\alpha|U(q) = x f_x \) for \( x = \alpha, \beta \). This tells us that if we choose a set \( \Sigma^- := \{ \varpi_q | q \in Q^- \} \) of mod \( p \) eigenvalues of \( \pi(Frob_q) \) for \( q \in Q^- := Q - Q^+ \), we have a unique local ring \( T^Q \) of \( h^Q \) and a surjective algebra homomorphism \( T^Q \to W[[Z_{Q^+}]] \) factoring through \( h^{Q^+} \to W[[Z_{Q^+}]] \) such that \( U(q) \mod m_{\varpi_q} = \varpi_q \) for all \( q \in Q^- \). For \( q \in Q^- \), if \( f \) is a theta series of \( F \), we have \( a_\varrho = 0 \); so, the residual class (modulo \( m_{\varpi_q} \)) of \( \alpha \) and \( \beta \) in \( \mathbb{Z}_p[\alpha, \beta] \subset \mathbb{Z}_p \) are distinct (because of \( p > 2 \)). Therefore if we change \( \Sigma^- \), the local ring \( T^Q \) will be changed accordingly. We record this fact as

**Corollary 1.3.** Suppose that \( \pi(Frob_q) \neq \pi(Frob_q') \) for all \( q|\Omega^+ \) and that \( W \) is sufficiently large so that we can choose a set \( \Sigma^- := \{ \varpi_q | q \in Q^- \} \) of mod \( p \) eigenvalues of \( \pi(Frob_q) \) for \( q \in Q^- := Q - Q^+ \) in the residue field \( \mathbb{F} \) of \( W \). Then we have a unique local ring \( T^Q \) of \( h^Q \) such that we have a surjective \( \Lambda \)-algebra homomorphism \( T^Q \to W[[Z_{Q^+}]] \) characterized by the following conditions:

1. \( T(l) \to \Phi(l) + \Phi(l') \) if \( l = ll' \) with \( l \neq l' \) and \( l \nmid N_{Q^+}p \);
2. \( T(l) \to 0 \) if \( l \) remains prime in \( F \) and is prime to \( N_{Q^+} \);
3. \( U(q) \to \Phi(q^\gamma) \) if \( q|\Omega^+ \);
4. \( U(p) \to \Phi(p^\gamma) \).

If \( F \) is real, the above homomorphism factors through the weight 1 Hecke algebra \( T^Q/(t^{p^m} - 1)T^Q \) for a sufficiently large \( m \geq 0 \).

We will later show that the quotient \( T^Q \to W[[Z_{Q^+}]] \) constructed above is the maximal quotient such that the corresponding Galois representation is induced from \( F \) under \( (h0-4) \) (see Proposition 2.6). Hereafter, more generally, fixing an integer \( k \geq 0 \) and the set \( \Sigma^- := \{ \varpi_q \in \mathbb{F} | q \in Q^- \} \), we put

\[
T_Q = T^Q/(t - \gamma)^{mQ}.
\]

The choice of \( q|\Omega^+ \) can be also considered to be the choice \( \Sigma^+ := \{ \varpi_q(Frob_q') \in \mathbb{F} : q|\Omega^+ \} \) of the eigenvalue of \( U(q) \). Thus the local rings \( T^Q \) and \( T_Q \) are considered to be defined with respect to the choice \( \Sigma = \Sigma^+ \cup \Sigma^- \) of one of the mod \( p \) eigenvalues of \( U(q) \) for each \( q \in Q \). In other words, \( T_Q \) is a local factor of \( h_{Q,k,\psi} \) with the prescribed mod \( p \) eigenvalues \( \Sigma = \varpi_q(Frob_q') \) for \( q \in Q \). Note that \( T_Q \) is classical if \( k \geq 1 \) but otherwise, it is defined purely \( p \)-adically. In the above corollary, we took \( k = 0 \) when \( F \) is real.

Assume that \( F \) is imaginary. In this case, we need later a rapid growth assertion of the group \( H_Q \) and the group ring \( W[[H_Q]] \) if we vary \( Q \) suitably. This growth result we describe now. We fix a positive integer \( r_+ \) and choose an infinite set \( Q^+ = \{ \Omega^+_m | m = 1, 2, \ldots \} \) of \( r_+ \)-sets of primes \( q \) of \( O \) such that \( N(q) \equiv 1 \mod p^m \). We assume that \( \Omega^+_m \) is made of primes split in \( F/\mathbb{Q} \) outside \( cp \) and that \( q \mapsto q \cap \mathbb{Z} \) induces a bijection between \( \Omega^+_m \) and \( Q^+_m := \{ q \cap \mathbb{Z} | q \in \Omega^+_m \} \). We regard \( Q^+_m \) as a set of rational primes. We write \( \Omega^+_m \) sometimes for the product \( \prod_{q \in Q^+_m} \mathbb{Z}/q \). The inclusion \( \mathbb{Z} \to O \) induces a natural isomorphism \( \prod_{q \in Q^+_m} \mathbb{Z}/q \to (O/\Omega^+_m)^x \). We identify the two groups by this isomorphism, and write \( \Delta_{Q^+_m} \) for the \( p \)-Sylow subgroup of this group. Then \( \Delta_{Q^+_m} \) is the product over \( q \in Q^+_m \) of the \( p \)-Sylow subgroup \( \Delta_q \equiv \Delta_q \) of \( (O/Q)^x \equiv (\mathbb{Z}/q\mathbb{Z})^x \). For the ray class group \( CL(\Omega^+_m, p^n) \), we have a natural exact sequence of abelian groups

\[
(O/\Omega^+_m)^x \to CL(\Omega^+_m, p^n) \to CL(p^n) \to 1,
\]
which induces the exact sequence of its maximal $p$-abelian quotients:

$$1 \rightarrow \Delta_{Q^+} \rightarrow Cl((\zeta_m^+)^n)_p \rightarrow Cl(\zeta^n)_p \rightarrow 1,$$

since the order of the finite group $\text{Ker}(i)$ is prime to $p$ (as $p > 3$). Passing to the projective limit with respect to $n$, we have an exact sequence of compact modules

$$(1.8) \quad 1 \rightarrow \Delta_{Q^+} \rightarrow Z_{Q^+} \rightarrow Z_\emptyset \rightarrow 1.$$ 

We consider the group algebra $W[[Z_{Q^+}^+]]$ which is an algebra over $W[\Delta_{Q^+}]$. We choose a generator $\delta_q$ of the cyclic group $\Delta_q$ and put $\Delta_q^+$ to be the quotient of $\Delta_{Q^+}$ by the subgroup generated by $\{\delta_q^n\}_{q \in Q^+}$ for $0 < n \leq m$; thus, $\Delta_q^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^*$. This include the ordering $Q^+_m = \{q_1, \ldots, q_r\}$ so that the above isomorphism sends $\Delta_q^+ / (\delta_q^n)$ to the $j$-th factor $\mathbb{Z}/p^n\mathbb{Z}$. In this way, we fix the identification of $\Delta_n^+$ with $(\mathbb{Z}/p^n\mathbb{Z})^*$ for all $n$ and $m$ once and for all. Thus, writing $W_n := W/p^nW$, we get a projective system

$$\{W_n[\Delta_n^+] \cong W_n[(\mathbb{Z}/p^n\mathbb{Z})^*]\}_{n > 0}$$

sending $(\mathbb{Z}/p^n\mathbb{Z})^* \ni x \mapsto (x \mod p^n) \in (\mathbb{Z}/p^n\mathbb{Z})^*$ for all $n$. We then have

$$W[[S_1, \ldots, S_r]] \cong \lim_{\rightarrow} W_n[\Delta_n^+]$$

sending $s_j = 1 + S_j$ to the image of $\delta_{q_j}$ in $\Delta_n^+$ for all $j$, $q_j \in Q^+_m$ and $m \geq n$.

Assuming that $F$ has class number prime to $p$, the natural isomorphism $\mathbb{Z}_p^\times \cong O_F^\times$ induces a group morphism $\mathbb{Z}_p^\times \rightarrow Cl(\zeta^n)$, which induces an isomorphism $\Gamma = 1 + p\zeta_p \cong \emptyset$. Then we can canonically split exact sequence (1.8) so that $Z_{Q^+_m} = \Delta_{Q^+_m} \times \Gamma$, making the following diagram commutative for all $m' \geq n' > n$ with $m \geq n$:

$$\begin{array}{c}
W_n[\Delta_n^+] \cong W_n[(\mathbb{Z}/p^n\mathbb{Z})^*] & \xrightarrow{\pi_n^*} & W_n[[\emptyset]] \\
\downarrow & & \downarrow \text{onto} \\
W_n[[\Gamma]][\Delta_n^+] \cong W_n[(\mathbb{Z}/p^n\mathbb{Z})^*] & \xrightarrow{\pi_n^*} & W_n[[\emptyset]],
\end{array}$$

where $\mathfrak{A}_n := (p^n, s_j p^n - 1)_{j=1,2,\ldots,r_q}$ as an ideal of $W[[S_1, \ldots, S_r]]$. In this way, we get a (bit artificial) projective system

$$\{W[[Z_{Q^+_m}^+]] / \mathfrak{A}_n \xrightarrow{\pi_n^*} W[[Z_{Q^+_m}^+]] / \mathfrak{A}_n \}_{n' > n}.$$ 

By this map, $W[[Z_{Q^+_m}^+]] / \mathfrak{A}_n$ is naturally a $\Lambda$-algebra via the canonical splitting $Z_{Q^+_m} = \Delta_{Q^+_m} \times \emptyset$, and hence a $\Lambda[[S_1, \ldots, S_r]]$-algebra. Since $\emptyset = \Gamma$, we get $\lim_{\rightarrow} W[[Z_{Q^+_m}^+]] / \mathfrak{A}_n \cong \Lambda[[S_1, \ldots, S_r]]$. We thus conclude

**Proposition 1.4.** Assume that $F$ is imaginary with class number prime to $p$. Identify $H_{Q^+_m}$ with $Z_{Q^+_m}$ by (1.6) (whence $\mathfrak{A}_n$ is the ideal of $W[[H_{Q^+_m}]]$). Then the limit ring $\lim_{\rightarrow} W[[H_{Q^+_m}]] / \mathfrak{A}_n$ is isomorphic to $\Lambda[[S_1, \ldots, S_r]]$.

This follows from the above argument, after identifying $Z_{Q^+_m}$ with $H_{Q^+_m}$ and identifying $\Lambda$ with $W[[\Gamma^-]]$.

We now explore the case where the class number of $F$ is divisible by $p$. In this case, we again study the set $\Omega^+$ of $r_q$-sets $\Omega^+_m$ of split primes in $F$ outside $N$ such that $N(q) \equiv 1 \mod p^m$ with $Q^+_m := \{(q) = q \cap \mathbb{Z}|q \in \Omega^+_m\}$ with an ordering. We still have the following exact sequence (1.8):

$$1 \rightarrow \Delta_{Q^+_m} \rightarrow Z_{Q^+_m} \xrightarrow{\pi_{Q^+_m}^*} Z_\emptyset \rightarrow 1.$$ 

Write $Z_{tor}$ for the maximal torsion subgroup of $Z_\emptyset$, and fix a splitting $Z_\emptyset = \Gamma_F \times Z_{tor}$ with a torsion-free group $\Gamma_F$. The projection $\pi_{Q^+_m}$ identifies the maximal torsion-free quotient of $Z_{Q^+_m}$ with $\Gamma_F$. Write $Z_{Q^+_m,tor} : \text{Ker}(Z_{Q^+_m} \rightarrow \Gamma_F)$ (the maximal torsion subgroup of $Z_{Q^+}$). Note that $\Delta_{Q^+_m} \rightarrow Z_{Q^+_m,tor}$. For $m$ running over integers with $m \geq n$, the isomorphism classes of the set of cokernels
\{Z_{Q_n,\text{tor}}/\Delta_p^n\}_{m \geq n} of pairs of abelian groups is finite. Here \(Z_{Q_n,\text{tor}}/\Delta_p^n\) and \(Z_{Q_m,\text{tor}}/\Delta_p^m\) are isomorphic if the following diagram for \(m' > m\) is commutative:

\[
\begin{array}{c}
\Delta_Q^n/\Delta_Q^m \\
\downarrow i_m \hspace{1cm} \downarrow i_{m,m'} \\
\Delta_Q^{m'}/\Delta_Q^{m''} \\
\end{array}
\]

Here \(i_{m,m'}\) is induced by sending the generator \(\delta_q \Delta_Q^m\) for \(Q_m^+ = \{q_1, \ldots, q_r\}\) to the generator \(\delta_q \Delta_Q^{m'}\) writing \(Q_{m'}^+ = \{q_1', \ldots, q_r'\}\) according to our choice of ordering. Starting with \(n = 1\), we have an isomorphism class \(S_1\) in \(\{Z_{Q_n,\text{tor}}/\Delta_p^n\}_{m \geq 1}\) with infinite elements. Suppose that we have constructed a sequence \(T_n \rightarrow T_{n-1} \rightarrow \cdots\rightarrow T_1\) of isomorphism classes \(T_j\) in \(\{Z_{Q_j,\text{tor}}/\Delta_p^j\}_{m \geq j}\) such that \(Z_{Q_n,\text{tor}}/\Delta_p^n \in T_j\) is sent onto \(Z_{Q_{j+1},\text{tor}}/\Delta_p^{j+1}\) in \(T_{j-1}\) for all \(j = 2, 3, \ldots, n\). Since

\[
T_{n+1} := \{Z_{Q_m,\text{tor}}/\Delta_p^{m+1} \mid (Z_{Q_m,\text{tor}}/\Delta_p^m) \in T_n\}_{m \geq n+1}
\]

is an infinite set, we can choose an isomorphism class \(T_{n+1} \subset T_{n+1}^{(i)}\) with \(|T_{n+1}| = \infty\). Thus by induction on \(n\), we find an infinite sequence \(\cdots \rightarrow T_{n} \rightarrow T_{n-1} \rightarrow \cdots \rightarrow T_1\) as above. Then we define \(m(n)\) for each \(n\) to be the minimal \(m\) appearing \(T_n\). Thus we have a projection \(\pi_{n+1,\text{tor}}: Z_{Q_m,\text{tor}}^{(m(n+1))}/\Delta_p^{m+1}\rightarrow Z_{Q_m,\text{tor}}^{(m(n))}/\Delta_p^n\) and a projective system of groups

\[
\begin{array}{c}
Z_{Q_m(n+1),\text{tor}}/\Delta_p^{m+1} \\
\downarrow \pi_{n+1,\text{tor}} \\
Z_{Q_m(n),\text{tor}}/\Delta_p^n \\
\end{array}
\]

\[
\begin{array}{c}
Z_{Q_m(n+1)+1}/\Delta_p^{m+1} \\
\downarrow \pi_{n+1} \\
Z_{Q_m(n)+1}/\Delta_p^n \\
\end{array}
\]

Passing to the limit, we have an exact sequence:

\[
1 \rightarrow \lim_n Z_{Q_m(n),\text{tor}}/\Delta_p^n \rightarrow \lim_n Z_{Q_m(n)/\Delta_p^n} \rightarrow \Gamma_F \rightarrow 1.
\]

Note here the subgroup \(\Delta_{\infty} := \lim_n \Delta_{Q_m(n)}/\Delta_p^n \cong \mathbb{Z}_p^+\) with \(W[\Delta_{\infty}] = W[[S_1, \ldots, S_{r+1}]]\) for the variable chosen as in Proposition 1.4 and \(W[[Z_S]]\) for \(Z_S := \lim_n Z_{Q_m(n),\text{tor}}/\Delta_p^n\) is an algebra free of finite rank over \(W[[\Delta_{\infty}]]\). We write \(\Gamma_S = Z_S/Z_{S,\text{tor}}\) for the maximal torsion subgroup \(Z_{S,\text{tor}}\) of \(Z_S\). Choose a splitting of the exact sequence \(Z_{S,\text{tor}} \rightarrow Z_S \rightarrow \Gamma_S\) so that \(\Gamma_S\) as a subgroup of \(Z_S\) contains \(\Delta_{\infty}\). Then \(W[[Z_S]] = W[[\Gamma_S]][Z_{S,\text{tor}}] \cong W[[\Gamma_S]][Z_S/\Gamma_S]\). By splitting the projection \(Z_{\infty} := \lim_n Z_{Q_m(n)/\Delta_p^n} \rightarrow \Gamma_F,\) we have a \(W[\Gamma_F]-\)algebra structure of \(W[[Z_{\infty}]]\).

**Proposition 1.5.** Let the notation be as above. Assume that \(F\) is imaginary with class number divisible by \(p\). Identify \(H_{Q_n}^+\) with \(Z_{Q_n}^+\) by (1.6) (where \(\mathfrak{a}_n\) is the ideal of \(W[[H_{Q_n}^+]]\)). Then there is a subsequence \(\{\Omega_{m(n)}\}_{n=1,2,\ldots} \subset Q^+\) such that \(W[[Q_{m(n)}]]/\mathfrak{a}_n\) forms a projective system of finite rings and that the limit ring \(\lim_n W[[Q_{m(n)}]]/\mathfrak{a}_n\) is isomorphic to the profinite group algebra \(W[[\Gamma_F \times \Gamma_S]][Z_{\infty}/\Gamma_S]\), and \(\Gamma_S\) (resp. \(\Gamma_F\)) contains \(\Delta_{\infty}\) (resp. \(\Gamma\)) as a subgroup of finite index. In particular, \(\lim_n W[[H_{Q_n}^+]]/\mathfrak{a}_n\) is free of finite rank over \(\Lambda[[S_1, \ldots, S_{r+1}]]\) and is a local complete intersection over \(\Lambda\).

2. The \(R = \mathbb{R}\) theorem and an involution of \(R\)

We place ourselves in the setting of Theorem B, but we allow any quadratic extension \(F/\mathbb{Q}\) (which can be real or imaginary). We assume that the residue field of \(W\) is given by \(F = \mathbb{Q}/\mathbb{R}\). For the moment, we only assume (h0−3) for a fixed connected component \(\text{Spec}(\mathbb{R})\) of \(\text{Spec}(h)\) for \(h := h^\mathbf{h}\) and its residual representation \(\overline{\varphi}\) of the form \(\text{Ind}_{\overline{\varphi}}^\mathbb{Q} \overline{\varphi}\) for a Galois character \(\varphi : \text{Gal}(\mathbb{Q}/F) \rightarrow \overline{\mathbb{F}}\).
We fix a weight $k \geq 0$ and pick a Hecke character $\varphi_k : \Gal(\overline{\Q}/F) \rightarrow W^\times$ of conductor at most $cP$ with $p$-type $-kiP|P$ for the identity embedding $i_P|P : F \hookrightarrow \Q_p$ such that $\varphi_k \equiv \varphi \mod m_W$. Let $\theta(\varphi_k) \in \delta_{k+1}(\Gamma_c(NP), \psi_k)$ for the corresponding theta series. Then $\psi_k$ is determined by $\varphi_k$ (i.e., $\psi_k = \varphi_k|_{\psi_k}$), regarding $\varphi_k$ and $\psi_k$ as idele characters; see [HMI, Theorem 2.71]). If $F$ is real, $k$ needs to be $0$. When $F$ is imaginary, we assume that $k \geq 1$.

Recall the identity $\psi_k\nu_p^k \mod m_W = \det(\overline{\varphi})$ for the $p$-adic cyclotomic character $\nu_p$; so, $\psi_0$ is the Teichmüller lift of $\det(\overline{\varphi})$. Hereafter, we simply write $\psi$ for $\psi_0 = \psi_k\nu_p^k$. Writing $e$ for the prime-to-$p$ conductor of $\overline{\varphi}$, by (h3), $N_{F/Q}(D) = N$ for the discriminant $D$ of $F$ (cf. [GME, Theorem 5.1.9]). By (h1), the conductor $e$ is square-free and only divisible by split primes in $F/\Q$. Since $\overline{\varphi} = \Ind_{F_p}^F \varphi$, for $l|N$, the prime $l$ either splits in $F$ or ramified in $F$. Write $l$ for the prime factor of $(l)$ in $F$. If $(l)$ splits into $\mathfrak{f}$, we may assume that the character $\varphi$ ramifies at $\mathfrak{f}$ and is unramified at $\mathfrak{f}$, and hence $\overline{\varphi}|_{\Gal(F_p/Q)} \cong \varphi \otimes \varphi$. If $(l) = l^2$ ramifies in $F$, we have $\overline{\varphi}|_{l} \cong 1 \oplus \chi$ for the quadratic character $\chi = \left(\frac{F}{l}\right)$. Here $l$ is the inertia subgroup of $\Gal(\overline{F}/l)$.

Write $CL_W$ for the category of $p$-profinite local $W$-algebras with residue field $F := W/m_W$ whose morphisms are local $W$-algebra homomorphisms. Let $\Q(NP) \subset \overline{\Q}$ be the maximal extension of $\Q$ unramified outside $NP\infty$. Consider the following deformation functor $D : CL_W \rightarrow SETS$ given by

$D(A) = D^0(A) := \{ \rho : \Gal(\Q(NP)/\Q) \rightarrow GL_2(A) : a representation satisfying (D1–4)) \}$.

Here are the conditions (D1–4):

(D1) $\rho \mod m_A \cong \overline{\rho}$ (i.e., there exists $a \in GL_2(F)$ such that $a\overline{\rho}(\sigma)a^{-1} = (\rho \mod m_A)$ for all $\sigma \in \Gal(\Q/Q(\overline{\varphi}))$).

(D2) $\rho|_{\Gal(F_p/Q)} \cong \left(\begin{smallmatrix} 1 & \delta \\ 0 & 1 \end{smallmatrix}\right)$ with $\delta$ unramified.

(D3) $\det(\rho)|_{I_l} = \epsilon_l(\varphi)$ for the $l$-part $\psi_l$ of $\psi$ for each prime $l|N$, where $\epsilon_l : W \rightarrow A$ is the morphism giving $W$-algebra structure on $A$ and $\psi_l = \psi|_{I_l}$ regarding $\psi$ as a Galois character by class field theory.

(D4) $\det(\rho)|_{I_p} \equiv \psi|_{I_p} \mod m_A$ (which is equivalent to $\epsilon|_{I_p} \equiv \psi|_{I_p} \mod m_A$).

If we want to allow ramification at primes in a finite set $Q$ of primes outside $NP$, we write $Q(NP)$ for the maximal extension of $\Q$ unramified outside $Q \cup \{l|N\} \cup \{\infty\}$. Consider the following functor

$D^Q(A) := \{ \rho : \Gal(\Q(NP)/\Q) \rightarrow GL_2(A) : a representation satisfying (D1–4) and (UQ)) \}$.

Here are the conditions (D1–4):

(UQ) $\det \rho$ is unramified at all $q \in Q$.

We may also impose another condition if necessary:

(det) $\det(\rho) = \epsilon_l(\varphi)\nu_p^k\psi_k$ for the $p$-adic cyclotomic character $\nu_p$,

and consider the functor

$D_{Q,k,\psi_k}(A) := \{ \rho : \Gal(\Q(NP)/\Q) \rightarrow GL_2(A) : a representation satisfying (D1–4) and (det)) \}$.

The condition (det) implies that if deformation is modular and satisfies (D1–4), then it is associated to a weight $k + 1$ cuspidal form of Neben character $\psi_k$; strictly speaking, if $k = 0$ (i.e., $F$ is real), we allow non-classical $p$-ordinary $p$-adic cusp forms. We often write simply $D_{k,\psi_k}$ for $D_{\emptyset,k,\psi_k}$ when $Q$ is empty. For each prime $q$, we write $D^Q_{k,\psi_k}$ for the deformation functor of $\overline{\varphi}|(\Gal(\Q/Q))$ satisfying the local condition (D2–4) which applies to $q$.

By our choice of $\overline{\varphi} = \Ind_{F_p}^F \varphi$, we have $\overline{\varphi}|_{\Gal(F_p/Q)} \cong \left(\begin{smallmatrix} T & 0 \\ 0 & \overline{T} \end{smallmatrix}\right)$ for two local characters $\overline{T}, \overline{T}_q$ for all $q \in Q$. If $\overline{T} \neq \varphi$ (i.e., (Rg)) and $\overline{T}_q(\Frob_q) \neq \overline{T}(\Frob_q)$ for all $q \in Q \cup \{l|N\} \cup \{\infty\}$, the $D_{k,\psi_k}$ and $D_{Q,k,\psi_k}$ are representable by universal objects $(R, \rho) = (R^0, \rho^0)$, $(R^Q, \rho^Q)$, $(R^0, \rho_0)$ and $(R_Q, \rho_Q)$, respectively (see [MFG, Proposition 3.30] or [HMI, Theorem 1.46 and page 186]).

Here is a brief outline of how to show the representability of $D$. It is easy to check the deformation functor $D_{\ord}$ only imposing (D1–2) is representable by a $W$-algebra $R_{\ord}$. The condition (D4) is actually redundant as it follows from the universality of the Teichmüller lift and the conditions (D1–2). Since $N$ is the prime-to-$p$ conductor of $\det(\overline{\varphi})$ and $p$ is unramified in $F/\Q$ (h2–3), if $l$ is a prime factor of $N$, writing $\rho|_l$ for its semi-simplification of $\rho$ over $I_l$, we see from (h0) that $\rho|_l = \epsilon_l(\psi_l) \psi_l \mod m_A$. Thus
by the character $\epsilon_N := \prod \epsilon_l$ of $I_N = \prod I_l$, $A$ is canonically an algebra over the group algebra $W[I_N]$. Then $R$ is given by the maximal residue ring of $R^{\text{red}}$ on which $I_N$ acts by $\psi_{1,N} = \prod I_N \psi_l I_l$; so, $R = R^{\text{red}} \otimes_{W[I_N],\psi_{1,N}} W$, where the tensor product is taken over the algebra homomorphism $W[I_N] \to W$ induced by the character $\psi_{1,N}$. Since $\mathfrak{p}$ is an induced representation, $\mathfrak{p}[I_l]$ is semi-simple and $\mathfrak{p}[I_l] = \mathfrak{t}_l \oplus \delta_l$ with $\mathfrak{t}_l = \epsilon_l \mod m_A$. Similarly one can show the representability of $D^Q$ and $D_{Q,k,\psi_\alpha}$.

Let $\mathbb{T}$ be the local ring of $h = h^0$ as in Theorem B whose residual representation is $\mathfrak{p} = \text{Ind}_{G}^{G} \mathfrak{t}$. The ring $\mathbb{T}$ is uniquely determined by (h1–3) as the unramified quotient of $\mathfrak{p}$ at each $l \mid Np$ is unique. Without assuming (h1–3), to have a universal ring and to have uniquely defined $T$, we need to specify in the deformation problem the unramified quotient character and for $\mathbb{T}$, the residue class of $U(l)$-eigenvalue (because of the existence of companion forms).

Since $\mathfrak{p}$ is irreducible, by the technique of pseudo-representation, we have a unique representation $\rho_T : \text{Gal}(\mathbb{Q}(Np)/\mathbb{Q}) \to \text{GL}_2(\mathbb{T})$ up to isomorphisms such that $\text{Tr}(\rho_T(\text{Frob}_{l})) = T(l) \in \mathbb{T}$ for all prime $l \nmid Np$ (e.g., [HMI, Proposition 3.49]). This representation is a deformation of $\mathfrak{p}$ in $D^0(\mathbb{T})$. Thus by universality, we have projections $\pi : R = R^0 \to \mathbb{T}$, such that $\pi \circ \rho \cong \rho_T$. Here is the “$R = \mathbb{T}$” theorem of Taylor, Wiles et al:

**Theorem 2.1.** Assume (Rg) and (h0–3) with either (h4) or (h5). Then the morphism $\pi : R \to \mathbb{T}$ is an isomorphism, and $\mathbb{T}$ is a local complete intersection over $\Lambda$.

See [Wi95, Theorem 3.3] and [DFG04] for a proof (see also [HMI, §3.2] or [MFG, Theorem 3.31] for details of how to lift the results in [Wi95] to the (bigger) ordinary deformation ring with varying determinant character). These references require the assumption (W) which is absolute irreducibility of $\mathfrak{p}_{[\text{Gal}(\mathbb{Q}/M)]}$ for $M = \mathbb{Q}[\sqrt{p}]$ with $p^* := (-1)^{(p-1)/2}p$. Note that (W) follows from either (h4) or (h5), as mentioned in the introduction. To eliminate the assumption (h0), we need to impose in addition to (D3) that $H^0(I_l, \rho) \cong A$ for prime factors $l$ of $N$ with $l \equiv 1 \mod p$ to have the identity $R = \mathbb{T}$ (or work with $\Gamma_1(l)$-level Hecke algebra), which not only complicates the setting but also the identification of $T/I \cong W[[H]]$ (for $I$ in Theorem B) could fail if (h0) fails (so, we always assume (h0); see Lemma 2.4). We will recall the proof of Theorem 2.1 in the following Section 4 to good extent in order to facilitate a base for a finer version we study there.

Perhaps the following fact is well known (e.g., [Ru91, Theorem 5.3]):

**Corollary 2.2.** Assume (h0–4) and that $F$ is an imaginary quadratic field of class number prime to $p$. Then $Y^{-}(\varphi^-)$ has homological dimension 1 (so, it does not have any pseudo-null submodule non-null). Thus if $Y^{-}(\varphi^-)$ is pseudo isomorphic to a cyclic $\mathbb{Z}_p[\varphi^-][[\Gamma_-]]$-module $\mathbb{Z}_p[\varphi^-][[\Gamma_-]]/(f^-)$ with $f^- \in \mathbb{Z}_p[\varphi^-][[\Gamma_-]]$, it has an injection into the cyclic module with finite cokernel.

**Proof.** Write the presentation of $R \cong \mathbb{T}$ as $R = \Lambda[[[T_1, \ldots, T_r]] / (S_1, \ldots, S_r)]$ for a regular sequence $(S_1, \ldots, S_r)$ of $\Lambda[[[T_1, \ldots, T_r]]$. Then by the fundamental exact sequence of differentials (e.g., [CRT, Theorem 25.2] and [HMI, page 370]), we get the following exact sequence

$$0 \to \bigoplus_i R\mathrm{d}S_i = (S_1, \ldots, S_r) / (S_1, \ldots, S_r)^2 \to \bigoplus_i R\mathrm{d}T_i \to \Omega_{R/\Lambda} \to 0.$$ 

Since the class number of $F$ is prime to $p$, the CM component $W[[H]]$ of $\mathbb{T} = R$ is isomorphic to $\Lambda$; so, tensoring $\Lambda$ over $R$, we get another exact sequence:

$$0 \to \bigoplus_i \Lambda\mathrm{d}S_i \to \bigoplus_i \Lambda\mathrm{d}T_i \to \Omega_{R/\Lambda} \otimes R \Lambda \to 0.$$ 

By a theorem of Mazur (cf. [MT90], [HT94, 3.3.7] and [H16, §6.3.6]), under (Rm) (which follows from (h2–3)) and (h0), we have $\Omega_{R/\Lambda} \otimes R \Lambda \cong Y^{-}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W$. Thus we get a $\Lambda$-free resolution of length 2 of the Iwasawa module, and hence it has homological dimension 1.

Suppose that we have a pseudo-isomorphism $i : Y^{-}(\varphi^-) \to \mathbb{Z}_p[\varphi^-][[\Gamma_-]]/(f)$. Then $i$ is an injection as $Y^{-}(\varphi^-)$ does not have any pseudo-null submodule non-null, and $\text{Coker}(i)$ is finite. □
Since $\mathfrak{p} = \text{Ind}_F^\mathbb{Q} \mathfrak{p}$, for $\chi = \left( \frac{\mathbb{Q}}{D} \right)$, $\mathfrak{p} \otimes \chi \cong \mathfrak{p}$. By ordinarity, $p$ splits in $F$; so, $\chi$ is trivial on $\text{Gal}(\mathbb{Q}_l/\mathbb{Q})$ for prime factors of $pN_F/Q(\mathfrak{c})$ and ramified quadratic on $\text{Gal}(\mathbb{Q}_l/\mathbb{Q})$ for $l|D$. Thus $\rho \mapsto \rho \otimes \chi$ is an automorphism of the functor $D^G$ and $D_{Q,p,\psi,k}$, and $\rho \mapsto \rho \otimes \chi$ induces automorphisms $\sigma_Q$ of $R_Q$ and $R^Q$.

We identify $R$ and $T$ now by Theorem 2.1; in particular, we have an automorphism $\sigma = \sigma_0 \in \text{Aut}(\mathbb{T})$ as above. We could think about $h_{W_0}$ defined over a smaller complete discrete valuation ring $W_0 \subset W$ (the smallest possible ring is $\mathbb{Z}_p[w]$). After extending scalar from $W_0$ to $W$, we get an involution. We may assume that $W = W(F)$ (the Witt vector ring of $F = T/m_F$). Since $\sigma$ fixes $W$ as it is an identity on $F$, we know that $\sigma$ preserves $T$ before extending scalar to $W$. Thus we get

**Corollary 2.3.** Assume (h0–4). Then for a complete discrete valuation ring $W_0$ flat over $\mathbb{Z}_p[w]$, we have an involution $\sigma \in \text{Aut}(\mathbb{T}/W_0)$ with $\sigma \rho_T \cong \rho_T \otimes \chi$.

We write $T_+$ for the subring of $T$ fixed by the involution in Corollary 2.3. More generally, for any module $X$ on which the involution $\sigma$ acts, we put $X_\pm = X^\pm = \{x \in X|\sigma(x) = \pm x\}$. In particular, we have $T_{\pm} = \{x \in T|x^\sigma = \pm x\}$.

We now study the fixed subscheme $\text{Spec}(\mathbb{T})^G$ of $G = \langle \sigma \rangle \subset \text{Aut}(\mathbb{T}/\Lambda)$. Consider the functor $D_F, D_F^\infty : \text{CLS}_W \rightarrow \text{SETS}$ defined by

$$D_F(A) = \{\lambda : \text{Gal}(\mathbb{Q}/F) \rightarrow A^\times|\lambda \equiv \mathfrak{p} \mod m_A \text{ has conductor a factor of } \mathfrak{p}\},$$

and

$$D_F^\infty(A) = \{\lambda : \text{Gal}(\mathbb{Q}/F) \rightarrow A^\times|\lambda \equiv \mathfrak{p} \mod m_A \text{ has conductor a factor of } \mathfrak{p}^\infty\}.$$ 

Let $F_{\mathfrak{p}}$ be the maximal abelian $p$-extension of $F$ inside the ray class field of conductor $\mathfrak{p}$. Put $C = C_0 := \text{Gal}(F_{\mathfrak{p}}/F)$. Similarly, write $F_{\mathfrak{p}} \infty$ for the maximal $p$-abelian extension inside the ray class field over $F$ of conductor $\mathfrak{p}^\infty$. Put $H := \text{Gal}(F_{\mathfrak{p}} \infty/F)$. Note that $F_{\mathfrak{p}} \infty/F$ is a finite extension if $F$ is real. Then $D_F$ is represented by $(W[C], \Phi)$ where $\Phi(x) = \varphi(x)x$ for $x \in C$, where $\varphi$ is the Teichmüller lift of $\mathfrak{p}$ with values in $W^\times$. Similarly $D_F^\infty$ is represented by $W[[H]] = \lim_{\longrightarrow} W/H/H'$ for $H := \text{Gal}(F_{\mathfrak{p}} \infty/F)$. If $F$ is real, $H$ is a finite group, but it is an infinite $p$-profinite group if $F$ is imaginary.

In the introduction, when $F$ is imaginary, we defined $H$ as the anticyclotomic $p$-primary part $\text{Gal}(K^-/F)$ of the Galois group of the ray class field $K$ of conductor $(c \cap c^p)p^\infty$. The present definition is a bit different from the one given there. However, the present $H$ is isomorphic to the earlier $\text{Gal}(K^-/F)$ by sending $\tau$ to $\tau^{1-c/p^2} = \sqrt{\tau c^p-c^-1}$, by (1.6). Thus we identify the two groups by this isomorphism, as the present definition makes the proof of the following results easier. We have the following simple lemma which can be proven in exactly the same way as [CV03, Lemma 2.1] and [H15, Theorem 7.2]:

**Lemma 2.4.** Assume (h0–4) and $p > 3$. Then the natural transformation $\lambda \mapsto \text{Ind}_F^\mathbb{Q} \lambda$ induces an isomorphism $D_F \cong D_F^\infty$ and $D_F^\infty \cong D_F^G$, where

$$D_F^G(A) = \{\rho \in D(A)|\rho \otimes \chi \cong \rho\} \quad \text{and} \quad D_F^G(A) = \{\rho \in D_F^G(A)|C(\text{det} \rho) \supset (NP)\}$$

for the conductor $C(\text{det} \rho)$ of $\text{det}(\rho)$.

**Proof.** Since the proof is essentially the same for the two cases, we only deal with $D_F^\infty \cong D_F^G$. By [DH98, Lemma 3.2], we have $\rho \otimes \chi \cong \rho$ for $\rho \in D(A)$ is equivalent to having $\lambda : \text{Gal}(\mathbb{Q}/F) \rightarrow A^\times$ such that $\rho \cong \text{Ind}_F^\mathbb{Q} \lambda$. We can choose $\lambda$ so that $\lambda$ has conductor a factor of $\mathfrak{p}^\infty$ by (D4) and $C(\text{det}(\rho))|NP^\infty$. Then $\lambda$ is unique by (D2–3) and (h0). Thus we get the desired isomorphism.

Since $D_F^G$ (resp. $D_F^G$) is represented by $\mathbb{T}/(TT+I) = \mathbb{T}/I \otimes \Lambda/(T)$ (resp. $\mathbb{T}/I$) for $I = T(\sigma-1)/T$, this lemma shows

**Corollary 2.5.** Assume (h0–4). Then we have $\mathbb{T}/I \otimes \Lambda/(T) \cong W[C]$ and $\mathbb{T}/I \cong W[[H]]$ canonically.
Anticyclotomic Cyclicity Conjecture

In the proof of Theorem 2.1, Taylor and Wiles considered an infinite sets $Q$ made up of finite sets $Q$ of primes $q \equiv 1 \mod p$ outside $Np$ such that $\mathfrak{P}(\text{Frob}_q) \sim \left( \begin{array}{cc} \alpha_q & 0 \\ 0 & \beta_q \end{array} \right)$ with $\alpha_q \neq \beta_q \in \mathfrak{F}$. Over the inertia group $I_q$, $\rho^Q$ has the following shape by a theorem of Faltings

$$\rho^Q|_{I_q} = \left( \begin{array}{cc} \delta_q & 0 \\ 0 & \delta_q' \end{array} \right)$$

for characters $\delta_q, \delta_q' : \text{Gal}(\overline{\mathbb{Q}}_q/Q_q) \to (R^Q) \times$ such that $\delta_q'|I_q = \delta_q^{-1}$ and $\delta_q([q, Q_q]) \equiv \overline{\rho} \mod \mathfrak{m}_T$ (e.g., [MFG, Theorem 3.32 (1)] or [HMI, Theorem 3.75]). Since $\overline{\mathfrak{P}}$ is unramified at $q$, $\delta_q$ factors through the maximal $p$-abelian quotient $\Delta_q$ of $\mathbb{Z}_q^\times$ by local class field theory, and in fact, it gives an injection $\delta_q : \Delta_q \to R^Q$ as we will see later. Note that $\rho \to \rho \otimes \chi$ is still an automorphism of $D^Q$ and hence induces an involution $\sigma = \sigma_Q$ of $R^Q$.

We can choose infinitely many distinct $Q$s with $\mathfrak{P}(\text{Frob}_q)$ for $q \in Q$ having two distinct eigenvalues. We split $Q = Q^+ \sqcup Q^-$ so that $Q^\equiv k = \{ q \in Q | \chi(q) = \pm 1 \}$. By choosing an eigenvalue $\overline{\rho} \equiv \mathfrak{m}(\text{Frob}_q)$ for each $q \in Q$, we have a unique Hecke algebra local factor $\mathbb{T}_Q$ of the Hecke algebra $\mathfrak{h}_{Q,k, \psi_k}$, whose residual representation is isomorphic to $\mathfrak{P}$ and $U(q)$ mod $\mathfrak{m}_{\mathfrak{P}Q}$ is the chosen eigenvalue $\mathfrak{P}$. This follows from Corollary 1.3 in the following way: We choose $\overline{\rho}$ for $q \in Q^-$ as in Corollary 1.3. For $q \in Q^+$, we choose a unique prime factor $q|q$ so that $\mathfrak{P}(\text{Frob}_q) = \mathfrak{P}_q$. In this way, we get a local factor $\mathbb{T}^Q$ of $h^Q$ which covers $W[[Z_Q]]$ as in Corollary 1.3. Recall (1.7):

$$\mathbb{T}_Q = \mathbb{T}^Q/(t - \gamma^k) \mathbb{T}^Q$$

denotes a local factor of $\mathfrak{h}_{Q,k, \psi_k}$ with the prescribed mod $p$ eigenvalues of $U(q)$ for $q \in Q$.

By absolute irreducibility of $\mathfrak{P}$, the theory of pseudo representation tells us that the Galois representation $\rho_{Q^+}$ in Section 1 can be arranged to have values in $\text{GL}_2(T^Q)$ (e.g., [MFG, Proposition 2.16]). The isomorphism class of $\rho_{Q^+}$ as representation into $\text{GL}_2(T^Q)$ is unique by a theorem of Carayol–Serre [MFG, Proposition 2.13], as Tr$(\rho_{Q^+}(\text{Frob}))$ is given by the image of $T(l)$ in $T^Q$ for all primes $l$ outside $N_{Q^+}$ by (Gal) in Section 1 (and by Chebotarev density theorem). We need to twist $\rho_{Q^+}$ slightly by a character $\delta$ to have $\rho_{Q^+} \otimes \delta$ satisfy (UQ). This twisting is done in the following way: By (Gal,q), write $\rho_{Q^+} \sim (\alpha_q 0 \gamma_q 1)$ as a representation of the inertia group $I_q$ for $q \in Q$. Then $\epsilon_q \equiv 1 \mod \mathfrak{m}_{\mathfrak{P}Q}$ so that $\mathfrak{P}$ is unramified at $q$. Thus $\epsilon_q$ has $p$-power order factoring through the maximal $p$-abelian quotient $\Delta_q$ of $\mathbb{Z}_q^\times$; so, it has a unique square root $\sqrt{\epsilon_q}$ with $\sqrt{\epsilon_q} \equiv 1 \mod \mathfrak{m}_{\mathfrak{P}Q}$. Since $\Delta_q$ is a unique quotient of $(\mathbb{Z}/q\mathbb{Z})^\times = \text{Gal}(\mathbb{Q}(\mu_q)/\mathbb{Q})$, we can lift $\sqrt{\epsilon_q}$ to a unique global character of $\text{Gal}(\mathbb{Q}(\mu_q)/\mathbb{Q})$. Write $\sqrt{\epsilon} := \prod_{q \in Q} \sqrt{\epsilon_q}$ as a character of $\text{Gal}(\mathbb{Q}(\mu_q)_{q \in Q}/\mathbb{Q}) \cong \prod_{q \in Q} (\mathbb{Z}/q\mathbb{Z})^\times$. Then we define

$$\rho^Q := \rho_{Q^+} \otimes \sqrt{\epsilon}^{-1}.$$}

Then $\rho^Q$ satisfies (UQ) and $\rho^Q \in D^Q(T^Q)$. In the same manner, we can define a unique global character $\delta : \text{Gal}(\mathbb{Q}(\mu_q)_{q \in Q}/\mathbb{Q}) \to (R^Q) \times$ such that $\delta|_{I_q} = \delta_q$ for all $q \in Q$.

By local class field theory, we identify $\Delta_q$ with the $p$-Sylow subgroup of $\mathbb{Z}_q^\times$. Then the $p$-abelian group $\Delta_Q$ defined above Theorem 1.2 has a canonical factorization: $\Delta_Q := \bigoplus_{q \in Q} \Delta_q$. By Lemma 1.1, the inertia action $I_q \to R^Q \to T^Q$ makes $T^Q$ free (of finite rank) over $W[\Delta_Q]$, and hence $\Delta_Q \hookrightarrow R^Q$ and $\Delta_Q \twoheadrightarrow T^Q$. The character $\delta_q : I_q \to R^Q \times$ (resp. $\delta^{-1}_q : I_q \to R^Q \times$) extends uniquely to $\delta_q : \text{Gal}(\mathbb{Q}_q/Q_q) \to R^Q$ (resp. $\delta^{-1}_q : \text{Gal}(\mathbb{Q}_q/Q_q) \to R^Q$) so that

$$\rho^Q|_{\text{Gal}(\mathbb{Q}_q/Q_q)} = \left( \begin{array}{cc} \delta_q & 0 \\ 0 & \delta^{-1}_q \end{array} \right)$$

with $\delta_q(\phi_q) \mod \mathfrak{m}_{RQ} = \overline{\rho}_q$ (resp. $\delta^{-1}_q(\phi_q) \mod \mathfrak{m}_{RQ} = \overline{\rho}_q$) for any $\phi_q \in \text{Gal}(\mathbb{Q}_q/Q_q)$ with $\phi_q \mod I_q = \text{Frob}_q$ (e.g., [MFG, Theorem 3.32] or [HMI, Theorem 3.75]).

We choose $q|q$ for $q \in Q^+$ so that $\mathfrak{P}(\text{Frob}_q) = \mathfrak{P}_q$, and define $\mathfrak{P}_+$ by the product over $q \in Q^+$ of $q$ thus chosen. Define the functor $D_{F, Q}^\infty : CLW \to SETS$ by

$$D_{F, Q}^\infty(A) = \{ \lambda : \text{Gal}(\overline{\mathbb{Q}}/F) \to A : \lambda \equiv \overline{\rho} \mod \mathfrak{m}_A \text{ has conductor a factor of } \mathfrak{P}_+ \mathfrak{p}^\infty \}.$$
Proposition 2.6. Assume $(h0-4)$. Let $I^Q = R^Q(\sigma_Q - 1)R^Q$. Then $R^Q/I^Q \cong W[[H_Q]]$ and $R^Q/I^Q \otimes_A (T/\ell) \cong W[C_Q]$ for $C_Q$ defined above Theorem B.

Proof. Since the proof is basically the same for $H_Q$ and $C_Q$, we shall give a proof for $H_Q$. If a finite group $G$ acts on an affine scheme Spec$(A)$ over a base ring $B$, the functor Spec$(A)^G : C \mapsto$ Spec$(A)/(C)^G = Hom_{B-Alg}(A, C)^G$ sending $B$-algebras $C$ to the set of fixed points is a closed subscheme of Spec$(A)$ represented by $A_G := A/\bigcap_{\varphi \in G} A(g-1)A$; i.e., Spec$(A)^G = Spec(A_G)$. Thus we need to prove that the natural transformation $\lambda \mapsto \text{Ind}_{\overline{\rho}}^\lambda \chi$ induces an isomorphism $D^\infty_{F, Q} \cong (D^Q)^\lambda$, where $(D^Q)^\lambda(A) = \{\rho \in D^Q(A) | \rho \otimes \chi \cong \rho\}$. If $\rho \in D^Q(A)$, we have a unique algebra homomorphism $\phi : R^Q \to A$ such that $\rho \cong \phi \otimes \overline{\rho}^Q$ and $\rho|_{I^Q} \cong \begin{pmatrix} 0 & 1 \\ \phi \otimes \delta \end{pmatrix}_{I^Q}$, where $\phi \otimes \delta \cong \delta \otimes \phi^{-1}$ for the global character $\delta : \text{Gal}(Q(\mu_q)/Q) \to \text{Spec}(Q)$, and hence its prime-to-$p$ conductor is a factor of $N_Q$. On the other hand, for $\rho = \text{Ind}_{\overline{\rho}}^\lambda \chi$, if $\rho$ ramifies at $q \in Q^-$, the $q$-conductor of $\rho \otimes (\phi \otimes \delta)$ is $N_{F/Q}(q) = q^2$, a contradiction as $q^2 \nmid N_Q$. Thus $\lambda$ is unramified at $q \in Q^-$, and we may assume $\lambda \in D^\infty_{F, Q}(A)$. Indeed, among $\lambda, \lambda_\epsilon$ for $\epsilon(q) = \lambda(\epsilon(q))$, we can characterize $\lambda$ uniquely by $(h0)$ so that $\lambda \mod m_A = \overline{\rho}$. Thus $D^\infty_{F, Q}(A) \to (D^Q)^\lambda(A)$ is an injection. Surjectivity follows from [DH98, Lemma 3.2].

3. The Taylor–Wiles system and Taylor–Wiles primes

In their proof of Theorem 2.1, Taylor and Wiles used an infinite family $Q$ of finite sets $Q$ made of primes $q \equiv 1 \mod p$ outside $N$. We can choose infinitely many distinct $Q$s with $\overline{\rho}(\text{Frob}_q)$ for $q \in Q$ having two distinct eigenvalues. Recall $\chi = (F/\overline{\rho})$ and $\overline{\rho} = \text{Ind}_{\overline{\rho}}^{\rho} \overline{\rho}$ as in Theorem B. We split $Q = Q^+ \cup Q^-$ so that $Q^\pm = \{q \in Q | \chi(q) = \pm 1\}$. By fixing a weight $k \geq 0$ and choosing an eigenvalue $\overline{\chi}_q$ of $\overline{\rho}(\text{Frob}_q)$ for each $q \in Q$, we have a unique local factor $T^Q$ (resp. $T_Q$) of the Hecke algebra $h^Q$ (resp. $h_{Q, k, \chi}$) as in (1.7), whose residual representation is isomorphic to $\overline{\rho} \otimes U(q)$ mod $m_{T^Q}$ the chosen eigenvalue $\overline{\chi}_q$. Though it is not necessary, we assume $k \geq 1$ if $F$ is imaginary (to stick to classical modular forms), but we are forced to assume that $k = 0$ if $F$ is real (as there are no holomorphic theta series of a real quadratic field of weight higher than 1; see [MFM, §4.8]).

To describe the Taylor–Wiles system used in the proof of Theorem 2.1 (with an improvement due to Diamond and Fujiwara), we need one more information of a $T^Q$-module $M_Q$ in the definition of the Taylor–Wiles system in [HMI, §3.2.3] and [MFG, §3.2.6]. Here we choose $M_Q := T^Q$ which is the choice made in [MFG, §3.2.7] (and [HMI, page 198]), though in the original work of Taylor–Wiles, the choice is $T^Q$-factor $H_1(X(\Gamma_Q), W) \otimes_{h^Q} T^Q$ of the homology group $H_1(X(\Gamma_Q), W)$ for the modular curve $X(\Gamma_Q)$ associated to $\Gamma_Q := \Gamma_Q(1)$ defined in (1.3).

The Hecke algebra $h^Q(\Gamma_Q, \psi; W)$ has an involution coming from the action of the normalizer of $\Gamma_Q$. Taking $\gamma \in SL_2(Z)$ such that $\gamma = \begin{pmatrix} q & 1 \\ 0 & 1 \end{pmatrix}$ mod $2^2$ and $\gamma = 1 \mod (N_Q/D)^2$, put $\eta := \gamma = \begin{pmatrix} q & 1 \\ 0 & 1 \end{pmatrix}$. Then $\eta$ normalizes $\Gamma_Q$, and the action of $\eta$ satisfies $\eta^2 = 1$, $\eta U(l)\eta^{-1} = \chi(l)U(l)$ for each prime $l | N_Q/D$ and $\eta T(l)\eta^{-1} = \chi(l)T(l)$ for each prime $l | N_Q$ (see [MFM, (4.6.22), page 168]). Thus the conjugation of $\eta$ induces on $T^Q$ an involution compatible with $\sigma_Q$ under the canonical surjection $R^Q \to T^Q$. Note that $\sigma_Q(U(q)) = -U(q)$ for each $q \in Q^-$; so, the role of $\overline{\chi}_q$ will be played by $-\overline{\chi}_q = \overline{\rho}$. This affects on the inertia action of $D_\ell$ at $q$ by $d_\ell \to d_\ell^{-1}$ for $q \in Q^-$, because the action is normalized by the choice of $\overline{\chi}_q$ with $\overline{\chi}_q = \overline{U}(q)$ mod $m_{T^Q}$ (see Lemma 3.1 and [HMI, Theorem 3.74]). Since $T^Q$ is the local component of the big Hecke algebra of tame level $\Gamma_Q$ whose reduction modulo $t - \gamma^k$ is $T^Q$, again $T^Q$ has involution $\sigma_Q$ induced from $\eta$. We have $T^Q_{\overline{\rho}}$ (resp. $T^Q_{\overline{\rho}}$) for the fixed subring of $T^Q$ (resp. $T^Q$) under the involution.

Since we follow the method of Taylor–Wiles for studying the local complete intersection property of $R_+ \cong \mathbb{T}_+$, we recall the Taylor–Wiles system argument (which proves Theorem 2.1) formulated by Fujiwara [Fu06] (see also [HMI, §3.2]). Identify the image of the inertia group $I_q$ for $q \in Q$ in the Galois group of the maximal abelian extension over $\mathbb{Q}_q$ with $\mathbb{Z}_q^\times$ by the $q$-adic cyclotomic character. Recall the $p$-Sylow subgroup $\Delta_q$ of $\mathbb{Z}_q^\times$ and $\Delta_Q := \prod_{q \in Q} \Delta_q$ in (1.4). If $q \equiv 1 \mod p^m$ for $m > 0$ for all $q \in Q$, $\Delta_q/\Delta_q^{p^m}$ for $0 < n \leq m$ is a cyclic group of order $p^m$. We put $\Delta_n = \Delta_{n, Q} := \prod_{q \in Q} \Delta_q/\Delta_q^{n}$. By Lemma 1.1, the inertia action $I_q \to \mathbb{Z}_q^\times \to R_q \to T_q$ makes $T_Q$ free of finite rank over $W[\Delta_Q]$. 
Then they found an infinite sequence $\mathcal{Q} = \{Q_m | m = 1, 2, \ldots \}$ of ordered finite sets $Q = Q_m$ of primes $q$ (with $q \equiv 1 \pmod{p^n}$) which produces a projective system:

$$\{(R_{m,n}(\alpha) = \alpha_n), \tilde{R}_{n,m}(\alpha), (f_1 = f_1^{(n)}, \ldots, f_r = f_r^{(n)})\}_n$$

made of the following objects:

1. $R_{n,m} := +\mathbb{T}_{Q_m}/(p^n, \delta_q^{n} - 1)_{q \in Q_m}$ for each $0 < n \leq m$. Since the integer $m$ in the system (3.1) is determined by $n$, we have written it as $m(n)$. In [HMI, page 191], $R_{n,m}$ is defined to be the image of $\mathbb{T}_{Q_m}$ in $\text{End}_{\mathbb{Q}/\mathbb{Z}^\varphi}(M)$ for $M_{n,m} := M_{Q_m}/(p^n, \delta_q^{n} - 1)_{q \in Q_m}$. $M_{n,m}$, but by our choice $M_{Q_m} = \mathbb{T}_{Q_m}$, the image is identical to $\mathbb{T}_{Q_m}/(p^n, \delta_q^{n} - 1)_{q \in Q_m}$. An important point is that $R_{n,m}$ is a finite ring whose order is bounded independent of $m$ (by (Q0) below).

2. $\tilde{R}_{n,m} := R_{n,m}/(\delta_q^{n} - 1)_{q \in Q_m}$, $\tilde{R}_{n,m}$.

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

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

Thus for each $n > 0$, the projection $\pi^{n+1} : R_{n+1,m(n+1)} \to R_{n,m(n)}$ is compatible with all the data in the system (3.1) (the meaning of this compatibility is specified below) and induces the projection $\tilde{\pi}^{n+1} : R_{n+1,m(n+1)} \to R_{n,m(n)}$. In [HMI, page 191], there is one more datum of an algebra homomorphism $\beta : R_{n,m} \to \text{End}_{\mathbb{T}_{Q_m}}(M_{n,m}) \subset \text{End}_{\mathbb{T}_{Q_m}}(M_{n,m})$. Since we have chosen $M_{Q_m}$ to be $\mathbb{T}_{Q_m}$, $M_{n,m}$ is defined $R_{n,m}$; so, $\beta$ is just the identity map (and hence we forget about it). The infinite set $\mathcal{Q}$ satisfies the following conditions (Q0–8):

(Q0) $M_{Q_m} = \mathbb{T}_{Q_m}$ is free of finite rank $d$ over $W[\Delta_{Q_m}]$ with $d$ independent of $m$ (see Lemma 1.1 and the remark after the lemma and [HMI, (tw3)], pages 190 and 199) making $M_{Q_m} := \mathbb{T}_{Q_m}$.

(Q1) $|Q_m| = r \geq \dim_{\mathbb{Q}/\mathbb{Z}^\varphi} D_{Q_m,k/\psi}(G[F])$ for $r$ independent of $m$ [HMI, Propositions 3.29 and 3.33], where $\epsilon$ is the dual number with $\epsilon^2 = 0$. (Note that $\dim_{\mathbb{Q}/\mathbb{Z}^\varphi} D_{Q_m,k/\psi}(G[F])$ is the minimal number of generators of $R_{Q_m}$ over $W$.)

(Q2) $q \equiv 1 \pmod{p^n}$ and $\overline{q}(\text{Frob}_q) := (\begin{smallmatrix} \overline{q} & 0 \\ 0 & \overline{q} \end{smallmatrix})$ with $\overline{q} / \overline{q} \in F$ if $q \in Q_m$ (so, $|\Delta_q| = p^e \geq p^m$). Actually as we will see later in Lemma 3.2, we can impose a slightly stronger condition: $q \equiv 1 \pmod{p}$ for $C = N_{F_k/Q}(\epsilon)$.

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

- $\Delta_{q_j} \subset \Delta_{Q_m}$ is identified with $\mathbb{Z}/p^n \mathbb{Z}^\varphi$ by $\delta_q^{n} - 1$; 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 $\Delta_n^{\alpha} / \Delta_n^{\alpha + 1} = ((\mathbb{Z}/p^n \mathbb{Z})^{\alpha} / (\mathbb{Z}/p^{n+1} \mathbb{Z}))^{Q_m(n)}$,
- the diagram

$$\begin{array}{ccc}
W_{n}[\Delta_{n+1}] & \xrightarrow{\alpha_{n+1}} & R_{n+1,m(n+1)} \\
\downarrow & & \downarrow \\
W_{n}[\Delta_{n}] & \xrightarrow{\alpha_{n}} & R_{n,m(n)}
\end{array}$$

is commutative for all $n > 0$ (and by (Q0), $\alpha_n$ is injective for all $n$).

(Q4) There exists an ordered set of generators $\{f_1^{(n)}, \ldots, f_r^{(n)}\} \subset \mathfrak{m}R_{n,m(n)}$ of $R_{n,m(n)}$ over $W$ for the integer $r$ in (Q1) such that $\pi_{n+1}^{n+1}(f_j^{(n+1)}) = f_j^{(n)}$ for each $j = 1, 2, \ldots, r$. In our case of $\overrightarrow{p} = \text{Im} \overrightarrow{\varphi}$, we can make the choice of generators canonical to good extent dependent on $Q_m(n)$ (see Theorem 6.4).

(Q5) $R_{\infty} := \lim_{n \to \infty} R_{n,m(n)}$ is isomorphic to $W[[T_1, \ldots, T_r]]$ by sending $T_j$ to $f_j^{(\infty)} := \lim_{n \to \infty} f_j^{(n)}$ for each $j$ (e.g., [HMI, page 193]).

(Q6) Inside $R_{\infty}, \text{Im}_{n \to \infty} W_{n}[\Delta_{n}]$ is isomorphic to $W[[S_1, \ldots, S_r]]$ so that $s_j := (1 + S_j)$ is sent to the generator $\delta_q^{n} / \Delta_n^{\alpha} \text{ of } \Delta_n^{\alpha} / \Delta_n^{\alpha + 1}$ for the ordering $q_1, \ldots, q_r$ of primes in $Q_m$ in (Q3).

(Q7) $R_{\infty}/(S_1, \ldots, S_r) \simeq \lim_{n \to \infty} \overline{R}_{n,m(n)} \simeq R_\varphi \simeq \overline{\mathbb{T}}_\varphi$, where $R_\varphi$ is the universal deformation ring for the deformation functor $D_{Q_m,k/\psi}$ and $\mathbb{T}_\varphi$ is the local factor of the Hecke algebra $\mathfrak{h}_{Q_m}$ whose residual representation is isomorphic to $\overrightarrow{p}$.

(Q8) We have $R_{Q_m} \simeq \mathbb{T}_{Q_m}$ by the canonical morphism, and $R_{Q_m} \simeq R_{\infty}/\mathfrak{A}_{Q_m} R_{\infty}$ for the ideal $\mathfrak{A}_{Q_m} := ((1 + S_j)^{\delta_q^{n}} - 1)_{j=1,2,\ldots,r}$ of $W[[S_1, \ldots, S_r]]$ is a local complete intersection.
Lemma 3.1. Let $\chi := \left(\frac{F/Q}{\cdot}\right)$ as before. Then the involution $\sigma_{Q_m}$ on $T_{Q_m}$ acts on $\delta_q|_{I_q}$ (the image of $s_q = 1 + S_q$) for $q \in Q'_m$ by $\sigma_{Q_m}(\delta_q|_{I_q}) = (\delta_q|_{I_q})^{\chi(q)}$. In particular, the ideal $(p^n, \delta_q^{p^n} - 1)_{q \in Q_m}$ of $T_{Q_m}$ is stable under $\sigma_{Q_m}$, and the involution $\sigma = \sigma_n$ of $R_n = R_{n,m}$ induces an involution $\sigma_n$ of $\sigma_{Q_m}$. Thus, we get the desired result as the canonical morphism $R_{Q_m} \to T_{Q_m}$ is $W[\Delta_{Q_m}]$-linear.

Proof. For each $q \in Q$, by (2.1), the restriction of $\rho^Q$ to the inertia group $I_q \subset \text{Gal}(\overline{\mathbb{Q}}_q/Q)$ has the form $\left(\begin{array}{cc} \delta_q & 0 \\ 0 & \delta_q^{-1} \end{array}\right)$ and the choice of the eigenvalue $\overline{\sigma}_q$ determines the character $\delta_q$ (i.e., $\overline{\sigma}_q$-eigenspace of $\mathfrak{p}(\text{Frob}_q)$ is the image of $\delta_q^{-1}$-eigenspace in $\overline{\mathfrak{p}}$ by (2.3); see also [MFG, Theorem 3.32 and its proof] or [HMI, Theorem 3.75]). By tensoring $\chi$, $\overline{\sigma}_q$ is transformed to $\chi(q)\overline{\sigma}_q = \overline{\chi}_q$, and hence $\delta_q$ will be transformed to $\delta_q^{\chi(q)}$ under $\sigma_{Q_m}$. Therefore, $\sigma_{Q_m} \in \text{Aut}(T_{Q_m})$ induces an involution $\sigma_n$ on $R_n = R_{n,m} = T_{Q_m}/(p^n, \delta_q^{p^n} - 1)_{q \in Q_m}$. □

We recall the way Wiles chose the sets $Q$ as we make a finer choice building on his way relating $q \in Q$ with generator choice $f_j$. Write $Ad$ for the adjoint representation of $\overline{\mathfrak{p}}$ acting on $s_4(\mathbb{F})$ by conjugation, and put $Ad^\ast$ for the $\mathbb{F}$-contragredient. Then $Ad^\ast(1)$ is one time Tate twist of $Ad^\ast$. Note that $Ad^\ast \cong Ad$ by the trace pairing as $p$ is odd. Let $Q$ be a finite set of primes, and consider

$$\beta_Q : H^1(Q^{(QNP)}/\mathbb{Q}, Ad) \to \prod_{q \in Q} H^1(Q_q, Ad),$$

$$\beta_Q' : H^1(Q^{(QNP)}/\mathbb{Q}, Ad^\ast(1)) \to \prod_{q \in Q} H^1(Q_q, Ad^\ast(1)).$$

Here is a lemma due to A. Wiles [Wi95, Lemma 1.12] which shows the existence of the sets $Q_m$. We state the lemma slightly different from [Wi95, Lemma 1.12], and for that, we write $K_1 = \mathbb{Q}^{\text{ker} Ad}$ (the splitting field of $Ad = Ad(\overline{\mathfrak{p}})$). Since $Ad \cong \overline{\chi} \oplus \text{Ind}_F^{\mathbb{Q}} \overline{\chi}^\ast$, we have $K_1 = F(\varphi^-)$.

Lemma 3.2. Assume (W). Pick $0 \neq x \in \text{Ker}(\beta_Q')$ and $0 \neq y \in \text{Ker}(\beta_Q)$, and write

$$f_x : \text{Gal}(Q^{(QNP)}/K_1(\mu_p))/K_1(\mu_p) \to Ad^\ast(1) \in \text{Hom}_{\text{Gal}(K_1(\mu_p)/Q)}(\text{Gal}(Q^{(QNP)}/K_1), Ad^\ast(1))$$

$$f_y : \text{Gal}(Q^{(QNP)}/K_1)/K_1 \to Ad \in \text{Hom}_{\text{Gal}(K_1/Q)}(\text{Gal}(Q^{(QNP)}/K_1), Ad)$$

for the restriction of the cocycle representing $x$ and $y$ to $\text{Gal}(Q^{(QNP)}/K_1(\mu_p))$ and $\text{Gal}(Q^{(QNP)}/K_1)$, respectively. Let $\overline{\rho}$ be the composite of $\overline{\rho}$ with the projection $GL_2(\mathbb{F}) \to PGL_2(\mathbb{F})$, and pick a positive integer $C$ which is a product of primes $l \neq p$ split in $F/\mathbb{Q}$. Then, $f_x$ (resp. $f_y$) factors through $\text{Gal}(Q^{(QNP)}/K_1(\mu_p))$ (resp. $\text{Gal}(Q^{(QNP)}/K_1)$), and there exists $\sigma_i \in \text{Gal}(Q^{(QNP)}/\mathbb{Q})$ for $i = x, y$ such that

1. $\overline{\rho}(\sigma_i) \neq 1$ (so, $Ad(\sigma_i) \neq 1$).
2. $\sigma_i$ fixes $Q(\mu_{C^{p^m}})$ for an integer $m > 0$.
3. $f_i(\sigma_i^a) \neq 0$ for $a := \text{ord}(\overline{\rho}(\sigma_i)) = \text{ord}(Ad(\sigma_i))$.

The argument is the same for $x$ and $y$, we give Wiles’ proof in details for $x$ and indicate how to modify the argument for $y$ at the end of the proof. Strictly speaking, [Wi95, Lemma 1.12] gives the above statement replacing $K_1$ by the splitting field $K_0$ of $\overline{\mathfrak{p}}$. Since the statement is about the cohomology group of $Ad$ (and $Ad^\ast(1)$), we can replace $K_0$ in his argument by $K_1$. We note also $\text{Ker}(Ad(\overline{\mathfrak{p}})) = \text{Ker}(\overline{\rho})$ as the kernel of the adjoint representation: $GL(2) \to GL_3$ is the center of $GL_2$ (so it factors through $PGL_2$).

Proof. Since $x \in \text{Ker}(\beta_Q')$, $f_x$ is unramified at $q \in Q$; so, $f_x$ factors through $\text{Gal}(Q^{(QNP)}/K_1(\mu_p))$.

We have two possibilities of $F' := K_1 \cap \mathbb{Q}(\mu_{C^{p^m}})$; i.e., $F' = \mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$ disjoint from $F$. Indeed, the maximal abelian extension of $\mathbb{Q}$ inside $K_1$ is either $F$ (when $\text{ord}((\overline{\mathfrak{p}}^-))$ is odd $> 1$) or a composite $FF'$ of the quadratic extensions $F$ and $F'$ over $\mathbb{Q}$ (if $\text{ord}((\overline{\mathfrak{p}}^-))$ is even...
If $\varphi^-$ has odd order, $F' = \mathbb{Q}(\mu_{p^m}) \cap K^1 = \mathbb{Q}$ as it is a subfield of $F$ and $\mathbb{Q}(\mu_{Cp^m})$ (because $(C,D) = 1$ and $F \cap (\mathbb{Q}(\mu_p)) = \mathbb{Q}$).

Assume that $\text{ord}(\varphi^-) = 2n > 3$. Let $D := \text{Gal}(K_1/\mathbb{Q})$ and $C := \text{Gal}(K_1/F)$. Then $C$ is a cyclic group of order $2n$. Pick a generator $g \in C$. Then $D = C \cup Cc$ for complex conjugation $c$, and we have a characterization $Cc = \{ r \in D | trg^{-1} = g^{-1}, \tau^2 = 1 \}$. For the derived group $D'$ of $D$, we have $D'^{ab} = D/D' \cong (\mathbb{Z}/2\mathbb{Z})^2$. We have $K_1^{D'} = FF'$, and $\text{Gal}(K_1/F')$ is equal to $C^2 \times \langle c \rangle$ (a dihedral group of order $2n$). If $n > 2$ (so, $2n > 4$), $\text{Ind}_{D}^{C}(\varphi^-)$ restricted to $\text{Gal}(K_1/F')$ is still irreducible isomorphic to $\text{Ind}_{D}^{C}(\varphi^-)$.

If $n = 2$, $F'$ is a unique quadratic extension in $K_1^{D'}$ unramified at $D$. In any case, $F' \neq F$ which is quadratic over $\mathbb{Q}$. Since $F' = \mathbb{Q}(\mu_{Cp^m}) \cap K_1$ is at most quadratic disjoint from $F$, we can achieve (1)-(2) by picking up suitable $\tau$ in $C^2 \times \langle c \rangle$ because $Ad = \chi \oplus \text{Ind}_{F}^{C}(\varphi^-)$.

Let $M_x := \mathbb{Q}^{K_1}(f_x)$. Then $Y := \text{Gal}(M_x/K_1(\mu_p))$ is embedded into $Ad^*(1)$ by $f_x$ and $f_x$ is equivariant under the action of $\text{Gal}(K_1(\mu_p)/\mathbb{Q})$ which acts on $Y$ by conjugation. Since $Ad = \chi \oplus \text{Ind}_{F}^{C}(\varphi^-)$, we have two irreducible invariant subspaces $X \subset Ad^*(1): X = \mathcal{O}_F$ and $\text{Ind}_{C}^{F}(\varphi^-)$. Thus $f_x(Y)$ contains one of $X$ as above. By (1), $\varphi(\sigma) \sim \left( \begin{smallmatrix} 0 & \alpha \\ -\alpha & 0 \end{smallmatrix} \right)$ with $\alpha \neq \beta$. By (2), $\alpha \beta = 1$ and hence $\alpha$ is a primitive $\alpha$-th root of unity with $\alpha > 1$, and $\alpha^2 \notin \{ 1 \}$. The eigenvalue of $Ad^*(1)(\sigma)$ is therefore $\alpha^2, 1, \alpha^{-2}$, which are distinct.

If $f_x(Y) \supset X$, we claim to find $\sigma$ satisfying (1), (2) and $\sigma$ has eigenvalue $1$ in $X$. If $X = \mathcal{O}_F$, the splitting field of $X$ is $F(\mu_p)$. Note that $F(\mu_{Cp^m})$ is abelian over $\mathbb{Q}$. Thus choosing $\sigma$ fixing $F(\mu_{Cp^m})$ with $\sigma \in C^2 \times \langle c \rangle$, and having $\text{ord}(\varphi^-)(\sigma) \geq \text{ord}(\varphi^-)(2) = |C^2| \geq 2$, we have $\sigma$ has eigenvalue $1$ on $X = \mathcal{O}_F$.

If $X = \text{Ind}_{C}^{F}(\varphi^-)$, we just choose $\sigma \in \text{Gal}(K_1(\mu_{Cp^m})/\mathbb{Q}(\mu_{Cp^m}))$ inducing the non-trivial automorphism on $F$ (i.e., the projection to the factor $\langle c \rangle$ of $C^2 \times \langle c \rangle$ is non-trivial). Since $\sigma$ fixes $\mathbb{Q}(\mu_{Cp^m})$, we have $\omega(\sigma) = 1$; so, we forget about $\omega$-twist. Then on $X$, $Ad^*(\sigma)$ has eigenvalue $-1$, and hence $Ad^*(\sigma)$ has to have the eigenvalue on $\text{Ind}_{C}^{F}(\varphi^-)$.

Since $f_x(Y) \supset X[1] = \{ v \in X[1] | Ad(\sigma)(v) = v \}$, we can find $1 \neq \tau \in Y$ such that $f_x(\tau) \in X[1]$; so, $f_x(\tau) \neq 0$. Thus $\tau$ commutes with $\sigma \in \text{Gal}(M_x/\mathbb{Q})$. This shows $(\sigma \tau)^a = \sigma^a \tau^a$, and $f_x((\sigma \tau)^a) = f(x(\sigma \tau)^a) = f(x(\sigma^a \tau^a))$. Since $f_x(\tau) \neq 0$, at least one of $f(x(\sigma^a \tau^a))$ is non-zero. Then $x_\sigma = \sigma$ or $x_\sigma = \sigma^a$ satisfies the condition (3) in addition to (1-2).

Now we describe the case for $f_y$. In this case, we write $M_y$ for the splitting field of $f_y$ over $K_1$.

We put $Y := \text{Gal}(M_y/K_1)$. Since $AD = \chi \oplus \text{Ind}_{F}^{C}(\varphi^-)$, for $X = \chi \oplus \text{Ind}_{F}^{C}(\varphi^-)$, we have $f_y(Y) \supset X$. Then we argue in exactly the same way as above and find $f_y$ with the required property. □

Let $Q = \emptyset$ and choose a basis $\{ x \}$ over $F$ of the “dual” Selmer group $\text{Sel}_F^1(D^*(1))$ inside $H^1(\mathbb{Q}(Np)/\mathbb{Q}, D^*(1))$ (see (3.2) below for the definition of the Selmer group). Then Wiles’ choice of $Q_m$ is a set of primes $q$ so that $\text{Frob}_q = \sigma_x$ on $M_x$ as in the above lemma. By Chebotarev density, we have infinitely many sets $Q_m$ with this property.

**Corollary 3.3.** Let the assumptions and the notation be as in Lemma 3.2 and its proof. Assume that $0 \neq f_x(\text{Gal}(M_x/K_1(\mu_p))) \subset \text{Ind}_{F}^{C}(\varphi^-)$ and $0 \neq f_y(\text{Gal}(M_y/K_1)) \subset \text{Ind}_{F}^{C}(\varphi^-)$. If $p > 3$, then there exists $\sigma \in \text{Gal}(\mathbb{Q}(Np)/\mathbb{Q})$ for $f = x, y$ such that

1. $\bar{p}(\sigma) \neq 1$,
2. $\sigma$ fixes $\mathbb{Q}(\mu_{Cp^m})$,
3. $f_x(\sigma^a) \neq 0$ and $f_y(\sigma^a) \neq 0$ for $a := \text{ord}(\varphi^-)(\sigma)$.

**Proof.** We first show that $\varphi^-$ on $\text{Gal}(K_1(\mu_p)/K_1)$ is non-trivial. Let $F' = K_1 \cap F(\mu_p)$. Thus $F'$ is an abelian extension of $\mathbb{Q}$. Since $\text{Gal}(K_1/F)$ is a dihedral group, its maximal abelian quotient has either order 2 or order 4 according as $\varphi^-$ has odd order or even order. If it has odd order, we have $\text{Gal}(F'/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ (as any element in the Galois group has order 2). Thus if $\varphi^-$ has an odd order, we have $F' = F$.

Suppose $\text{Gal}(F'/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Then $\varphi^-$ must have even order $2n > 3$. Since we have only three quadratic subfields in $F(\mu_p)$, i.e., $F, \mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{-D})$ for $p^* = (-1)^{(p-1)/2}$. We have $F' = F(\sqrt{p})$ which is a splitting field of $(\varphi^-)^2$. Thus if $F(\mu_p) = F'$, we have $p = 3$. This is not the case, as we have assumed that $p > 3$. Thus $K_1(\mu_p) \neq K_1$ and hence $\varphi^-$ on $\text{Gal}(K_1(\mu_p)/K_1)$ is non-trivial.
Note that $f_x(\text{Gal}(M_x/K_1(\mu_p)) \subset \text{Ind}_F^\varnothing \varnothing^{-1}$ and $f_y(\text{Gal}(M_y/K_1)) \subset \text{Ind}_F^\varnothing \varnothing^{-1}$ and that $f_x$ and $f_y$ are $F[\text{Gal}(K_1(\mu_p)/Q)]$-linear. Here the Galois group $\tau \in \text{Gal}(K_1(\mu_p)/Q)$ acts on $\text{Gal}(M_x/K_1(\mu_p))$ and $\text{Gal}(M_y/K_1(\mu_p))$ by $\tau g = \bar{\tau}g^{-1}$ taking a lift $\bar{\tau} \in \text{Gal}(Q(N^P)/K_1(\mu_p))$ of $\tau$ (i.e., $\bar{\tau}|_{K_1(\mu_p)} = \tau$). We may assume that $\mathbb{F}$ is generated over $\mathbb{F}_p$ by the values of $\varnothing^{-1}$ (and hence $\mathbb{F}$ is generated over $\mathbb{F}_p$ by the values of $\varnothing^{-1}$ as $\varnothing$ has values in $\mathbb{F}_p$). Thus $f_y$ restricted to $\text{Gal}(Q(N^P)/K_1(\mu_p))$ has image isomorphic to $\text{Ind}_F^\varnothing \varnothing^{-1}$ as $\text{Gal}(Q(N^P)/Q(\mu_p))$-modules; i.e.,

$$X_y := f_y(\text{Gal}(M_y/K_1(\mu_p)) \cong f_x(\text{Gal}(M_x/K_1(\mu_p)) =: X_x$$

as $\text{Gal}(Q(N^P)/Q(\mu_p))$-modules, since $\text{Gal}(K_1(\mu_p)/Q)$ acts on $X_y$ via the quotient $\text{Gal}(F(\varnothing^{-1})/Q)$ for the splitting field $F(\varnothing^{-1}) = \text{Ker}(\varnothing^{-1})$. Thus we have two possibilities inside $Q(N^P)$: (i) $M_y(\mu_p) = M_x$ or (ii) $M_y(\mu_p) \neq M_x$. If $\text{Ind}_F^\varnothing \varnothing^{-1} \cong \text{Ind}_F^\varnothing \varnothing^{-1}$ as $\text{Gal}(Q(N^P)/\mathbb{Q})$-modules, $\varnothing^{-1}$ has to be quadratic and $p = 3$ and $p$ ramifies in $F/Q$. This is impossible by our assumption $p \nmid D$. Thus we may assume that $\text{Ind}_F^\varnothing \varnothing^{-1} \cong \text{Ind}_F^\varnothing \varnothing^{-1}$ as $\text{Gal}(K_1(\mu_p)/\mathbb{Q})$-modules.

Since $f_x$ and $f_y$ are $F[\text{Gal}(K_1(\mu_p)/Q)]$-linear and the values of $\varnothing^{-1}$ generate $F$ over $\mathbb{F}_p$, $X_x \cong \text{Ind}_F^\varnothing \varnothing^{-1}$ as $\text{Gal}(K_1(\mu_p)/Q)$-modules and $X_y \cong \text{Ind}_F^\varnothing \varnothing^{-1}$ as $\text{Gal}(K_1(Q)/Q)$-modules. In particular, elements $\xi \in \text{Gal}(K_1(\mu_p)/K_1)$ acts on $X_x$ by the scalar multiplication by $\varnothing^{-1}(\xi)$ and on $X_y$ trivially. As a $\text{Gal}(K_1(\mu_p)/K_1)$-module, the Galois group $Z := \text{Gal}(M_y/(\mu_p) \cap M_x)/K_1(\mu_p))$ is the quotient of $X_x$ and $X_y$, which implies $Z$ is trivial; so, $M_y(\mu_p) \cap M_x = K_1(\mu_p)$. Thus $M_y(\mu_p)$ and $M_x$ are linearly disjoint over $K_1(\mu_p)$. Then starting with the same $\sigma_0$ as in the proof of Lemma 3.2 to find $\sigma_x$ and $\sigma_y$, we find $\sigma_x \in \text{Gal}(M_x/Q)$ and $\sigma_y \in \text{Gal}(M_y(\mu_p)/Q)$ (satisfying the requirements of Lemma 3.2 respectively for $\text{Ind}_F^\varnothing \varnothing^{-1}$ and $\text{Ind}_F^\varnothing \varnothing^{-1}$) which coincides with $\sigma_0|_{K_1(\mu_p)}$ over $K_1(\mu_p)$. Note that $\sigma_x^1|_{M_x} \times \sigma_y^1|_{M_y(\mu_p)}$ is in $\text{Gal}(M_x/K_1(\mu_p)) \times \text{Gal}(M_y(\mu_p)/K_1(\mu_p))$ which is isomorphic (by the restriction maps) to $\text{Gal}(M_xM_y/K_1(\mu_p))$ by linear disjointness of $M_x$ and $M_y(\mu_p)$ over $K_1(\mu_p)$. Thus we can find $\sigma' \in \text{Gal}(Q(N^P)/K_1(\mu_p))$ such that $\sigma'|_{M_x} = \sigma_x^1|_{M_x}$ and $\sigma'|_{M_y(\mu_p)} = \sigma_y^1|_{M_y(\mu_p)}$. Then $\sigma := \sigma_0\sigma'$ does the job.

Corollary 3.4. Let the notation be as in Lemma 3.2 and its proof. If $0 \neq f_x(Y) \subset \text{Ind}_F^\varnothing \varnothing^{-1}$, the field automorphism $\sigma$ in Lemma 3.2 satisfies $\left(\frac{E/Q}{\sigma}\right) = -1$. Otherwise, we can choose $\sigma$ so that $\left(\frac{E/Q}{\sigma}\right) = 1$.

Proof. In this case, we can have $X[1] \subset \text{Ind}_F^\varnothing \varnothing^{-1}$ in the above proof of the corollary is given by the subspace of “anti-scalars” $\{\left(\begin{array}{c} a \\ b \end{array}\right) | a \in F\} \subset \text{Ad}^*(1)$, and therefore the anti-diagonal trace map $T : \text{Ad}^*(1) \to F$ induces an isomorphism $X[1] \cong F$ and Ker$(T) = X[1]$ (as $p > 2$). Here the anti-diagonal trace means $T\left(\begin{array}{c} a b \\ c d \end{array}\right) = b + c$. This fact becomes important later in the proof of Corollary 6.3.

Definition 3.6. Let $\mathcal{Y}$ be the Galois group over $K_0F(\phi)$ of the maximal $p$-abelian extension $L_0$ of $K_0F(\phi)$ unramified outside $p$. Define $\mathcal{Y}^{-}(\phi) := \mathcal{Y}^{-} \otimes_{Z_p[\phi]}(\text{Gal}(F(\phi)/F), \mathbb{Z}_p[\phi])$ similarly to $Y^{-}(\phi)$ in the introduction. More generally write $\mathcal{Y}_Q^{-}(\phi)$ for the Galois group over $K_0F(\phi)$ of the maximal $p$-abelian extension $L_Q$ of $K_0F(\phi)$ unramified outside $p$ and $Q$. Define $\mathcal{Y}_Q^{-}(\phi) := \mathcal{Y}_Q^{-} \otimes_{Z_p[\phi]}(\text{Gal}(F(\phi)/F), \mathbb{Z}_p[\phi])$.

Thus we have a natural restriction map $\mathcal{Y}^{-} \to Y^{-}$ which is an isomorphism if $p \nmid h_F$. In particular $\mathcal{Y}^{-}(\phi) = Y^{-}(\phi)$ if $p \nmid h_F$.

Let $D_Q := D_Q(k, \psi_k)$ and $D_Q^\prime$ for the corresponding local functor at a prime $l|N_QP$ defined below (det) in Section 2. Regard $D_Q^\prime(\mathbb{F}[\epsilon])$ for the dual number $\epsilon$ as a subspace of $H^1(\mathbb{Q}_q, Ad)$ in the standard way: For $\rho \in D_Q^\prime(\mathbb{F}[\epsilon])$, we write $\rho \bar{\epsilon}^{-1} = 1 + \epsilon u_\rho$. Then $u_\rho$ is the cocycle with values in $s\mathbb{Q}(\mathbb{F}) = Ad$. Thus we have the orthogonal complement $D_Q^\prime(\mathbb{F}[\epsilon])^\perp \subset H^1(\mathbb{Q}_q, Ad^*(1))$ under Tate
local duality. We recall the definition of the Selmer group giving the global tangent space \( D_Q(\mathbb{F}[\epsilon]) \) and its dual from the work of Wiles and Taylor–Wiles (e.g., [HMI, §3.2.4]):

\[
\text{Sel}_Q(Ad) := \text{Ker}(H^1(Q(\mathbb{Q}^p)/\mathbb{Q}, \text{Ad})) \rightarrow \prod_{l \mid N_p} H^1(Q_l, \text{Ad})/\mathcal{D}_Q^l(\mathbb{F}[\epsilon])) \quad (\cong D_Q(\mathbb{F}[\epsilon]))
\]

(3.2)

\[
\text{Sel}_Q^l(Ad^*(1)) := \text{Ker}(H^1(Q(\mathbb{Q}^p)/\mathbb{Q}, Ad^*(1))) \rightarrow \prod_{l \mid N_p} H^1(Q_l, \text{Ad}^*(1)) \times \prod_{\ell \neq Q} H^1(Q_{\ell}, Ad^*(1)).
\]

**Remark 3.7.** As noticed in [CV03, Theorem 3.1], the decomposition \( Ad = \chi \oplus \text{Ind}_F^Q \varphi^- \) for \( \chi := (\chi \mod p) \), \( \text{Sel}_Q(Ad) \) (resp. \( \text{Sel}_Q^l(Ad^*(1)) \)) induces the direct sum of the Selmer groups \( \text{Sel}_Q(\chi) \) (resp. \( \text{Sel}_Q^l(\chi) \)) and \( \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) \) (resp. \( \text{Sel}_Q^l(\text{Ind}_F^Q \varphi^-) \)).

To prove the direct sum decomposition in Remark 3.7, we need to decompose \( \mathcal{D}_Q^l(\mathbb{F}[\epsilon]) \) as in (3.3) (which is equivalent to the decomposition of the original \( \mathcal{D}_Q^l(\mathbb{F}[\epsilon]) \)). We consider \( \text{Sel}_Q^l(Ad^*(1)) \) (whose decomposition as above is equivalent to (3.3) below). Then \( \mathcal{D}_Q^l(\mathbb{F}[\epsilon]) \) is made of classes of cocycles such that \( u,p,I_p \) is upper nilpotent and \( u,p,\text{Gal}(\mathbb{Q}_p, \mathbb{Q}) \) is upper triangular. Thus we confirm for \( l = p \) that

\[
\mathcal{D}_Q^p(\mathbb{F}[\epsilon]) = (\mathcal{D}_Q^p(\mathbb{F}[\epsilon]) \cap H^1(Q_l, \mathbb{Q})) \oplus (\mathcal{D}_Q^p(\mathbb{F}[\epsilon]) \cap H^1(Q_l, \text{Ind}^Q_F \varphi^-)),
\]

and \( \mathcal{D}_Q^p(\mathbb{F}[\epsilon]) \cap H^1(Q_p, \text{Ind}^Q_F \varphi^-) \) is made of upper nilpotent matrices in \( Ad^*(1) \) (since \( \text{Ind}_F^Q \varphi^- \) is the direct sum of the upper nilpotent Lie algebra and the lower nilpotent Lie algebra). Therefore \( \mathcal{D}_Q^p(\mathbb{F}[\epsilon]) \cap H^1(Q_p, \text{Ind}^Q_F \varphi^-) \) is the direct factor \( H^1(F_p, \varphi^-) \) of

\[
H^1(F_p, \text{Ind}_F^Q \varphi^-) = H^1(F_p, \varphi^-) \oplus H^1(F_p, \varphi^-)^{\sim},
\]

where \( \varphi^- \) (\( \tau \mapsto \varphi^-(\tau) \)) is complex conjugation. This implies

(3.4)

a cocycle \( u \) giving a class in \( \text{Sel}_Q^l(\text{Ind}^Q_F \varphi^-) \) is possibly ramified at \( p \) but trivial at \( F \).

We now compute \( \mathcal{D}_Q^p(\mathbb{F}[\epsilon]) \cap H^1(Q_p, \mathbb{Q}) \). Since \( \chi \) is trivial on \( \text{Gal}(\mathbb{Q}_p, Q_p) \), we have \( H^1(Q_p, \mathbb{Q}) = H^1(Q_p, \mathbb{Q}) \otimes \mathbb{Q} \) by Kummer theory. Since \( \varphi^- \) ramifies at \( p \), we have \( H^0(I_p, \mathbb{Q}) = 0 \), and by inflation and restriction sequence, we have an exact sequence:

\[
0 = H^1(\text{Frob}_p, H^0(I_p, \mathbb{Q})) \rightarrow H^1(Q_p, \mathbb{Q}) \rightarrow H^1(I_p, \mathbb{Q})^{\text{Frob}_p = 1} \rightarrow H^2(\text{Frob}_p, H^0(I_p, \mathbb{Q})) = 0.
\]

This implies all non-zero classes in \( H^1(Q_p, \mathbb{Q}) \) is ramified. Similarly, since \( \chi \) is unramified and \( \hat{\mathbb{Z}} \) has cohomological dimension 1, we have a commutative diagram with exact rows:

\[
\begin{array}{ccc}
H^1(\text{Frob}_p, \chi) & \longrightarrow & H^1(Q_p, \chi) \longrightarrow H^1(I_p, \chi)^{\text{Frob}_p = 1} \\
\downarrow & & \downarrow \\
\text{Hom}(\text{Frob}_p, \mathbb{F}) & \longrightarrow & \text{Hom}(Q_p, \mathbb{F}) \longrightarrow \text{Hom}(\hat{\mathbb{Z}}^{\times}, \mathbb{F})^{\text{Frob}_p = 1}.
\end{array}
\]

By the requirement of the cocycle in \( \mathcal{D}_Q^p(\mathbb{F}[\epsilon]) \) is upper nilpotent over \( I_p \) and is upper triangular over \( D_p := \text{Gal}(\mathbb{Q}_p/Q_p) \), we have \( \mathcal{D}_Q^p(\mathbb{F}[\epsilon]) \cap H^1(Q_p, \chi) = \text{Hom}(\text{Frob}_p, \mathbb{F}) \) whose \( p \)-local Tate dual is \((p^{\infty}/p^{\infty}) \otimes \mathbb{F} \subset (\mathbb{Q}_p^{\times}/(\mathbb{Q}_p^{\times})^p) \otimes \mathbb{F} = H^1(Q_p, \mathbb{Q}) \) by Kummer theory. Thus we have

\[
\mathcal{D}_Q^p(\mathbb{F}[\epsilon]) \cap H^1(Q_p, \mathbb{Q}) = H^1(I_p, \mathbb{Q})^{\text{Frob}_p = 1} = (\mathbb{Z}_p^{\times}/(\mathbb{Z}_p^{\times})^p) \otimes \mathbb{F}.
\]

So, it is ramified, and hence

(Km) the Selmer cocycle \( u \) in \( \text{Sel}_Q(\mathbb{Q}) \) for \( \chi \) can ramify at \( p \) and is a Kummer cocycle in \( (\mathbb{Z}_p^{\times}/(\mathbb{Z}_p^{\times})^p) \otimes \mathbb{F} \subset (\mathbb{Q}_p^{\times}/(\mathbb{Q}_p^{\times})^p) \otimes \mathbb{F} \) projecting down trivially to \( \mathbb{F} \) by sending \( z \in \mathbb{Q}_p^{\times} \) to its \( p \)-adic valuation modulo \( p \).

For a prime \( l \mid N_{F/Q}(\chi), \ Ad \equiv \chi \oplus \varphi^- \oplus (\varphi^-)^{-1} \) and \( Ad^*(1) \equiv \chi \oplus \varphi^- \oplus (\varphi^-)^{-1} \) over \( \text{Gal}(\mathbb{Q}_l/Q_l) \) (as \( F_l = Q_l \oplus \chi_l \)). Write \( \varphi^- \) (resp. \( \chi \)) for \( \varphi^- \) and \( \varphi^- \) (resp. for \( \chi \) and \( \chi \)) in order to treat the two cases at the same time. We normalize \( Ad \) so that the character \( \chi \) is realized on \( \mathbb{F}((\ell_{Q_l})) \) and \( \varphi^- \) appears on the upper nilpotent matrices and \( (\varphi^-)^{-1} \) acts on lower nilpotent matrices, and we also normalize \( Ad^*(1) \) accordingly. Since \( H^0(I_l, \varphi^-) = 0 \), we have an isomorphism \( H^1(Q_l, \varphi^-) \cong \mathbb{Z}_l^{\times}/(\mathbb{Z}_l^{\times})^p \otimes \mathbb{F} \).
We have the following facts:

\[ 0 \to H^1(I, \mathcal{P}) \to H^1(I, \mathcal{P}) \to \text{Hom}(\mathcal{P}(I), \mathcal{P}) \to H^2(I, \mathcal{P}). \]

Since \( \mathcal{P}(I) \) has order prime to \( p \), we have \( H^1(I, \mathcal{P}) = 0 \) for all \( j > 0 \). Thus \( H^1(I, \mathcal{P}) \cong \text{Hom}(\mathcal{P}(I), \mathcal{P}) \). Any elements in \( \text{Hom}(\mathcal{P}, \mathcal{P}) \) factors through the same quotient of \( I \) which is abelian, the conjugation action of \( \mathcal{P}(I) \) on \( \text{Ker}(\mathcal{P}|_I) \) is trivial, while \( \phi' \) is non-trivial; so, we conclude \( H^1(I, \mathcal{P}) \cong \text{Hom}(\mathcal{P}(I), \mathcal{P}) \) vanishes. Thus we get

\[ H^1(Q_\ell, \text{Ad}) = \text{Hom}(\text{Gal}(\mathcal{Q}_\ell/K), \mathcal{P}(I)) \cong \mathcal{P} \text{ and } H^1(Q_\ell, \text{Ad}^*(1)) = H^1(Q_\ell, \mathcal{P}(I)) \cong \mathcal{P} \]

where \( \mathcal{P} = \lim_{\mathcal{Q}_\ell \to 0} \mathcal{P} \).

We have the following facts:

\[ Y_\gamma := \text{Sel}(\text{Gal}(\mathcal{Q}_\ell/F), \mathcal{P}(I)) \]

and

\[ \mathcal{P}(I) = \mathcal{P}_0 \cong \text{Hom}(\text{Gal}(\mathcal{Q}_\ell/F), \mathcal{P}(I)) \]

for the maximal \( \ell \)-adic subfield of \( \mathcal{Q}_\ell \). The central idea behind the ANTICYCLOTOMIC CYCLICITY CONJECTURE is that the ray class group modulo \( \mathcal{Q}_\ell \) has an action of \( \text{Gal}(\mathcal{Q}_\ell/F) \) which is unramified outside \( \mathcal{Q}_\ell \), and hence

\[ \mathcal{P}(I) = \mathcal{P}_0 \cong \text{Hom}(\text{Gal}(\mathcal{Q}_\ell/F), \mathcal{P}(I)). \]

Thus any subgroup \( G \) of \( \text{Gal}(\mathcal{Q}_\ell/F) \) is stable under \( \text{Gal}(\mathcal{Q}_\ell/F) \), and hence any intermediate field \( X \) of \( \mathcal{Q}_\ell \) is a Galois extension over \( \mathcal{Q}_\ell \). Thus if \( X/F \) is unramified at \( \mathcal{Q}_\ell \), it is also unramified at \( \mathcal{Q}_\ell \). Since \( 
\mathcal{P}(I) \) is unramified at \( \mathcal{Q}_\ell \), it is also fully \( \mathcal{Q}_\ell \)-ramified and hence

\[ X = \text{Gal}(\mathcal{Q}_\ell/F). \]

Thus we have the vanishing of the \( \mathcal{Q}_\ell \)-eigenspace

\[ \text{Coker}(\mathcal{Y} \longrightarrow \text{Gal}(M_\ell/F(\mathcal{Q}_\ell))) \cong \text{Coker}(\mathcal{Y} \longrightarrow \text{Gal}(M_\ell/F(\mathcal{Q}_\ell))) \cong \mathbb{Z}_p[\text{Gal}(F(\mathcal{P}_\ell)/F)], \mathcal{P}_\ell \omega W = 0, \]
and we find \( \text{Gal}(M_{\omega}/F(\omega^{-})) \mid \omega^{-} = \chi^{-} \omega^{-})_H = H_0(H, \chi^{-} \omega^{-})) \) and
\[
\text{Hom}_{\text{Gal}(F(\omega^{-})/F)}(\text{Gal}(M_{\omega}/F(\omega^{-})), \overline{\omega}^{-}) = \text{Hom}(\chi^{-}(\omega^{-})_H, F) = \text{Hom}_{W[[H]]}(\chi^{-}(\omega^{-}), F).
\]

**Proposition 3.8.** Let \( C_{-}^{Q+} = \{ x \in C_{Q+} \mid c(x) = x^{-1} \} \), and write \( CL_{\chi^{-}}(p^{\infty}) \) for the class group of the splitting field of \( \chi^{-} \). Then, under (h0–4), we have \( \chi^{-} \omega^{-} = \chi^{-} \omega^{-} \) for \( Q \in Q, \)
\[
\text{Sel}_{Q}(\chi^{-}) \cong \text{Hom}(C_{-}^{Q+}, F) \text{ including } Q = 0, 
\]
\[
\text{Sel}_{Q}(\text{Ind}_{F}^{Q}(\varphi^{-})) \cong \text{Hom}_{W[[H]]}(\chi^{-}(\varphi^{-}), F) \text{ including } Q = 0, 
\]
\[
\text{Sel}_{b}^{\varphi}(\chi^{-}) \cong \text{Hom}(C_{1}(p^{\infty}), F)[\overline{\varphi}] 
\]
\[
\text{Sel}_{b}^{\varphi}(\chi^{-}) \cong \text{Hom}_{W[[H]]}(\chi^{-}(\varphi^{-}), F),
\]
\[
\text{Sel}_{b}^{\varphi}(\chi^{-}) \cong \text{Hom}_{W[[H]]}(\chi^{-}(\varphi^{-}), F),
\]
and
\[
\text{Sel}_{Q}(A_{d}) \cong \text{Hom}(C_{-}^{Q+}, F) \oplus \text{Hom}_{W[[H]]}(\chi^{-}(\varphi^{-}), F) \text{ including } Q = 0, 
\]
\[
\text{Sel}_{b}^{\varphi}(A_{d}(1)) \cong \text{Hom}(C_{1}(p^{\infty}), F)[\overline{\varphi}] \oplus \text{Hom}_{W[[H]]}(\chi^{-}(\varphi^{-}), F).
\]

**Proof.** We have already proven the last two identities of (3.5) and the second identity of (3.6). Thus we deal the rest. The subspace \( D_{Q}^{*}[[\mathbb{F}[\varphi]]] \) is made of classes of cocycles with values in \( Ad = s_{2}(F) \) such that \( u_0|_{I_{p}} \) is upper nilpotent and \( u_0|_{D_{p}} \) (\( D_{p} := \text{Gal}([\mathbb{Q}_{p}]/\mathbb{Q}_{p}) \)) is upper triangular. Similarly \( D_{Q}^{*}[[\mathbb{F}[\varphi]]] \) for \( l | N \) is made of classes of unramified cocycles \( u_{p} \) with values in diagonal matrices over \( D_{l} \). Then by the same argument proving (3.3) (or by the dual statement of (3.3)), we note that
\[
\text{Sel}_{Q}(Ad) = \text{Sel}_{Q}(\chi^{-}) \oplus \text{Sel}_{Q}(\text{Ind}_{F}^{Q}(\varphi^{-})),
\]
where \( \text{Sel}_{Q}(\chi^{-}) = \text{Ker}(H^{1}(Q^{QNP})/Q, \chi^{-}) \rightarrow \prod_{l | N} H^{1}(I_{l}, \chi^{-}) \) and
\[
\text{Sel}_{b}^{\varphi}(\chi^{-}) \cong \text{Ker}(H^{1}(Q^{QNP})/Q_{I}, \text{Ind}_{F}^{Q}(\varphi^{-})) \rightarrow \prod_{l | N} H^{1}(Q_{I}, \text{Ind}_{F}^{Q}(\varphi^{-})).
\]
By the inflation restriction sequence,
\[
\text{Sel}_{Q}(\chi^{-}) \cong \text{Ker}(\text{Hom}_{\text{Gal}(F/Q)}(\text{Gal}(F^{Q})), \chi^{-}) \rightarrow \prod_{l | N} H^{1}(I_{l}, \chi^{-}) \cong \text{Hom}(C_{-}^{Q+}, F).
\]
However the order of \( \text{Ker}(C_{1}^{-}, C_{-}^{Q+}) \) is \( \prod_{q \in Q^-}(q+1) \), which is prime to \( p \); so, we conclude
\[
\text{Sel}_{Q}(\chi^{-}) \cong \text{Hom}(C_{-}^{Q+}, F).
\]

Again by the inflation restriction sequence, identifying \( \text{Gal}(\mathbb{Q}_{p}/\mathbb{Q}) \) with the decomposition group at \( \mathbb{F} \), we have an exact sequence
\[
0 = H^{1}(\text{Frob}_{p}^{\mathbb{F}}, H^{0}(I_{p}, \varphi^{-})) \rightarrow H^{1}(I_{p}, \varphi^{-}) \rightarrow H^{1}(I_{p}, F(\varphi^{-}))_{\text{Frob}_{p}} \rightarrow 0,
\]
since \( H^{0}(I_{p}, \varphi^{-}) = 0 \) (i.e., \( \varphi^{-} \) ramified at \( p \) and also at \( \mathbb{F} \)). Thus we conclude
\[
\text{Ker}(H^{1}(I_{p}, \varphi^{-})) \rightarrow H^{1}(I_{p}, \varphi^{-}) = 0,
\]
and \( \text{Sel}_{Q}(\text{Ind}_{F}^{Q}(\varphi^{-})) \) is actually given (by replacing \( H^{1}(I_{p}, \varphi^{-}) \) by \( H^{1}(I_{p}, \varphi^{-}) \)) in (3.7)
\[
\text{Ker}(H^{1}(Q^{QNP})/Q, \text{Ind}_{F}^{Q}(\varphi^{-})) \rightarrow H^{1}(I_{p}, \varphi^{-}) \times \prod_{l | N} H^{1}(I_{l}, \text{Ind}_{F}^{Q}(\varphi^{-})).
\]
By the inflation-restriction sequence, we have an exact sequence \( H^{1}(\text{Frob}_{p}^{\mathbb{F}}, (\varphi^{-})_{I}) \rightarrow \prod_{l | N} H^{1}(I_{l}, \varphi^{-}) \), with \( (\varphi^{-})_{I} = 0 \) for \( l | N \), and hence by Shapiro’s lemma (and (h0)), we can rewrite
\[
\text{Sel}_{Q}(\text{Ind}_{F}^{Q}(\varphi^{-})) = \text{Ker}(H^{1}(Q^{QNP})/Q, \varphi^{-}) \rightarrow H^{1}(I_{p}, \varphi^{-}) \times \prod_{l | N} H^{1}(I_{l}, \varphi^{-})).
\]
where \( I \) running over all prime factors of \( N \) in \( F \). Thus, restricting to the Galois group over \( F(\overline{\sigma}) \), by the restriction-inflation sequence, we have

\[
\text{Sel}_Q(\text{Ind}_F^Q \sigma) \cong \text{Hom}_{W[[H_Q]]}(Y_Q(\sigma), \mathbb{F}).
\]

Similarly, \( \text{Sel}_Q(\overline{\chi}) \cong \text{Hom}_{\text{Gal}(F/\overline{Q})}(\text{Gal}(\mathbb{Q}(\mathbb{N}^p)/F), \overline{\chi}) = \text{Hom}(\text{Cl}_Q, \mathbb{F}) \). Therefore the first identity of (3.6) follows if we prove \( Y_Q^-(\sigma^-) \otimes_{W[[H_Q]]} \mathbb{F} = Y^-(-\sigma^-) \otimes_{W[[H]]} \mathbb{F} \).

To prove \( Y_Q^-(\sigma^-) \otimes_{W[[H_Q]]} \mathbb{F} = Y^-(-\sigma^-) \otimes_{W[[H]]} \mathbb{F} \), writing \( I_{\Omega}^p \) for the maximal \( p \)-abelian quotient of the inertia group \( I_{\Omega} \subset \text{Gal}(\overline{\mathbb{Q}}/K_Q F(\sigma^-)) \) of a prime \( \Omega \mid q \) in \( K_Q F(\sigma^-) \), we have an exact sequence

\[
\prod_{\Omega \mid q \in Q} I_{\Omega}^p \rightarrow Y_Q^- \rightarrow Y^- \rightarrow 0
\]

as \( \text{Ker}(Y_Q^- \rightarrow Y^-) \) is generated by the image \( I_{\Omega}^p \cong \mathbb{Z}_p \). The surjectivity of the restriction map: \( Y_Q^- \rightarrow Y^- \) follows from linear-disjointness of \( L_0 \) and \( K_Q F(\sigma^-) \) over \( K^-(\sigma^-) \) as at least one of \( q \in Q \) ramifies in any intermediate field of \( K_Q F(\sigma^-) \). Note that \( q \in Q^- \) totally splits in \( K_Q F(\sigma^-)/F \). Thus \( I_{\Omega q}^{-} := \prod_{\Omega \mid q} (I_{\Omega}^p) \) for \( q \in Q^- \) is isomorphic to

\[
Z_p^{\text{Gal}(K_Q F(\sigma^-)/F)} = Z_p[[\text{Gal}(K_Q F(\sigma^-)/F)]] = Z_p[[H_Q]][\text{Im}(\varphi^-)]
\]

as \( Z_p[[\text{Gal}(K_Q F(\sigma^-)/F)]] \)-modules. Since \( I_{\Omega q}^p \cong Z_p \) is the quotient of the maximal \( q \)-tame quotient of \( I_{\Omega q} \), \( \text{Frob}_q \) (for the prime \( q \in Q^- \) in \( F \)) acts on it via multiplication by \( q^2 \). Since \( \varphi^- \circ \text{Frob}_q = 1 \), the map \( I_q^- \otimes_{Z_p}[\text{Im}(\varphi^-)], \varphi^- W \rightarrow Y_Q^- \varphi^- W \) is the quotient of the maximal \( q \)-tame quotient of \( I_{\Omega q} \), \( \varphi^- W \) acts by multiplication by \( q^2 \). Thus we have \( I_q^- \otimes_{Z_p}[\text{Im}(\varphi^-)], \varphi^- W \cong W[[H_Q]]/(q^2 - 1). \)

The set \( \Omega_q^+ \) of primes \( \Omega \) in \( K_Q F(\sigma^-) \) above \( q \mid q \in Q^+ \) is a finite set on which the Galois group \( \text{Gal}(K_Q F(\sigma^-)/F) \) acts by permutation. Then, writing \( D(\Omega)/q \subset \text{Gal}(K_Q F(\sigma^-)/F) \) for the decomposition gruop of \( \Omega \), we have

\[
I_q^+ := \prod_{\Omega \in \Omega_q^+} I_{\Omega q}^p \cong Z_p^{\Omega_q^+} \cong Z_p[[\text{Gal}(K_Q F(\sigma^-)/F)/D(\Omega)/q]]
\]

on which \( \text{Frob}_q \) acts by \( \sigma D(\Omega)/q \rightarrow q \sigma \text{Frob}_q D(\Omega)/q = q \sigma D(\Omega)/q \) for \( \sigma \in \text{Gal}(K_Q F(\sigma^-)/F) \) and \( \Delta_q \subset H_Q \) act trivially. Thus putting \( I_q^+(\varphi^-) := I_q^+ \otimes_{Z_p}[\text{Im}(\varphi^-)], \varphi^- W \), we conclude from \( q \equiv 1 \mod p \)

\[
I_q^+(\varphi^-) \otimes_{W[[H_Q]]} \mathbb{F} = \begin{cases} 0 & \text{if } \varphi^- \circ \text{Frob}_q \neq 1, \\ \mathbb{F} & \text{if } \varphi^- \circ \text{Frob}_q = 1, \end{cases}
\]

since \( q \equiv 1 \mod p \) (i.e., after tensoring \( F \), \( \text{Frob}_q \) acts on \( F[\text{Gal}(K_Q F(\sigma^-)/F)/D(\Omega)/q] \) by multiplication by \( q \equiv 1 \mod p \)). By our choice of \( Q \in \Omega \), \( \mathbb{F}[\text{Frob}_q] \) has two distinct eigenvalues, and hence \( \varphi^- \circ \text{Frob}_q \neq 1 \). Thus we get the following isomorphism: \( Y_Q^- \otimes_{W[[H_Q]]} \mathbb{F} \cong Y^- \otimes_{W[[H]]} \mathbb{F} \) which implies

\[
Y_Q^-(\varphi^-) \otimes_{W[[H_Q]]} \mathbb{F} = Y^-(-\varphi^-) \otimes_{W[[H]]} \mathbb{F}
\]

as desired.

The primes \( q_x \in Q_m \) is indexed by a basis \( \{ x \}_{x} \) of the Selmer group \( \text{Sel}_Q^d(\text{Ad}^*(1)) \) so that \( f_x \) as in Lemma 3.2 has non-trivial value at \( \text{Frob}_{q_x} \). Thus writing \( Q_m^+ := \{ q \in Q_m | x(q) = \pm 1 \} \), we get from our choice in Corollary 3.4

\[
|Q_m^+| = \dim \text{Hom}_{W[[H]]}(Y^-(-\varphi^-), \mathbb{F}) \quad \text{and} \quad |Q_m^-| = \dim \text{Sel}_Q^d(\overline{\chi}).
\]
4. A sufficient condition for complete intersection property for $R_+$

We now claim to be able to add the compatibility (Q9) to the above list of the conditions (Q0–8):

(Q9) $\pi_{n+1}^n \circ \sigma_{n+1} = \sigma_n \circ \pi_{n+1}^n$, and the set $\{j_1^{(n)}, \ldots, j_r^{(n)}\}$ is made of eigenvectors of $\sigma_n$ for all $n$ (i.e., $\sigma_n(j_j^{(n)}) = \pm f_j^{(n)}$).

Lemma 4.1. We can find an infinite family $Q = \{Q_m\}_m$ of r-sets of primes outside $Np$ satisfying (Q0–9).

Proof. Pick an infinite family $Q$ satisfying (Q0–8). We modify $Q$ to have it satisfy (Q9). Since $p > 2$, plainly, $R_n$ is generated over $W$ by $\sigma_n$-eigenvectors $\{\sigma_n(f_j^{(n)}) \pm f_j^{(n)}\}_{j=1, \ldots, r}$. Since $r$ is larger than or equal to the minimal number of generators $\dim_{\mathbb{F}}{\mathcal{D}_{Q,m,k,\psi_\omega}(\mathbb{F}[\ell])}$ for the co-tangent space $t_{R_n} := m\mathcal{R}_n / (m^2\mathcal{R}_n + m_{\mathcal{W}})$, we can choose $r$ generators among $\{\sigma_n(f_j^{(n)}) \pm f_j^{(n)}\}$. Once compatibility $\pi_{n+1}^n \circ \sigma_{n+1} = \sigma_n \circ \pi_{n+1}^n$ is shown, we get

$$\pi_{n+1}^n(\sigma_n(f_j^{(n+1)}) \pm f_j^{(n+1)}) = \sigma_n(f_j^{(n)}) \pm f_j^{(n)}$$

for each $j$ from $\pi_{n+1}^n(f_j^{(n+1)}) = f_j^{(n)}$, so we may assume that the set of generators is made of eigenvectors of the involution (and is compatible with the projection $\pi_{n+1}^n$).

We now therefore show that we can make the system compatible with the involution. The triple with $0 < n \leq m(n)$:

$$(R_{n,m(n)}, \alpha), \tilde{R}_{n,m(n)}, (f_1, \ldots, f_r)$$

in the system (3.1) actually represents an isomorphism class $\mathcal{I}_n^{TW}$ made of infinite triples

$$\{(R_{n,m}, \alpha), \tilde{R}_{n,m}, (f_1, \ldots, f_r)\}_{m \geq n}$$

satisfying (Q0–8) with $m$ varying in the choosing process of $Q$ (of Taylor–Wiles; see [HMI, page 191] or [MFG, §3.2.6]). Then $m(n)$ is chosen to be minimal choice of $m$ in the class $\mathcal{I}_n^{TW}$; so, we can replace $m(n)$ by a bigger one if we want (as $\mathcal{I}_n^{TW}$ is an infinite set). In other words, choosing $m$ appearing in $\mathcal{I}_n^{TW}$ possibly bigger than $m(n)$, we would like to show that we are able to add the datum of the involution $\sigma$ induced by $\sigma_{Q_m}$. Therefore, we look into isomorphism classes in the infinite set of $(\sigma$-added) quadruples (varying $m$)

$$\{(R_{n,m}, \alpha), \tilde{R}_{n,m}, (f_1, \ldots, f_r), \sigma_{n,m}\}_{m \geq n+1}$$

of level $n$ in place of triples $\{(R_{n,m}, \alpha), \tilde{R}_{n,m}, (f_1, \ldots, f_r)\}_{m \geq n}$, where $\sigma_{n,m}$ indicates the involution of $R_{n,m}$ induced by $\sigma_{Q_m}$ (which is compatible with the projection $R_{n,m} \rightarrow \tilde{R}_{n,m}$).

We start an induction on $n$ to find the projective system satisfying $\pi_{n+1}^n \circ \sigma_{n+1} = \sigma_n \circ \pi_{n+1}^n$. The projection $\pi_{Q_m} : R_{Q_m} \rightarrow R_0$ (for any $m \geq 1$) of forgetting ramification at $Q_m$ is $\sigma$-compatible (by definition) for the involution $\sigma_{Q_m}$ and $\sigma_0$ coming from the $\chi$-twist, which induces a surjective $W$-algebra homomorphism $\tilde{\sigma}_0 : R_{1,m} \rightarrow R_{1,0}$ for $R_{1,0} = \mathbb{T}_0 / \mathbb{P}\mathbb{T}_0$ satisfying $\tilde{\sigma}_0^0 \circ \sigma_1 = \sigma_0 \circ \pi_0^1$. Thus the initial step of the induction is verified. In the same way, the projection $R_{n,m} \rightarrow \tilde{R}_{n,m}$ is compatible with the involution.

Now suppose that we find an isomorphism class $\mathcal{I}_n$ of the $(\sigma$-added) quadruples (indexed by $r$-sets $Q_m \in Q$ satisfying (Q0–9) varying $m$ with $m \geq n$) containing infinitely many quadruples of level $n$ whose reduction modulo $(p^{n-1}, \delta_q^{n-1} - 1)_{q \in Q}$ is in the unique isomorphism class $\mathcal{I}_{n-1}$ (already specified in the induction process). Since the subset of such $Q \in Q$ of level $m \geq n + 1$ (so $q \equiv 1 \mod p^{n+1}$ for all $q \in Q$) whose reduction modulo $(p^n, \delta_q^n - 1)_{q \in Q}$ falls in the isomorphism class $\mathcal{I}_n$ is infinite, we may replace $\mathcal{I}_n$ by an infinite subset $\mathcal{I}_n' \subset \mathcal{I}_n$ coming with this property (i.e., $m > n$), and we find an infinite set $\mathcal{I}_{n+1}'$ of $\{(R_{n,m+1}, \alpha), \tilde{R}_{n,m+1}, (f_1, \ldots, f_r), \sigma_{n,m+1}\}_{m \geq n+1}$ which surjects down modulo $(p^n, \delta_q^n - 1)_{q \in Q}$ isomorphically to a choice

$$\{(R_{n,m}, \alpha), \tilde{R}_{n,m}, (f_1, \ldots, f_r), \sigma_{n,m}\} \in \mathcal{I}_n$$

at the level $n$. Indeed if all $q \in Q$ satisfies $q \equiv 1 \mod p^{n+1}$, as we now vary $m$ so that $m > n$ (rather than $m \geq n$), we can use the same $Q = Q_m$ to choose the isomorphism class of level $n + 1$. Therefore, for $R_{Q,m} = \mathbb{T}_Q / (p^r, \delta_q^r - 1)_{q \in Q}$, the projections

$$R_{Q,n+1} \rightarrow R_{Q,n} \text{ and } \tilde{R}_{Q,n+1} = R_Q / (p^{n+1}, \delta_q^{n+1} - 1)_{q \in Q} \rightarrow \tilde{R}_{Q,n} = R_Q / (p^n, \delta_q^n - 1)_{q \in Q}$$

are isomorphisms.
are compatible with the involutions induced by \( \sigma_Q \), and hence for the same set of generators \( \{f_j\}_j \), the two quadruples
\[
\{(R_{Q,j}, \alpha), (R_{Q,j}, (f_1, \ldots, f_r), \sigma_j)\}_j
\]
of level \( j = n+1, n \) are automatically \( \sigma_j \)-compatible.

Since the number of isomorphism classes of level \( n+1 \) in \( \mathcal{I}_n \) is finite, we can choose an isomorphism class \( \mathcal{I}_{n+1} \) of level \( n+1 \) with \( \mathcal{I}_{n+1} = \infty \) inside \( \mathcal{I}_n \) whose members are isomorphic each other (this is the pigeon-hole principle argument of Taylor–Wiles). Thus by induction on \( n \), we get the desired compatibility \( \pi_{n+1}^r \circ \sigma_{n+1} = \sigma_n \circ \pi_{n+1}^r \) for \( \mathcal{I}_{n+1} \); i.e., \( \mathcal{I}_{n+1} \xrightarrow{\text{reduction}} \mathcal{I}_n \rightarrow \mathcal{I}_{n-1} \rightarrow \cdots \rightarrow \mathcal{I}_1 \) with \( \mathcal{I}_j = \infty \) for all \( j = 1, 2, \ldots, n+1 \). We hereafter write \( m(n) \) for the minimal of \( m \) with \((\mathcal{R}_n, m, \alpha), (\mathcal{R}_{n,m}, (f_1, \ldots, f_r), \sigma_{n,m}) \) appearing in \( \mathcal{I}_n \).

\[\square\]

Lemma 4.2. Suppose that the family \( Q = \{Q_m|m=1,2,\ldots\} \) satisfies (Q0–9). Define \( Q_\pm^m = \{q \in Q_m | \chi(q) = \pm 1\} \). Then \( |Q_m| (\text{and hence } |Q_\pm^m|) \) is independent of \( m \) for \( Q_m \in \mathcal{Q} \).

Proof. Since \( |Q_m| = \dim_\mathbb{F} \text{Hom}_{\mathcal{W}[\mathcal{H}]}(\mathcal{W}^{-}(\varphi^{-}\omega), \mathcal{F}) \) by Proposition 3.8, it is independent of \( m \). \( \square \)

By (Q9), we have the limit invariant \( \sigma_\infty \) acting on \( R_\infty = \lim_{\leftarrow n} R_{n,m(n)} \), and we may assume that the generators \( (f_j^{(n)}) \) to satisfy \( \sigma_n(f_j^{(n)}) = \pm f_j^{(n)} \). Therefore we may assume that \( (f_j^{(n)}, \ldots, f_r^{(n)}) = (f_j^{(1)}, \ldots, f_i^{(1)}, \ldots, f_r^{(1)}) \) and \( \sigma_\infty(f_j^{(n)}) = \pm f_j^{(n)} \) for \( r = r'+r'' \), and hence, we may assume that
\[
R_\infty \cong W[[T_1^+, \ldots, T_{r'+1}, T_{1-}, \ldots, T_{r''-}]]
\]
with variables \( T_j \) satisfying \( \sigma_\infty(T_j) = \pm T_j \) for \( r = r'+r'' \), and we have the following presentation for \( \mathfrak{A}_Q := \{s_j^{\Delta_{j-1}} - 1\}_j \):
\[
R_\infty/\mathfrak{A}_Q = W[[T_1^+, \ldots, T_{r'+1}, T_{1-}, \ldots, T_{r''-}]]/\mathfrak{A}_Q \cong \mathbb{T}_Q
\]
Strictly speaking, we may have to modify slightly the isomorphism class \( \mathcal{I}_n \) of tuples for each \( n \) to achieve this presentation (see the argument around (4.7) in the proof of the following Theorem 4.10).

Since \( \mathbb{T}_Q/\langle t - \gamma^k \rangle \mathbb{T} \cong \mathbb{T}_Q \), we can lift, as is well known, the above presentation over \( W \) and the involution \( \sigma_\infty \) to that of \( \mathbb{T}_Q \) over \( A \) to obtain:
\[
\Lambda[[T_1^+, \ldots, T_{r'+1}, T_{1-}, \ldots, T_{r''-}]]/\mathfrak{A}_Q \Lambda[[T_1^+, \ldots, T_{r'+1}, T_{1-}, \ldots, T_{r''-}]] \cong \mathbb{T}_Q
\]
where \( \sigma_\infty(T_j) = \pm T_j \) intact. We write simply \( \mathcal{R} = \mathcal{R}_\infty := \Lambda[[T_1^+, \ldots, T_{r'+1}, T_{1-}, \ldots, T_{r''-}]] \).

Here is a brief outline how to lift the presentation (cf. [MFG, §5.3.5]): Let \( f_j^{(\infty)} := \lim_{n \to \infty} f_j^{(n)} \).
Since \( f_j^{(n)} \) is an eigenvector of \( \sigma_n \), \( f_j^{(\infty)} \) is an eigenvector of \( \sigma_\infty \). Let \( \mathcal{R} := \Lambda[[T_1^+, \ldots, T_r^+]] \) and define an involution \( \sigma \) on \( \mathcal{R} \) by \( \sigma(T_i) = \pm T_i \iff \sigma_\infty(f_j^{(\infty)}) = \pm f_j^{(\infty)} \). Choose \( f_i \in \mathcal{R} \) such that \( f_i \mod (t - \gamma^k) = f_j^{(\infty)} \) and \( g_j \in \mathbb{T} = \mathbb{T}_Q \) such that \( g_j \mod (t - \gamma^k) \) giving the image of \( f_j^{(\infty)} \) in \( \mathbb{T}_Q \).
We can impose that these \( f_i \) and \( g_j \) are made of eigenvectors of the involution. By sending \( T_i = f_i \) to \( g_j \), we have \( \mathcal{R}/\mathfrak{A}_Q \mathcal{R} \cong \mathcal{R}, \mathcal{R}^+ \mathfrak{A}_Q = \mathcal{R}^+, /(t - \gamma^k) = \mathcal{R}_\infty \) and \( \mathcal{R}^+/((t - \gamma^k) = \mathcal{R}_\infty^+ \).

We reformulate the ring \( \mathbb{T}[S_1, \ldots, S_r] \) in terms of group algebras. Let \( \Delta_{Q_{m}}^\pm = \prod_{q \in Q_{m}} \Delta_{q} \) and \( \Delta_{n}^\pm := \prod_{q \in Q_{n}} \Delta_{q}/\Delta_{q}^n \); so, \( \Delta_{n} = \Delta_{n}^\pm \times \Delta_{n}^\pm \). Define \( p \)-profinite groups \( \Delta \) and \( \Delta_{\pm} \) by \( \Delta = \lim_{\leftarrow n} \Delta_{n} = Z_{p}^r \) and \( \Delta_{\pm} = \lim_{\leftarrow n} \Delta_{n}^\pm = Z_{p}^r \) for \( r := |Q_{m}| \). Here the limits are taken with respect to \( \pi_{n+1}^r \) restricted to \( \Delta_{n+1} \).

Set
\[
S := \mathbb{T}[\Delta] = \lim_{n \to \infty} \mathbb{T}[\Delta/\Delta_{n}^\pm] = \lim_{n \to \infty} \mathbb{T}[\Delta_{n}]
\]
for the \( p \)-profinite group \( \Delta = \lim_{\leftarrow n} \Delta_{n} = Z_{p}^r \) with \( \Delta = \Delta_{\pm} \times \Delta_{\pm} \) and \( A \) be a local \( S \)-algebra. Thus by identifying \( \Delta/\Delta_{n} \) with \( \Delta_{n} \), we have the identification \( S = \mathbb{T}[S_1, \ldots, S_r] \). The image \( S_n := W_n[\Delta_{n}] (W_n = W/p^nW) \) of \( S \) in \( R_n \) is a local complete intersection and hence Gorenstein.

We assume that the ordering of primes in \( Q \in \mathcal{Q} \) preserves \( Q_{m}^+ \) and \( Q_{m}^- \). In other words, the ordering of (Q3) induces \( Q_{m}^+ := \{q_1, \ldots, q_r\} \) and \( Q_{m}^- := \{q_{r+1} = q_1^+, \ldots, q_r = q_r^+\} \). We now write \( s_j^\pm \) for the generator of \( \Delta \) corresponding to \( \delta_{q_j} \).
Definition 4.3. Write $s_j^±$ for the generator of $\Delta_\pm$ corresponding to $\delta_j^±$. Then define $S_j^± := s_j^± − 1$ and $S_j^− := s_j^− (s_j^−)^{-1}$. Thus $\sigma_\infty(S_j^±) = ±S_j^±$. Write $G$ for the subgroup of involutions in $\text{Aut}(W[[\Delta]])/W)$ generated by the involutions $b_i (i = 1, \ldots, r)$ such that $b_i(S_j^−) = (−1)^{δ_i, j}S_j^−$ for Kronecker’s delta $δ_i, j$ and $b_i(S_j^+) = S_j^+$ for all $j = 1, 2, \ldots, r$. Put $S := S^G = W[[\Delta]]^G$.

Since $\sigma_\infty$ acts as $\sigma_\infty(S_j^−) = −S_j^−$ for all $j = 1, 2, \ldots, r$, the group $G = \langle \sigma \rangle$ embeds into $G$ so that $\sigma_\infty = \prod_j b_j$ on $W[[\Delta]]$.

For the ideal $a_n := \text{Ker}(W[[\Delta^+]] → W[[\Delta^+]])$ for $W_n := W/p^nW$, we put

$$a_n := a_n + ((s_1^−)^{p^n} − 1, \ldots, (s_r^−)^{p^n} − 1) \subset S$$

as an $S$-ideal. Then $a_n$ is stable under $\sigma$, and $\mathfrak{A}_n := \text{Ker}(S → W_n[[\Delta^+]])$. Put

$$\mathfrak{G}_n := \mathfrak{A}_n \cap W[[\Delta]^G] = \text{Ker}(W[[\Delta]^G → W_n[[\Delta^+]]^G])$$

$$= a_n + (((s_1^−)^{p^n} − 1) + \sigma((s_1^−)^{p^n} − 1), \ldots, ((s_r^−)^{p^n} − 1) + \sigma((s_r^−)^{p^n} − 1))$$

By this expression, we confirm the following fact:

Lemma 4.4. The ring $S_n := S/\mathfrak{G}_n = W_n[[\Delta^+/\Delta^+]]^G$ is a local complete intersection over $W_n := W/p^nW$ and is a Gorenstein ring free of finite rank over $W_n$.

Using the natural projection $\Delta → \Delta_{Q_m}$ sending $s_j^±$ to $\delta_j^±$, we get $\mathfrak{A}_{Q_m} := \text{Ker}(S → W[[\Delta_{Q_m}]])$. Let $A$ be a local $S_m$-algebra for $S_m = S/\mathfrak{A}_n = W_n[[\Delta^+]]^G$ (and hence $A$ is an $S_m$-algebra for $S_m = S/\mathfrak{G}_n \subset S$). We suppose that $\sigma$ acts on $A$ as an involution extending its action on $S_m$. Then $\sigma$ acts on $A^1 := \text{Hom}_S(A, S_m)$ (resp. $A^# := \text{Hom}_S(A, S_n)$) by $f^σ(x) = \sigma(f(\sigma(x)))$. Indeed, $f^σ(sx) = \sigma(f(sx)) = \sigma(f(s))\sigma(x) = \sigma(\sigma(s))\sigma(f(\sigma(x))) = sf^σ(x)$, and hence $f^σ$ is $S$-linear. We put $S_\infty = S$ and $S_\infty = S$ and allow $n = \infty$.

Remark 4.5. Let $C ⊂ A$ be $B$-algebras. Suppose that

(1) $B$ and $C$ are Gorenstein,

(2) $A$ and $C$ are $B$-modules of finite type,

(3) $C$ is $B$-free of finite rank.

Then we have $\text{Hom}_B(C, B) \cong C$ as $B$-modules (cf., Lemma 11.1). Thus by [BAL, Proposition II.4.1.1],

$$\text{Hom}_C(A, C) \cong \text{Hom}_C(A, \text{Hom}_B(C, B)) \cong \text{Hom}_B(A \otimes_C C, B) = \text{Hom}_B(A, B).$$

This isomorphism is sending $g ∈ \text{Hom}_C(A, \text{Hom}_B(C, B))$ to $\bar{g} ∈ \text{Hom}_B(A \otimes_C C, B)$ given by $\bar{g}(a \otimes c) = g(a)c$. Applying this to $(A, B, C) := (R_n, S_n, S_m)$ and then to $(A, B, C) := (R_n, W_n, S_m)$, we get $A^# \cong A^1 \cong A^*$ as $A$-modules for $A^* = \text{Hom}_W(A, W_n)$. The identity $A^# \cong A^1$ is valid for $n = \infty$ also. Since the isomorphism $S_n \cong S_n^1$ can be chosen to be compatible with the action of $G$ (including $\sigma$), the isomorphisms

$$A^# \cong A^1 \cong A^*$$

can be chosen to be $\sigma$-compatible. Note that $W_n$-duality is equivalent to Pontryagin duality for profinite $W$-modules as long as $W$ is finite over $\mathbb{Z}_p$.

By the above remark, noting $R_\infty$ is free of finite rank over $S$, we get the following $\sigma$-compatible identity:

$$\lim_{n} R_n^1 \overset{(1)}{=} \lim_{n} R_n^# \overset{(2)}{=} \lim_{n} \text{Hom}_S(R_n, S_n)$$

$$\overset{(2)}{=} \lim_{n} \text{Hom}_S(R_\infty/\mathfrak{A}_n R_\infty, S/\mathfrak{A}_n) \cong \text{Hom}_S(R_\infty, S) \overset{(1)}{=} R_\infty^# \cong R_\infty^1.$$

Here the identities (1) are from Remark 4.5 and the identity (2) is by the fact: $R_n = R_\infty/\mathfrak{A}_n R_\infty$ and by the definition $S_n := S/\mathfrak{A}_n$.

Define

$$\text{Hom}_B(A, B)^\pm := \{ φ ∈ \text{Hom}_B(A, B) | φ \circ \sigma = ±\sigma \circ φ \}.$$
for $A = T_{Q_m}^f := \text{Hom}_{W[\Delta_{Q_m}]}(T_{Q_m}, W[\Delta_{Q_m}])$ or $R_{n}^i$ and $B = T_{Q_m}$ or $R_{n}$ accordingly. Write $\text{Isom}_B(A, B)^{\pm} \subset \text{Hom}_B(A, B)^{\pm}$ for the subset made of isomorphisms. Using the Gorenstein-ness of $T_{Q}$ for $Q = Q_m$ or $Q = \emptyset$ (which follows from the presentation (4.1) and for $Q = \emptyset$ from Theorem 2.1), by Lemma 11.2 (1) applied to the involution $\sigma_{Q_m}$ of $T_{Q_m}$, we have

$$\text{Isom}_{T_{Q_m}}(T_{Q_m}^f, T_{Q_m}^f)^{\epsilon} \neq \emptyset$$

for at least a sign $\epsilon \in \{\pm\}$.

**Lemma 4.6.** We have

$$\text{Isom}_{T_{Q_m}}(T_{Q_m}^f, T_{Q_m}^f)^{\epsilon} \neq \emptyset \Leftrightarrow \text{Isom}_{R_{n,m}}(R_{n,m}^i, R_{n,m}^i)^{\epsilon} \neq \emptyset$$

for each $0 < n \leq m$.

**Proof.** The direction $(\Rightarrow)$ is just reduction modulo $(p^n, \delta^n_q - 1)_{q \in Q_n}$. We prove the converse. If we have $\phi \in \text{Isom}_{R_{n,m}}(R_{n,m}^i, R_{n,m}^i)^{\epsilon}$, then $\sigma(\phi^{-1}(1)) = \varepsilon \phi^{-1}(1)$. We can lift $\phi^{-1}(1)$ to $v \in T_{Q_m}^f$ with $\sigma(v) = \varepsilon v$ so that $v \mod (p^n, \delta^n_q - 1)_{q \in Q_m} = \phi^{-1}(1)$. Define $\Phi : T_{Q_m} \to T_{Q_m}^f$ by $\Phi(t) = tv$. Then $\Phi$ is a $T_{Q_m}$-linear map. By definition, $\Phi \mod (p^n, \delta^n_q - 1)_{q \in Q_m} = \phi^{-1}$; so, by Nakayama’s lemma, $\Phi$ is onto. Since $T_{Q_m}$ and $T_{Q_m}^f$ are $W$-free of equal rank, $\Phi$ must be an isomorphism. Thus $\Phi^{-1} \in \text{Isom}_{R_{n,m}}(T_{Q_m}^f, T_{Q_m})^{\epsilon}$. \hfill \Box

We want to add one more datum $\phi_n \in \text{Isom}_{R_{n}}(R_{n}^i, R_{n}^i)^{\epsilon}$ to the data $((R_n, \alpha, \overline{R}_n, (f_1, \ldots, f_r), \sigma_n)$ which is required to satisfy the following compatibility condition:

(Q10) We have $\phi_n \in \text{Isom}_{R_{n}}(R_{n}^i, R_{n}^i)^{\epsilon}$ with $\epsilon \in \{\pm\}$ independent of $n$ for all $n > 0$.

**Remark 4.7.** Let $A$ and $B$ be a finite Gorenstein local rings of residual characteristic $p$. We suppose to have a surjective ring homomorphism $\pi : A \to B$. By adding $*$, we denote the Pontryagin dual module. Since $A$ and $B$ are Gorenstein, we have isomorphisms $A^* \cong A$ as $A$-modules and $B^* \cong B$ as $B$-modules. Thus we have a diagram

$$A \xrightarrow{\pi} B,$$

$$\begin{array}{c}
t \downarrow \phi_A \downarrow \phi_B \downarrow \varepsilon_B \downarrow \phi_A \downarrow \\
A^* \xrightarrow{\varepsilon} B^*. \end{array}$$

By defining $\varepsilon := \phi_B^{-1} \circ \pi \circ \phi_A$, the above diagram is commutative. Thus we can always adjust $A^* \to B^*$ making the above diagram commutative. Suppose that $A$ and $B$ have involutions $\sigma_X \subset X$ for $X = A, B$. By duality, the involution $\sigma_X$ acts on the dual $X^*$, which we denote by $\sigma_{X^*}$. If $\phi_X \circ \sigma_X = \varepsilon \sigma_X \circ \phi_X$ for $\varepsilon = \pm 1$ independent of $X = A, B$ and $\sigma_B \circ \pi = \pi \circ \sigma_A$, we have

$$\varepsilon \circ \sigma_A := \phi_B^{-1} \circ \pi \circ \phi_A \circ \sigma_A = \phi_B^{-1} \circ \pi \circ \varepsilon \sigma_A \circ \phi_A = \phi_B^{-1} \circ \varepsilon \sigma_A \circ \pi \circ \phi_A = \varepsilon \sigma_B \circ \phi_B^{-1} \circ \pi \circ \phi_A = \sigma_B \circ \varepsilon.$$

Thus the adjusted $\varepsilon$ commutes with the involution.

This remark shows that if we have a projective system $\{(R_n, \alpha, \overline{R}_n, (f_1, \ldots, f_r), \sigma_n)\}_{n}$ satisfying (Q0-9), we can add the datum of an $R_{n}$-linear isomorphism $\phi_n : R_{n}^i \cong R_{n}^i$ compatible with $\sigma$; i.e., (Q10) is automatically satisfied for $\phi_n$ induced by $\phi_{Q_{m(n)}}$ as long as we can take $\phi_{Q_{m(n)}} \in \text{Isom}_{T_{Q_m}}(T_{Q_m}^f, T_{Q_m})^{\epsilon}$ with $\epsilon$ independent of $m(n)$. Explicitly, the compatibility of $\phi_n$ means the following:

1. the datum $\phi_n$ satisfies $\phi_n \circ \sigma_n^* = \varepsilon \sigma_n \circ \phi_n$ for all $n$ and for $\varepsilon$ as in (Q10) independent of $m = m(n)$, and
2. the projections $\pi_{n', n} : R_{n'} \to R_{n}$ and $\varepsilon_{n', n} : R_{n'}^f = R_{n'}^f \to R_{n}^f$ for all $n' > n$ commute with the involution in addition to the commutativity of the diagram:

$$\begin{array}{c}
R_{n'} \xrightarrow{\pi_{n', n}} R_{n} \\
\downarrow \phi_{n'} \downarrow \phi_n \\
R_{n'} \xrightarrow{\varepsilon_{n', n}} R_{n}^f. \end{array}$$
Now we again go through the Taylor-Wiles system argument made of the augmented tuples
\[(R_n, \alpha), \tilde{R}_n, (f_1, \ldots, f_r), \sigma_n, \phi_n)\]
with \(\phi_n = (\phi_{Q_m}, \mod (p^n, \delta_{Q_m}^n - 1))_{m \in Q_m} \in \text{Isom}_{R_n}(R^I_n, R^n_q)^G\) for \(m = m(n)\); then, we obtain \(R_\infty\) with the limit involution \(\sigma_\infty\) and the limit isomorphism \(\phi_\infty \in \text{Isom}_{R_\infty}(R^I_\infty, R_\infty)^G\). Here \(R^I_n = \text{Hom}_S(R_n, S_n)\). Thus we get

**Corollary 4.8.** Suppose (h0–4). Then we can choose the Taylor–Wiles projective system
\[(R_n, \alpha), \tilde{R}_n, (f_1, \ldots, f_r), \sigma_n, \phi_n)\]
satisfying (Q0–10). If \(\varepsilon = +\) in (Q10), then we conclude that \(R^+_\infty\) is a Gorenstein ring over \(S = S^G\), \(R_\infty/\mathfrak{A}_{Q_m} R_\infty \cong R_{Q_m} \cong T_{Q_m}\).

Here is a prototypical example of the rings of type \(R_\infty, R^+_\infty\) corresponding to the choice \(r_+ = r' = 0\) and \(r_- = r'' = 1\):

**Example 4.9.** Consider \(0 \neq \delta \in \mathfrak{m}_W\) and put
\[W[\sqrt{\delta}] = \begin{cases} W + W\sqrt{\delta} & \text{if } \delta \notin W^2, \\ \{(x, y) \in W + W | (x \mod \sqrt{\delta}) = y \mod \sqrt{\delta}\} & \text{if } \sqrt{\delta} \in W. \end{cases}\]

Define
\[A = \{(x, y) \in W \oplus W[\sqrt{\delta}] | (x \mod \sqrt{\delta}) = (y \mod \sqrt{\delta})\} \text{ and } B = \{(x, y) \in W + W | x \equiv y \mod (\delta)\}.\]

Note that \(A = W[[T_-]]/(S_-)\) with \(S_- = T_- (T^2 - \delta)\) by sending \(T_-\) to \((0, \sqrt{\delta}) \in A\) and \(B = W[[T^2]](T_-) S_-\) by sending \(T^2\) to \((0, \delta) \in B\). Then \(W[[T_-]] \supset W[[T^2]]\) and \(W[[T_-]] \supset W[[S_-]]\). We have an involution \(\sigma\) of \(W[[T_-]]\) over \(W[[T^2]]\) with \(\sigma(T_-) = -T_-\) and \(\sigma(S_-) = -S_-\).

For \(Q \in \mathbb{Q}\), recall \(r_- = |Q^-|\) with
\[Q^- := \{q \in Q | Q\text{ is inert in } F/\mathbb{Q}\} \text{ and } Q^+ := \{q \in Q | q\text{ is split in } F/\mathbb{Q}\}.\]

Now we would like to prove

**Theorem 4.10.** Suppose (h0–4) and that the family \(Q\) satisfies (Q0–10). Let \(Q \in \mathbb{Q} \neq Q = 0\). Suppose that \(\sigma\) is non-trivial on \(T_0 \) (so, non-trivial on \(T^0\)). Then we have \(\varepsilon = +\) in (Q10), and the following three assertions hold.

1. We have \(0 < r_- = \dim_\mathbb{F} \text{Hom}_W[|H|] (Q^-(\varphi^{-\omega}), \mathbb{F}) = r''\).

2. If \(r_- = 1\), the \(T^Q_\infty\)-module \(T^Q_\infty\) is generated by a single element over \(T^Q_\infty\).

3. If \(r_- = 1\), the ring \(T_+ = T^Q_\infty\) is a local complete intersection over \(\Lambda\). More generally, for \(Q \in \mathbb{Q}\), the rings \(T^Q_\infty\) and \(T^Q\) are local complete intersection.

**Proof.** By (Q9), \(\sigma\) is compatible with the projective system of tuples
\[(R_n, \alpha), \tilde{R}_n, (f_1, \ldots, f_r), \sigma_n) \in \mathcal{I}_n,\]
and by constancy of \(\varepsilon\), we can find an isomorphism class \(\mathcal{I}_n\) with \(|\mathcal{I}_n| = \infty\) of the tuples
\[(R_n, \alpha), \tilde{R}_n, (f_1, \ldots, f_r), \sigma_n, \phi_n)\]
with an extra datum \(\phi_n\) compatible with projections. Indeed, we will see in Lemma 5.3 that if \(\sigma\) is non-trivial on \(T^0\), we have \(\text{Isom}_{Q_m}(\mathcal{T}_{Q_m}^\dagger, \mathcal{T}_{Q_m})^{-}\) for all \(m\), where we recall \(\mathcal{T}_{Q_m}^\dagger = \text{Hom}_W[|\Delta_m|](T_{Q_m}^\dagger, \mathcal{T}_{Q_m})^{-}\), and hence \(\text{Isom}_{Q_m}(\mathcal{T}_{Q_m}^\dagger, \mathcal{T}_{Q_m})^{-} \neq 0\) by Lemma 11.2 (1), proving \(\varepsilon = +\) for \(\varepsilon\) in (Q10). As explained after Remark 4.7, by Lemma 4.6, we can add the datum \(\phi_n\) to our tuples without changing the isomorphism class \(\mathcal{I}_n\) as long as \(\varepsilon\) is constant for all \(Q_m\). In other words,
\[(R_n, \alpha), \tilde{R}_n, (f_1, \ldots, f_r), \sigma_n, \phi_n) \mapsto ((R_n, \alpha), \tilde{R}_n, (f_1, \ldots, f_r), \sigma_n)\]
induces a bijection between \(\mathcal{I}_n\) and \(\mathcal{I}_n\). Then by the finiteness of isomorphism classes of the tuples
\[(R_n, \alpha), \tilde{R}_n, (f_1, \ldots, f_r), \sigma_n, \phi_n)\]
of level \(n + 1\) in \(\mathcal{I}_n\) combined with infiniteness of \(\mathcal{I}_n\), the projection maps \(R_{n+1} \to R_n\) and its dual are compatible with \(\phi_j \in \text{Isom}_{R_j}(R_j^I, R_j^\dagger)\) for \(j = n + 1, n\) for \(R_j^I = \text{Hom}_{S_j}(R_j, S_j)\) with \(S_j\) as in
Remark 4.5. Since $T'_{\infty}$ and $T_{\infty}$ are in bijection, hereafter we use the symbol $T_{\infty}$ also for $T'_{\infty}$ (identifying the two index sets).

We have the limit involution $\sigma_{\infty}$ acting on $R_{\infty}$ which is uniquely lifted to an involution $\sigma = \sigma_{\infty}$ acting on $R := R_{\infty}$ for $R_{\infty}$ defined just below (4.2). Put

$$R_{\pm} := \{ x \in R | \sigma(x) = \pm x \}. $$

Let $I_{\infty} = R(\sigma - 1)R = RR_{-}$. Note that $r_{\pm} := |Q_{\pm}|$ is independent of $Q$ by Corollary 4.2.

We now claim that $r_{-} > 0$ if $\sigma$ acts non-trivially on $\mathbb{T}^0 = R^0$. Here is a proof of this claim. First assume that the class number of $R$ is prime to $p$ (so, $C = C_0$ in the introduction is trivial). Note that $\mathbb{T}^2/Q^2 \cong W[[H_Q]]$ for $I^2 := \mathbb{T}^2/(\sigma - 1)^2\mathbb{T}^2$ by Proposition 2.6 and $H_Q = H_{Q_{-}}$ by definition. By our choice of $Q$, if $r_{-} = 0$ (i.e., $r = r_{+}$ and hence $Q = Q_{+}$), by Proposition 1.4, for $I_{\infty} = R(\sigma_{\infty} - 1)R$, we have $R/I_{\infty} = \lim_{\longleftarrow n} W[[H_{Q_{n}}]]/\mathfrak{A}_{n} \cong W[[S_{r_{+}}^{1}, \ldots, S_{r_{+}}^{t}]]$; so, $\dim R = \dim R/I_{\infty}$.

If the class number of $F$ is divisible by $p$, by Proposition 2.6, we have a canonical isomorphism

$$R^Q/Q^m \otimes_{\Lambda} \Lambda/(T) \cong W[C_{Q_{m}}]$$

for $C_{Q_{m}}$ defined above Theorem B in the introduction. By [H16, Section 3.1], the ring $W[C_{Q_{m}}]$ determines functorially the group $C_{Q_{m}}$; so, the projection $R^Q(m + 1)/\mathfrak{A}_{n + 1} \to R^Q(m)/\mathfrak{A}_{n}$ induces a surjective group homomorphism

$$C_{Q_{m}(n + 1)}/\Delta_{Q_{m}(n + 1)}^{p_{m + 1}} \to C_{Q_{m}(n)}/\Delta_{Q_{m}(n)}^{p_{m}}.$$ 

Here $C_{Q_{m}}$ is as in the introduction. This tells us that we have a surjective group homomorphism $Z_{Q_{m}}/\Delta_{Q_{m}(n + 1)}^{p_{m + 1}} \twoheadrightarrow Z_{Q_{m}(n)}/\Delta_{Q_{m}(n)}^{p_{m}}$. Thus the sequence $\{Q_{m}(n)\}_{n}$ satisfies the requirement of the sequence in Proposition 1.5, and by Proposition 1.5, we have $R/I_{\infty} = \lim_{\longleftarrow n} W[[H_{Q_{n}}]]/\mathfrak{A}_{n}$ which is free of finite rank over $\Lambda[\Delta] = \Lambda[\Delta_{\infty}]$: so, $\dim R = \dim R/I_{\infty}$ without assuming that the class number is prime to $p$. Thus, if $Q$ is $0$, then $\text{Spec}(R/I_{\infty})$ contains an irreducible component of the integral scheme $\text{Spec}(R)$. This implies $\text{Spec}(R) = \text{Spec}(R/I_{\infty})$, and hence the involution $\sigma$ acts trivially on $R$, a contradiction (against the non-triviality of $\sigma$ on $\mathbb{T}^0 = R/\mathfrak{A}_{0}R$). Therefore we conclude that $r_{-} = |Q_{-}| > 0$. This implies that $R/I_{\infty}$ is a torsion $S_{\Lambda}$-module of finite type for $S_{\Lambda} = \Lambda[[\Delta]]/(S_{r_{+}}^{2}) = \Lambda \otimes_{W} S$ with $S$ as in Definition 4.3. Since $R_{\infty}/I_{\infty} \cong R_{\infty}/I_{\infty}^{1}$ has finite flat over $W[[\Delta_{\infty}]]$ which is the ramification locus (fixed by $\sigma_{\infty}$), we find that $r' = \dim W \text{Spec}(R_{\infty}/I_{\infty}) = \dim W \text{Spec}(W[[\Delta_{\infty}]]) = r_{+}$, which implies $0 < r_{-} = r''$ as $r_{+} = r_{-}$ and $r_{-} = r_{-} - r_{-}$. The identity $r_{-} = \dim \text{Hom}_{W}[W][Y^{\infty}](\phi^\infty, \omega, F)$ follows from (3.9). Later we see directly that $r' = \dim \text{Sel}_{Q}(\text{Ind}_{W}^{0} F^{\infty}) = \dim \text{Sel}_{W}^{0}(\text{Ind}_{W}^{0} F^{\infty}) = r_{-}$ in Lemma 6.2.

Since $R$ is free of finite rank over $S_{\Lambda}$ by the Auslander-Buchsbaum formula (e.g., [CMA, Theorem 19.9]), regularity of $R$ implies that $R$ is a Gorenstein ring over $S_{\Lambda}$; in particular, $R_{+} := \text{Hom}_{S_{\Lambda}}(R, S_{\Lambda}) \cong R$ as $R$-modules. By Corollary 4.8 (and (4.6)), $\phi_{\infty}$ commutes with $\sigma_{\infty}$, and we conclude that $\phi_{\infty} := \text{Hom}_{S}(R_{\infty}, S) \cong R_{\infty}$ induces $\phi_{\infty} := \text{Hom}_{S}(R_{\infty}, S) \cong R_{\infty}$ as $R_{\infty}$-modules. Since $R_{+}/R_{\infty}$ is Gorenstein by [CMT, Exercise 18.1], and by Lemma 11.1, $R_{+} := \text{Hom}_{S_{\Lambda}}(R_{+}, S_{\Lambda}) \cong R_{+}$ as $R_{+}$-modules.

Suppose $r_{-} = r'' = 1$. Let $S_{\Lambda} = S_{\Lambda} \otimes_{W} \Lambda = \Lambda[[\Delta]]$. Then plainly $S_{\Lambda}$ is flat over $S_{\Lambda} := S_{\Lambda}^{0}$. By Lemma 11.4, $R_{-}$ is generated over $R_{+}$ by a single element $\delta$ with $\sigma(\delta) = -\delta$. If a power series $\Phi(T_{1, +}, \ldots, T_{r_{-} +}, T_{1, -})$ is fixed by $\sigma_{\infty}$, by equating the coefficients of the identity:

$$\Phi(T_{1, +}, \ldots, T_{r_{-} +}, T_{1, -}) = \sigma(\Phi(T_{1, +}, \ldots, T_{r_{-} +}, T_{1, -})) = \Phi(T_{1, +}, \ldots, T_{r_{-} +}, T_{1, -}),$$

we find that $\Phi$ is actually a power series of $(T_{1, +}, \ldots, T_{r_{-} +}, T_{1, -})$. Thus the fixed part $R_{+} := R_{G}$ for $G = \{ \text{id}, \sigma_{\infty} \}$ is still a power series ring, and we have $R_{+} = \Lambda[[T_{1, +}, \ldots, T_{r_{-} +}, T_{1, -}]]$. Since $T_{\infty} = \lim_{\longleftarrow m} T_{m}$ by the original Taylor--Wiles argument (e.g., [HMI, page 194]), lifting it to $\Lambda$, we get $T = T_{\infty} = \Lambda/\mathfrak{A}_{0}R$ and $T_{\infty}$ is the surjective image of $R_{-}$. Since $R_{+}$ is generated by one element $\delta$ over $R_{+}$ (which can be given by $T_{1, -}$), its image $T_{-}$ in $T$ is generated by one element $\theta$ over $T_{+}$. This proves the assertion (2) for $Q = \emptyset$.

For a given $Q = Q_{m_{0}} \neq \emptyset$, we take $n_{0}$ such that $p_{m_{0}} = \max_{e \in Q(|\Delta_{w}|)}$. Then we restart the Taylor-Wiles argument from $T_{Q}$ in place of $T_{\emptyset}$. In other words, we consider the projective system for $n \geq n_{0}$:

$$(4.7) \quad ((R_{n}, \alpha), R_{\infty}, f_{1}, \ldots, f_{r}, \sigma_{n}, \phi_{n}) \in I_{n}$$
for \( \bar{R}_{Q,n} = R_n/(p^n) + \mathfrak{A}_Q R_n \). Then by the same argument, we get

\[
\mathbb{T}_Q \cong \lim_{n \to \infty} \bar{R}_{Q,n} = R_\infty/\mathfrak{A}_Q.
\]

Thus again lifting over \( \Lambda \), we get \( \mathbb{T}_Q = R/\mathfrak{A}_Q R \). Since \( \mathcal{R}_- \) is generated by one element \( \delta \) over \( \mathcal{R}_+ \), \( \mathbb{T}_Q^\delta \) (which is a surjective image of \( \mathcal{R}_- \)) is generated by a single element \( \theta_Q \) over \( \mathbb{T}_Q^\delta \). We may assume that the projection maps send \( T_{1,-} \mapsto \theta_Q \mapsto \theta \) in \( T_- \). This finishes the proof of the assertion (2).

We now prove (3). Since \( r^r = r_- = 1 \), we can write \( Q^+ = Q_m^+ = \{ q_1, \ldots, q_{r_1} \} \) and \( Q^- = Q_m^- = \{ q_r \} \). Recall \( S_\Lambda = \mathcal{S}_{\mathcal{W} W} = \Lambda[[\Delta]] \), and write \( \{ s_j = 1 + S_j \}_{j=1,\ldots, r} \) for the basis of \( \Delta \) corresponding to \( \lim_{m \to \infty} \delta_q \). Since \( r'' = r_- = 1 \), \( \mathcal{R}_+ = \Lambda[[T_{1,+}, \ldots, T_{r-1,+}, T_{1,-}]] \) and \( \mathfrak{A}_Q = \mathfrak{A}_Q \cap S_\Lambda \) is generated by an \( S \)-sequence

\[
\{ s_1^{\Delta_{q_1}} - 1, \ldots, s_{r-1}^{\Delta_{q_{r-1}}} - 1, s_r^{\Delta_{q_r}} - 1, s_r^{-\Delta_{q_r}} + 2 \}
\]

(which is hence an \( \mathcal{R}_- \)-sequence), \( \mathcal{R}_+ / \mathfrak{A}_Q \mathcal{R}_+ \) is a local complete intersection and hence is a Gorenstein ring (e.g., [CRT, Exercise 18.1]). We have a surjection \( \mathcal{R}_+ \to \mathbb{T}_Q^\delta \) and hence a surjection \( \mathcal{R}_+ / \mathfrak{A}_Q \mathcal{R}_+ \to \mathbb{T}_Q^\delta \subset \mathbb{T}_Q \). Then we have

\[
b_Q := \ker(\mathcal{R}_+ / \mathfrak{A}_Q \mathcal{R}_+ \to \mathbb{T}_Q^\delta \subset \mathbb{T}_Q) = \ker(\mathcal{R} \to \mathbb{T}_Q) \cap \mathcal{R}_+ = \mathfrak{A}_Q \mathcal{R} \cap \mathcal{R}_+ = H^0(G, \mathfrak{A}_Q \mathcal{R}) = \mathfrak{A}_Q + (T_{1,-}(s_r^{\Delta_{q_r}} - s_r^{-\Delta_{q_r}})),
\]

since \( \mathfrak{A}_Q \mathcal{R} / \mathfrak{A}_Q \mathcal{R}_+ \) is generated by \( T_{1,-} \mathfrak{A}_Q \mathcal{R} = T_{1,-} \mathfrak{A}_Q \mathcal{R} + (T_{1,-}(s_r^{\Delta_{q_r}} - s_r^{-\Delta_{q_r}})) \). Thus \( b_Q \) is generated by the regular sequence

\[
\{ s_1^{\Delta_{q_1}} - 1, \ldots, s_{r-1}^{\Delta_{q_{r-1}}} - 1, T_{1,-}(s_r^{\Delta_{q_r}} - s_r^{-\Delta_{q_r}}) \}.
\]

Since \( S_j (j \leq r-1) \) is fixed by \( \sigma \), we find that \( \mathbb{T}_Q^\delta = \Lambda[[T_{1,+}, \ldots, T_{r-1,+}, T_{1,-}]] / b_Q \) is a local complete intersection. \( \square \)

5. Proof of Theorem B

In Sections 5–10, unless otherwise mentioned, we assume that \( \mathfrak{p} = \text{Ind}_Q^T \mathfrak{p} \) for the imaginary quadratic field \( F \). Let \( Q \) be either \( Q \in Q \) as in Theorem 4.10 or \( Q = 0 \). Thus \( \mathbb{T}^0 = T \) by our convention. So, when \( Q = 0 \), we omit the superscript or subscript “\( Q \)” from the notation. Recall the fixed integer \( k \geq 1 \) and the local direct summand \( \mathbb{T}_Q = \mathbb{T}_Q^\delta / (t - \gamma^k) \mathbb{T}_Q \) of \( b_{Q,k,\psi} \). Since we use the anticyclotomic Katz \( p \)-adic \( L \)-function \( L_p^\ast \) defined as an element of \( W[[H]] \), the base ring \( W \) is a finite extension of \( W(\mathfrak{p}_p) \) (see [Ka78]), though, replacing \( L_p^\ast \) by a generator of the ideal (\( L_p^\ast \)) defined in \( W_0[[H]] \) for a finite extension \( W_0 \) of \( \mathbb{Z}_p \) (see Theorem 5.2), we do not need to take \( W \) bigger than \( W_0 \). By Corollary 2.5 and Proposition 2.6, we have \( \mathbb{T}_Q^\delta / I_Q \cong W[[H]] \). Write \( K := \text{Frac}(\Lambda) \) for the weight Iwasawa algebra \( \Lambda \). Since \( \mathbb{T}_Q \) is a reduced algebra finite flat over \( \Lambda \) (cf. [H13, Corollary 1.3]), we have \( \text{Frac}(\mathbb{T}_Q) = \mathbb{T}_Q \otimes K = X + \text{Frac}(W[[H]]) \) for a ring direct summand \( X \). Put \( \mathbb{T}_Q, \text{ncm} \) for the image of \( \mathbb{T}_Q \) in \( X \). Then we have \( I_Q = (\mathbb{T}_Q, \text{ncm} \oplus 0) \cap \mathbb{T}_Q \in \text{Frac}(\mathbb{T}_Q) \). In particular, the involution \( \sigma_Q \) preserves the quotient ring \( \mathbb{T}_Q, \text{ncm} \) as an automorphism of \( \text{Frac}(\mathbb{T}_Q) \).

Since \( W[[H]] \) is \( \Lambda \)-free of finite rank, the exact sequence of Proposition 2.6

\[
0 \to I_Q \to \mathbb{T}_Q \to W[[H]] \to 0
\]

is split exact, and hence \( I_Q \) is \( \Lambda \)-free of finite rank. Recall \( M^\vee = \text{Hom}_\Lambda(M, \Lambda) \) for \( \Lambda \)-modules \( M \). Since \( (\mathbb{T})^\vee \cong \mathbb{T}_Q \) by Theorem 2.1 and Theorem 4.10 and \( W[[H]] \vee \cong W[[H]] \) as \( \mathbb{T}_Q \)-modules, from the above exact sequence, we get the dual diagram with exact rows:

\[
\begin{array}{rll}
W[[H]] \hspace{-7mm} & \hookrightarrow & (\mathbb{T}_Q)^\vee \overset{i}{\longrightarrow} (I_Q)^\vee \\
& \downarrow & \downarrow & \downarrow \\
W[[H]] & \longrightarrow & \mathbb{T}_Q \longrightarrow \mathbb{T}_Q, \text{ncm}.
\end{array}
\]

Thus we get
Lemma 5.1. Suppose (h0–4). Let \( a_Q := \mathbb{T}^Q \cap (0 \oplus \text{Frac}(W[[H]]) = \text{Ker}(\mathbb{T}^Q \to \mathbb{T}_{\text{ncm}}^Q). \) Then \( a_Q \) is a principal ideal generated by \( a_Q \in \mathbb{T}_{\text{ncm}}^Q \) in \( \mathbb{T}_{\text{ncm}}^Q \) isomorphic to \( W[[H]] \) as \( \mathbb{T}_{\text{ncm}}^Q \)-modules (since \( W[[H]] \) is fixed by \( \sigma_Q \)).

If \( Q = \emptyset \), we have the anticyclic Katz measure \( L_p^- \in W[[Z_p^-]] \) with branch character given by the anticyclic projection \( \varphi^- \) of the Teichmüller lift \( \varphi \) of \( \mathbb{T} \) (see [H15, 36]). Identifying \( H \) with \( Z^- \) when \( Q = \emptyset \), we regard \( L_p^- \in W[[H]] \). Then from [H15, Theorem 7.2], we get

Theorem 5.2. Suppose (h0–4) and \( p > 3 \). The ideal \( a = a_Q \) is generated by \( L_p^- \in W[[H]] \).

Let \( \mathbb{T}_Q^Q = \{ x \in \mathbb{T}^Q | x^\sigma = \pm x \} \), \( \mathbb{T}_{\text{ncm}}^Q = \{ x \in \mathbb{T}_{\text{ncm}}^Q | x^\sigma = \pm x \} \) and \( \mathbb{T}_Q^+ = \{ x \in \mathbb{T}_Q | x^\sigma = \pm x \} \).

Since no irreducible components of \( \text{Spec}(\mathbb{T}_{\text{ncm}}^Q) \) is fixed by \( \sigma_Q \) and \( I_Q^Q = \mathbb{T}^Q(\sigma_Q - 1) \mathbb{T}^Q \to \mathbb{T}^Q \cdot \mathbb{T}^Q \), we have \( \mathbb{T}_Q^Q = \mathbb{T}_{\text{ncm}}^Q = I_Q^Q \). Also \( I_Q^Q \subset \mathbb{T}_{\text{ncm}}^Q \), as \( I_Q^Q \) is generated by \( \mathbb{T}_Q^Q \subset \mathbb{T}_{\text{ncm}}^Q \). Taking \( \sigma_Q \)-invariant, from \( \mathbb{T}^Q/I_Q^Q = W[[H]] \), we conclude \( \mathbb{T}_Q^+/I_Q^+ = W[[H]] \).

We now prove the following key lemma.

Lemma 5.3. Assume (h0–4) and that \( F \) is imaginary. Let \( Q = Q_m \in Q \) or \( Q = \emptyset \) as in Theorem 4.10. If \( \sigma \) acts non-trivially on \( \mathbb{T} = \mathbb{T}_+ \), then the condition (Q10) is satisfied with \( \varepsilon = + \) and the ring \( \mathbb{T}_+^Q \) and \( \mathbb{T}_Q^+ \) are both Gorenstein. Indeed, we have \( \text{Isom}_{\mathbb{T}_+^Q}(\mathbb{T}_+^Q)^\vee, \mathbb{T}_Q^+)^+ \neq \emptyset \) and

\[
\text{Isom}_{\mathbb{T}_+^Q}(\mathbb{T}_+^Q)^\vee, \mathbb{T}_Q^+)^- = \text{Isom}_{\mathbb{T}_+^Q}(\mathbb{T}_+^Q, \mathbb{T}_Q^+)^- = \emptyset,
\]

where \( M^+ = \text{Hom}_{W}(M, W) \) and \( M^\vee = \text{Hom}_{A}(M, A) \).

In the lemma, we can replace \( \mathbb{T}_+^Q \) (resp. \( \mathbb{T}_+^Q \)) by \( \text{Hom}_{\mathbb{Q}}(\mathbb{T}_Q, \mathbb{Q}) \) (resp. \( \text{Hom}_{\mathbb{Q}}(\mathbb{T}_Q, \mathbb{Q}) \)) for the image \( S_Q \) (resp. \( S_{\Lambda, Q} \)) of \( S \) (resp. \( S_{\Lambda} \)) in \( \mathbb{T}_Q \) (resp. in \( \mathbb{T}_+^Q \)) (e.g., Remark 4.5).

Proof. Since the proof is the same for any \( Q \) including \( Q = \emptyset \) and also for \( \mathbb{T}_Q \) and \( \mathbb{T}_Q^Q \), we prove the lemma for \( \mathbb{T}_+^Q = \mathbb{T}_+^Q \).

Recall \( C := \text{Gal}(F_{c\mathfrak{p}}/F) \) for the maximal \( p \)-abelian extension \( F_{c\mathfrak{p}}/F \) of conductor dividing \( c\mathfrak{p} \). Since \( \mathbb{T}/I = W[[H]] \) by Corollary 2.5 and \( W[[H]] \) is a \( \Lambda \)-free rank \( |C| \), \( I \) is a \( \Lambda \)-direct summand of \( \mathbb{T} \), and hence \( I \) is \( \Lambda \)-free. Taking the \( \Lambda \)-dual sequence of \( 0 \to I \to T \to W[[H]] \to 0 \) (with all \( \Lambda \)-free terms), we have another exact sequence: \( 0 \to I^\vee \to T^\vee \to W[[H]]^\vee \to 0 \) of \( \mathbb{T} \)-modules.

By Theorem 2.1, \( T \) is a local complete intersection. Since \( W[[H]] \) is a group algebra, it is a local complete intersection, and hence they are Gorenstein. Then we have \( T^\vee \cong T \) and \( W[[H]]^\vee \cong W[[H]] \) as \( \mathbb{T} \)-modules. From this, we conclude \( \mathbb{T}_{\text{ncm}}^Q \cong I^\vee \). Thus \( \mathbb{T}_{\text{ncm}}^Q \) is \( \Lambda \)-free and is non-trivial as \( \sigma \) acts on \( T \) non-trivially. Since \( \mathbb{T}_{\text{ncm}}^Q \) is reduced (by cube-freeness of \( N \); see [H13, Corollary 1.3]) and there is no irreducible component of \( \text{Spec}(\mathbb{T}_{\text{ncm}}^Q) \) on which \( \sigma \)-acts trivially, \( \text{Frac}(\mathbb{T}_{\text{ncm}}^Q) \) is equal to \( \text{Frac}(\mathbb{T}_{\text{ncm}}^Q) \otimes \mathbb{K} \) for a non-zero divisor \( \delta \) of \( \mathbb{T}_{\text{ncm}}^Q \). In other words, \( \text{Frac}(\mathbb{T}_{\text{ncm}}^Q) \) is a \( \text{Frac}(\mathbb{T}_{\text{ncm}}^Q) \)-free module of rank 2, and \( \text{Frac}(\mathbb{T}_{\text{ncm}}^Q) \otimes \mathbb{K} = \mathbb{T}_- \otimes \mathbb{K} \) is a \( \text{Frac}(\mathbb{T}_{\text{ncm}}^Q) \)-free module of rank 1. In particular, we have

\[
\text{rank}_A \mathbb{T}_{\text{ncm}}^Q = \text{rank}_A \mathbb{T}_{\text{ncm}}^Q = \text{rank}_A \mathbb{T}_- > 0.
\]

The positivity of \( \text{rank}_A \mathbb{T}_- \) follows from non-triviality of \( \sigma \) on \( T \), and \( \mathbb{T}_{\text{ncm}}^Q \) is identical to \( \mathbb{T}_- \) as \( \sigma \) acts trivially on \( W[[H]] \). Since \( I = \text{Ker}(T \to W[[H]]) \), we have \( I = T \cap (0 \oplus \text{Frac}(\mathbb{T}_{\text{ncm}}^Q)) \) inside \( \text{Frac}(T) \), and hence \( \mathbb{T}_{\text{ncm}}^Q/I \) is the congruence module between the two components \( \text{Spec}(\mathbb{T}_{\text{ncm}}^Q) \) and \( \text{Spec}(W[[H]]) \) of \( \text{Spec}(T) \). Thus, by Theorem 5.2, we have (cf. [MFG, §5.3.3])

\[
\mathbb{T}_{\text{ncm}}^Q/I \cong \mathbb{T}_{\text{ncm}}^Q \otimes_T W[[H]] \cong W[[H]]/(L_p^-),
\]

which is a torsion \( \Lambda \)-module. Thus we get

\[
\text{rank}_A I_+ = \dim_K I_+ \otimes \mathbb{K} = \dim_K \text{Frac}(\mathbb{T}_{\text{ncm}}^Q) = \text{rank}_A \mathbb{T}_{\text{ncm}}^Q = \text{rank}_A \mathbb{T}_- > 0.
\]

Taking the \( \sigma \)-invariant of the two sides of the identity \( T/I = W[[H]] \), we have \( T_+/I_+ \cong W[[H]] \).

Thus we get

\[
\text{rank}_A T_+ = \text{rank}_A I_+ + \text{rank}_A W[[H]] = \text{rank}_A \mathbb{T}_- + \text{rank}_A W[[H]] > \text{rank}_A \mathbb{T}_- > 0.
\]

By Lemma 11.2 (2) applied to \( A = \mathbb{T} \) and \( S = \Lambda, \phi \in \text{Isom}_T(T^\vee, T) \) must commutes with the involution; so, we get \( \text{Isom}_T(T^\vee, T)^+ \neq \emptyset \) and \( T_+ \cong T_+^Q \). Thus \( T_+ \) is a Gorenstein ring (by Lemma 11.1) as well as \( \text{Isom}_T(T^\vee, T)^- = \emptyset. \)

\( \square \)
Under these equivalent conditions, the ring \( \mathbb{T}_{\text{ncm}} \) and \( \mathbb{T}_{\text{ncm}}^+ \) are both local complete intersections.

Assume the case when \( p \nmid h_F \).

**Proof.** For simplicity, we write \( A := \mathbb{T}_{\text{ncm}} \) and \( A_+ := \mathbb{T}_{\text{ncm}}^+ \) and \( S = W \). Suppose (1). Then \( A, A_+ \) are local complete intersections; so, Gorenstein. Thus the different inverse \( \Omega^{-1}_{A/A_+} \) and \( \Omega^{-1}_{A_+/W} \) are \( A \)-free modules of rank 1 and \( \Omega^{-1}_{A_+/W} \) is an \( A_+ \)-module of rank 1. (See Section 11 for the definition of the different inverse). Since

\[
\text{Spec}(A)_{\sigma=1} = \text{Spec}(A/I) \cong \text{Spec}(W[[H]]/(L_p)) = \text{Spec}(A_+/I_+),
\]

the ramified locus of Spec(\( \mathbb{T}_{\text{ncm}} \)) is a non-trivial divisor given by the zero set of \( L_p \) which is a non-zero divisor of \( W[[H]] \). Thus \( \Omega^{-1}_{A/A_+} \) is the characteristic ideal \( (L_p) \) (e.g., [MFG, Lemma 5.21]), which is contained in \( m_A \). By Lemma 11.4, we get the assertion (2).

Suppose (2). By the proof of the anticyclotomic main conjecture in [H06] (see also [H15, Section 7]), we have an identity \( \mathbb{T}_{\text{ncm}} \cap I \cong W[[H]]/(L_p) \) and by the technique of [MT90] (see also [H16, \S 6.3.6]), we have an isomorphism \( \mathcal{Y}^{-\varphi} \otimes_{Z_p[\varphi^{-1}]} W \cong \Omega_{\mathbb{T}/A} \otimes_{\mathbb{T}} W[[H]] \) as \( \Lambda \)-modules, where \( \varphi \) is the unique character satisfying the assumption of the anticyclotomic cyclicity conjecture such that \( \chi_{\varphi}|_{\Lambda^\times} \) is the Teichmüller lift of \( \det(\bar{\varphi}) \) (i.e., the Neben character of \( h \)). Thus we conclude \( L_p = L_p(\varphi^{-1}) \) for the Katz measure \( L_p \) in Theorem 5.2. Then by [H86c, Lemma 1.1], we have a canonical isomorphism of \( W[[H]] \)-modules:

\[
\Omega_{\mathbb{T}/A} \otimes_{\mathbb{T}} W[[H]] \cong I/I^2 = (\theta)/\theta^2
\]

whose left-hand-side is cyclic to \( \mathcal{Y}^{-\varphi} \otimes_{Z_p[\varphi^{-1}]} W \). Here \( \theta \) is the generator of \( I \) as in Theorem 5.4 (2). Since \( \theta \) is a non-zero divisor, multiplication by \( \theta \) induces an isomorphism of \( W[[H]] \)-modules

\[
\Lambda/(L_p(\varphi^{-1})) \cong \mathbb{T}_{\text{ncm}}/(\theta) \xrightarrow{\sigma=1} (\theta)/\theta^2 \cong \mathcal{Y}^{-\varphi} \otimes_{Z_p[\varphi^{-1}]} W.
\]

This shows the cyclicity of \( \mathcal{Y}^{-\varphi} \) over \( W[[H]] \), which proves (3).

Assume (3). Then by the above identity, \( I/I^2 \cong \mathcal{Y}^{-\varphi} \) is cyclic over \( W[[H]] \); so, \( I \) is generated by one element by Nakayama’s lemma. Let \( t_Q \) be the tangent space of \( \mathbb{T}_Q \) over \( W[\Delta_Q] \). Then \( t_Q \cong \text{Sel}_p(Ad) \) and its minus-eigenspace for \( \sigma_Q \) is isomorphic to \( \text{Hom}_W[[H]](\mathcal{Y}^{-\varphi}, F) \) by (3.6). Thus \( I_Q/I_0^Q \) is generated by one element over \( W[\Delta_Q] \). Consider the Taylor Wiles system \( (R_n, \ldots) \) as in (3.1). Writing \( I_n = R_n(\sigma_n - 1)R_n \) for the involution \( \sigma_n \) of \( R_n \). Since \( I_n/I_0^2 \) is the image of \( I_Q/I_0^Q \) by \( \sigma_n \) it is generated by one element over \( R_n \). Since \( I_0^2/I_0^1 = \lim_{n} I_n/I_0^2, I_0^2/I_0^1 \otimes_{R_\infty} F \) factor through \( I_n/I_0^2 \otimes_{R_n} F \) for some \( n \); so, \( I_0^2/I_0^1 \) is generated by one element over \( R_\infty \). Since \( R_\infty = W[[T_1^+, \ldots, T_n^+, \overline{T}_1, \ldots, \overline{T}_n]] \), \( I_0^2/I_0^1 \) is generated by \( r^n \) elements over \( R_\infty \), we conclude \( r^n = 1 \). Since \( r^n = r^t \) by Proposition 3.8, we conclude \( r^n = 1 \) and \( \mathcal{Y}^{-\varphi} \) is cyclic over \( W[[H]] \), proving (4).

Assume (4). By Lemma 5.3 combined with Lemma 4.6, the assumption of Theorem 4.10 is satisfied. Then \( r^t = 1 = r^t \) by Theorem 4.10 (1). Then \( T_- \) is generated by a non-zero divisor \( \theta \) by Theorem 4.10 (2), and \( L_+ \) is generated by \( \theta^2 \). This implies \( \mathbb{T}_{\text{ncm}}/(\theta) \cong W[[H]]/(L_p^2) \cong \mathbb{T}_{\text{ncm}}/(\theta^2). \)
Since $W[[H]]/(\theta)$ is a local complete intersection over $W$, by Lemma 5.5, the assertion (1) holds. Moreover, by Theorem 4.10 (3), $T_+$ is a local complete intersection. □

Here is the ring theoretic lemma we used:

**Lemma 5.5.** Let $A$ be a complete local noetherian ring finite flat over $\Lambda$. Then $A$ is a local complete intersection if and only if for a non-zero divisor $\delta \in m_A$, $A/(\delta)$ is a local complete intersection.

**Proof.** We first prove the “if”-part. Take a presentation $\Lambda[[x_1, \ldots, x_m]] \rightarrow A$ for the $m$-variable power series ring $\Lambda[[x_1, \ldots, x_m]]$ over $\Lambda$. Write the kernel of this map as $a$. Lifting $\delta$ to $\tilde{\delta} \in \Lambda[[x_1, \ldots, x_m]]$ so that $\tilde{\delta}$ has image $\delta$ in $A$, we have $\Lambda[[x_1, \ldots, x_m]]/(a + \tilde{\delta}) = A/(\delta)$. Write $\mu(b)$ for the minimal number of generators of an ideal $b$ of a ring. Since $A/(\delta)$ is a local complete intersection of dimension 1, $a + \tilde{\delta}$ is generated by a regular sequence of length $m + 1$ as $\mu(a + \tilde{\delta})$ is equal to $m + 1 = \dim \Lambda[[x_1, \ldots, x_m]] - \dim A/(\delta)$ for the complete intersection ring $A/(\delta)$ (cf. Theorems 17.1 and 21.2 of [CRT]). Since the height of $a + \tilde{\delta}$ is $m + 1$ and the height of $a$ is $m$ (by $\dim A = 1 + \dim A/(\delta)$ as $\delta$ is a non-zero divisor; see [CRT, Theorem 17.4]), we conclude $\mu(a + \tilde{\delta}) = \mu(a) + 1 = m + 1$ from $\mu(a) \leq \mu(a + \tilde{\delta})$. Then by [CRT, Theorem 17.4 (iii)], we conclude that a minimal set of generators $a_1, \ldots, a_m$ of $a$ is a regular sequence. Thus $A \cong \Lambda[[x_1, \ldots, x_m]]/(a_1, \ldots, a_m)$ is a local complete intersection by [CRT, Theorem 21.2 (ii)].

We now prove the “only if”-part. Let $(a_1, \ldots, a_m)$ be a sequence generating $a$. Pick a non-zero divisor $\delta \in m_A$ and lift it to $\tilde{\delta} \in \Lambda[[x_1, \ldots, x_m]]$. Then plainly $(a_1, \ldots, a_m, \tilde{\delta})$ is a regular $\Lambda[[x_1, \ldots, x_m]]$-sequence; so, $A/(\delta)$ is a local complete intersection. □

**Conjecture 5.6** (Semi-simplicity). Suppose $p > 3$. If $\mathfrak{c}$ is a square-free product of primes split in $F/\mathbb{Q}$, then the projection of $L_\mathfrak{c}^-$ to each irreducible component of $\text{Spec}(W[[H]])$ is square-free.

Note that each irreducible component of $\text{Spec}(W[[H]])$ is the spectrum of a regular local ring $\mathfrak{A} := W[[\mathfrak{T}_-]]$, which is a unique factorization domain; so, square-freeness of elements of $\mathfrak{A}$ is well defined. If $\mathfrak{c}$ is divisible by non-split primes, there are some cases where $L_\mathfrak{c}^-$ is divisible by $p^\alpha$ (e.g., [H10, §5.3]). It is a well known conjecture that the Kubota-Leopoldt $p$-adic $L$ function is square-free in the Iwasawa algebra (the semi-simplicity conjecture of Iwasawa; see [CPI, (P3–4)_x in No.62 and see also U3]). Thus the above conjecture is an anti-cycloptotnic version of Iwasawa’s semi-simplicity conjecture.

### 6. A GOOD CHOICE OF GENERATORS OF $R_Q$ OVER $W$

To prove Theorem A, we need to further refine the Taylor–Wiles system choosing a good system of generators over $F$ of the minus part of the cotangent space of $R_Q$ (resp. $R^2$) ($Q \in \mathfrak{Q}$ at $\mathfrak{m}_W$ (resp. at $\mathfrak{m}_A$). For the system $\mathfrak{Q} = \{Q_m | m = 1, 2, \ldots \}$ of set of primes as in Sections 3 and 4, we will show, choosing $\mathfrak{Q}$ further well, that the image of $T(q)$ for $q \in Q^-$ gives rise to a canonical set of generators at the end. As shown in Lemma 3.2, we hereafter choose $\mathfrak{Q}$ so that $q \equiv 1 \mod Cp^m$ for every $q \in Q_m \in \mathfrak{Q}$ ($m = 1, 2, \ldots$). The main result in this section is Theorem 6.4. Throughout this section, we assume $(h_0-4)$ and $Q \in \mathfrak{Q}$.

Let $F^Q$ denote the maximal extension of $K_0$ (the splitting field of $\mathfrak{p} = \text{Ind}^Q_F \mathfrak{p}$) unramified outside $Q$ and $p$. Any deformation satisfying (D1–4) of $\mathfrak{p}$ factors through $\text{Gal}(F^Q/\mathbb{Q})$ by (h0).

**Lemma 6.1.** Let $F$ be real or imaginary. The image of the cohomology group $H^1(F^Q/\mathbb{Q}, \text{Ind}^Q_F \mathfrak{p}^-)$ (resp. $H^1(F^Q/\mathbb{Q}, \text{Ind}^Q_F \mathfrak{p}^- \mathfrak{p}^-)$) to the local cohomology group of $\text{Gal}(\mathbb{Q}_q/F_q)$ falls in the one dimensional subspace $\text{Hom}(\text{Frob}_q^\mathfrak{p}, F)$ for $q \in Q^-$ after applying the restriction map and then Shapiro’s lemma. For $q \in Q^+$, we have $H^1(\mathbb{Q}_q, \text{Ind}^Q_F \mathfrak{p}^-) = H^1(\mathbb{Q}_q, \text{Ind}^Q_F \mathfrak{p}^- \mathfrak{p}^-) = 0$.

Since the proof for $\text{Ind}^Q_F \mathfrak{p}^- \mathfrak{p}^-$ and $\text{Ind}^Q_F \mathfrak{p}^- \mathfrak{p}^-$ is the same, we give a proof for $\text{Ind}^Q_F \mathfrak{p}^- \mathfrak{p}^-$. \hspace{1cm} \text{Proof.} Note that $\mathfrak{p}^-|_{\text{Gal}(\mathbb{Q}_q/F_q)} = 1$ as $q \equiv 1 \mod p$. Thus we ignore $\mathfrak{p}^-$ when we compute local cohomology groups at $q$. We compute $H^1(\mathbb{Q}_q, \text{Ind}^Q_F \mathfrak{p}^- \mathfrak{p}^-)$. First suppose that $q$ is inert in $F/\mathbb{Q}$ (i.e., $q \in Q^-$). Then by Shapiro’s lemma, we have

$$H^1(\mathbb{Q}_q, \text{Ind}^Q_F \mathfrak{p}^- \mathfrak{p}^-) = H^1(F_q, F) = \text{Hom}(\mu_{q-1} \times q^2, F) = \text{Hom}(\mu_{q-1}, F) \times \text{Hom}(\text{Frob}_q^\mathfrak{p}, F) \cong F^2,$$
since \( \varphi^- \) is trivial on \( \text{Gal}(\mathbb{Q}_q/F_q) \) as \( \varphi^-(\text{Frob}_q) = 1 \) and \( \omega(\text{Frob}_q) = q \equiv 1 \mod p \). By the inflation restriction sequence applies to \( \text{Gal}(\mathbb{Q}_q/Q_q)/I_q = \text{Frob}_q^{2} \), we have an exact sequence

\[
0 \to H^1(\text{Frob}_q, \text{Ind}_F^Q \varphi^-) \to H^1(Q_q, \text{Ind}_F^Q \varphi^-) \to \text{Hom}_{\text{Frob}_q}(I_q, \varphi^- \oplus \varphi^-^{-1}) \to 0,
\]

since \( H^2(\text{Frob}_q, M) = 0 \) for all discrete finite modules \( M \). Since \( \text{Frob}_q \) acts by multiplication by \( q \equiv 1 \mod p \) on the tame inertia group \( I_q \) and \( \text{Frob}_q \) interchange \( \varphi^- \) and its inverse, we have \( \text{Hom}_{\text{Frob}_q}(I_q, \varphi^- \oplus \varphi^-^{-1}) \cong \mathbb{F} \). By Shapiro’s lemma, we have

\[
H^1(\text{Frob}_q, \text{Ind}_F^Q \varphi^-) = H^1(\text{Frob}_q^{2}, \varphi^-) = H^1(\text{Frob}_q^{2}, \mathbb{F}) \cong \mathbb{F}
\]
as \( \varphi^- \) is trivial on \( \text{Frob}_q \). We have the following commutative diagram:

\[
\begin{array}{ccc}
H^1(F^Q/Q, \text{Ind}_F^Q \varphi^-) & \xrightarrow{\text{Res}} & H^1(Q_q, \text{Ind}_F^Q \varphi^-) \\
\downarrow & & \downarrow \\
H^1(F^Q/F, \varphi^-) & \xrightarrow{\text{Res}} & \text{Hom} (\text{Gal}(\mathbb{Q}_q/F_q), \mathbb{F}) \cong \mathbb{F}^2.
\end{array}
\]
The image of the bottom Res has trivial intersection with \( \text{Hom}_{\text{Frob}_q}(I_q, \varphi^- \oplus \varphi^-^{-1}) \) which is diagonally embedded into \( \text{Hom}(I_q, \varphi^- \oplus \varphi^-^{-1}) \) (while the image of the top Res lands in single \( \text{Hom}_{\text{Frob}_q}(I_q, \varphi^-) \). Thus \( \text{Im}(H^1(F^Q/Q, \text{Ind}_F^Q \varphi^-) \xrightarrow{\text{Res}} H^1(Q_q, \text{Ind}_F^Q \varphi^-)) \) is unramified and is canonically isomorphic to a subgroup of \( \text{Hom}(\text{Frob}_q^{2}, \mathbb{F}) \cong \mathbb{F} \).

Now assume that \( q \) splits in \( F/Q \). Then we see \( \text{Ind}_F^Q \varphi^- |_{\text{Gal}(\mathbb{Q}_q/Q_q)} = \varphi^- \oplus \varphi^-^{-1} \). We first compute \( H^1(Q_q, \varphi^-) \). By the inflation restriction sequence applies to \( \text{Gal}(\mathbb{Q}_q/Q_q)/I_q = \text{Frob}_q^{2} \), we have an exact sequence

\[
0 \to H^1(\text{Frob}_q, \varphi^-) \to H^1(Q_q, \varphi^-) \to \text{Hom}_{\text{Frob}_q}(I_q, \text{Frob}_q(F^-)).
\]

Since \( \varphi^-(\text{Frob}_q) \neq 1 \) by our choice of \( q \in \mathbb{Q}^+ \), we have \( H^1(\text{Frob}_q, \varphi^-) \cong \mathbb{F}/(\varphi^-(\text{Frob}_q) - 1)\mathbb{F} = 0 \). Since \( \text{Hom}_{\text{Frob}_q}(I_q, \text{Frob}_q(F^-)) \cong \text{Hom}_{\text{Frob}_q}(I_q, \text{Frob}_q(F^-)) \) for the maximal tame quotient \( I_q \) of \( I_q \) and on \( I_q \), \( \text{Frob}_q \) acts by multiplication by \( q \equiv 1 \mod p \). Since \( \varphi^-(\text{Frob}_q) \neq 1 \equiv (q \mod p) \), we find \( \text{Hom}_{\text{Frob}_q}(I_q, \text{Frob}_q(F^-)) = 0 \). Thus \( H^1(Q_q, \varphi^-) = 0 \); so, \( H^1(Q_q, \text{Ind}_F^Q \varphi^-) = H^1(Q_q, \text{Ind}_F^Q \varphi^-) = 0 \) as \( \varphi = 1 \) on \( \text{Gal}(\mathbb{Q}_q/Q_q) \).

### Lemma 6.2.

For the minus part \( t^-_Q \) of the tangent space \( t_Q \) of \( T_Q \), we have

\[
t^-_Q \cong \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) \cong \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) \cong \text{Sel}_Q(\text{Ind}_F^Q \varphi^-)
\]
as vector spaces over \( \mathbb{F} \) for all \( Q \in \mathbb{Q} \) contributing to the Taylor–Wiles system in (3.1) including \( Q = 0 \).

The isomorphism at \( \ast \) is not canonical, and we just choose one.

**Proof.** By Proposition 3.8 and the construction of the system, we have \( r_- = \dim_{\mathbb{F}} \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) \) which is independent of \( Q \). For \( n > 1 \), we have defined \( R_n = T_{Q_n} \otimes S_n \) with \( S_n = S/\mathfrak{A}_n \) for the ideal \( \mathfrak{A}_n := ((s_1)^n - 1, (s_2)^n - 1, p^n)_{1,...,r_{+},j=1,...,r_{-}} \) for some \( m \geq n \). Therefore \( t^-_{Q_n} = \dim_{\mathbb{F}} \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) \). On the other hand, by Proposition 3.8, we have \( \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) \cong t^-_{Q_n} \cong \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) \). Thus \( \dim_{\mathbb{F}} \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) = \dim_{\mathbb{F}} \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) \), and we can choose an \( \mathbb{F} \)-linear isomorphism \( \ast \). This finishes the proof. \( \square \)

We pick an \( \mathbb{F} \)-linear isomorphism \( \iota : \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) \cong \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) \). Choose a basis \( \{ x \} \) of \( \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) \) over \( \mathbb{F} \) and write \( y = y(x) = i(x) \) which gives rise to a basis of \( \text{Sel}_Q(\text{Ind}_F^Q \varphi^-) \). Then we define Galois homomorphisms \( f_x \in \text{Hom}_{\text{Gal}(K_3/\mu_p)}(\text{Gal}(\mathbb{Q}(N^p)/K_3), \text{Ind}_F^Q(\varphi^-)) \) and \( f_y \in \text{Hom}_{\text{Gal}(K_3/\mu_p)}(\text{Gal}(\mathbb{Q}(N^p)/K_3), \text{Ind}_F^Q(\varphi^-)) \) by restricting the classes \( x \) and \( y \) (as in Lemma 3.2).
Since \( p \mid [K_1(\mu_p) : \mathbb{Q}] \), the two homomorphisms \( f_x \) and \( f_y \) are non-zero. Choose \( \sigma \in \text{Gal}(\mathbb{Q}(N^p) / \mathbb{Q}) \) as in Corollary 3.3 for \( f_x \) and \( f_y(x) \). Thus we have from Lemma 6.1

\[
\text{Sel}_0^Q(\text{Ind}_F^G \varphi/\varphi) \cong \prod_{q \in Q^-} \text{Hom}(\text{Frob}_q^2, \mathbb{F}) \cong \text{Sel}_Q(\text{Ind}_F^G \varphi) \cong \text{Sel}_Q(\text{Ind}_F^G \varphi^-) \cong \text{Sel}_Q(\text{Ind}_F^G (-\varphi)).
\]

We then choose primes \( q \in Q^- = Q_m^m \) so that \( \text{Frob}_q = \text{Frob}_{q_m} = \sigma|_{M_l,M_{q_m}} \). By Chebotarev density theorem, we thus have infinite sets \( \{Q_m^m|m = 1, 2, \ldots \} \). We choose as in Wiles’ work \( Q_m^m \) as explained in Lemma 3.2 for split primes and put \( Q_m^m \cup Q_{m+}^m \), which makes \( Q \).

**Corollary 6.3.** We make the choice of \( Q \) as above. The image \( a(q) \) of Hecke operator \( T(q) \) in \( T_0 \) for \( q \in Q^- \) gives rise to a basis of the minus eigenspace \( t_{q^-}^* \) of the cotangent space \( t_q^* \) under the involution \( \sigma \) induced by \( \rho \mapsto \rho \otimes \chi \) for the deformation \( \rho \). More generally, writing \( b(q) \) for the image of \( U(q) - q^kU(q)^{-1} \) in \( T_Q \) which projects down to \( a(q) \) in \( T_0 \), the set \( \{b(q)\}_{q \in Q^-} \) gives rise to a basis of the minus eigenspace \( t_{q^-}^* \).

Since \( \det(X - \rho_{Q}(q, \mathcal{Q}_q)) = (X - U(q))(X - q^k\chi U(q)^{-1}) \in T_Q[X] \) and \( \det(X - \rho_Q(\text{Frob}_q)) = X - T(q)X - q^k\chi U(q)^{-1} \in T_Q[X] \), the image of \( b(q) \) in \( T_0 \) is \( a(q) \).

**Proof.** Write simply \( R = T_0 \) and \( \sigma \) for the involution. Similarly we write \( R_Q \) for \( T_Q \). Since \( \sigma(T(q)) = \chi(q)T(q) = -T(q) \), we have \( a(q) \in I = R(\sigma - 1)R \). Since \( t_{q^-}^* = I/I \cdot m_R \), we have the natural image \( \overline{\Phi}(q) \in t_{q^-}^* \). As Mazur noticed, the tangent space is identified with \( \text{Sel}_Q(\text{Ad}(\merge)) \) (e.g., [H16, §6.3.6]). The minus part is then identified with \( \text{Sel}_Q(\text{Ind}_F^G(\varphi)) \subset \text{Sel}_Q(\text{Ad}(\merge)) \) in the following way. Consider \( \rho_Q := \rho_Q \mod m_R^2 + m_W^2 \) for the universal representation \( \rho_Q : \text{Gal}(\mathbb{F}^Q / \mathbb{Q}) \to \text{GL}_2(R_Q) \). Then \( \rho_Q \in D_Q(\mathbb{F}^Q / \mathbb{Q}) \) as \( R/(m_R^2 + m_W^2) \cong F[t_Q^2] \) as rings. Writing \( \rho_Q = \overline{\varphi} \otimes \ell \) for \( \ell : \text{Gal}(\mathbb{F}^Q / \mathbb{Q}) \to t_Q^* \otimes \mathbb{F} M_2(\mathbb{F}) = M_2(t_\overline{\varphi}) \), the map \( c_\varphi : g \mapsto \left( \Phi \circ \ell(g) \overline{\Phi}(g)^{-1} \right) \) for each \( \Phi \in t_{\overline{\varphi}}^* \) gives rise to a cocycle representing an element of \( \text{Sel}_Q(\text{Ad}(\merge)) \). Here for the matrix \( \ell(g) = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in M_2(t_Q) \), we have written \( \Phi \circ \ell(g) \) for \( \Phi_1 \circ \ell(g) \). Then \( \overline{\Phi} \) acts on \( M_2(\mathbb{F}) \) from the right. Note that \( \text{Ad}(\merge) = \text{Ind}_F^G(\varphi) \otimes \chi \), and the subspace \( V := \text{Ind}_F^G(\varphi) \subset \text{Ad}(\merge) \) is made of anti-diagonal matrices. The anti-diagonal trace map \( T : \text{Ad}(\merge) \to \mathbb{F} \) induces a linear form on \( V \) and gives rise to an isomorphism of \( X[1] \) in Remark 3.5 (in which the value \( c_\varphi(\varphi) \) lands onto \( F \). The isomorphism \( \text{Sel}_Q(\text{Ind}_F^G(\varphi)) \cong \text{Hom}(\prod_{q \in Q^-} \text{Frob}_q^2, \mathbb{F}) \) by our choice of \( Q^- \) is given by evaluating each Selmer 1-cocycle at \( \varphi_q := [q, \mathcal{Q}_q] \) (the local Artin symbol) and then projecting the value in \( V \) to \( \mathbb{F} \) via \( T \). Thus we have

\[
T((\Phi \circ \ell(\varphi_q)) \overline{\Phi}(\varphi_q)^{-1}) = T(\Phi \left( \rho_Q(\varphi_q) - \left( \begin{smallmatrix} 0 & \overline{\varphi}(\varphi_q^2) \\ \varphi(\varphi_q^2) & 0 \end{smallmatrix} \right) \right) \left( \begin{smallmatrix} 0 & \overline{\varphi}(\varphi_q^2) \\ \varphi(\varphi_q^2) & 0 \end{smallmatrix} \right)^{-1}) = \Phi(T(\rho_Q(\varphi_q))) \overline{\Phi}(\varphi_q^2)^{-1}) = \Phi(\overline{\varphi}(\varphi_q^2)^{-1}) \in \mathbb{F}.
\]

Since \( \Phi \) is arbitrary, this shows the evaluation at \( \varphi_q \) corresponds to \( \overline{\varphi}(\varphi_q^2)^{-1} \in t_{\overline{\varphi}}^* \). Thus \( \{\overline{\varphi}(q)\}_{q \in Q^-} \) (resp. \( \{\overline{\varphi}(q)\}_{q \in Q^-} ) \) generates \( I_Q / I_Q \cdot m_R, I_Q / I_Q \cdot m_R \) over \( \mathbb{F} \). \( \square \)

Combining all these records, we see the following have been proven:

**Theorem 6.4.** Assume \( (I0,4) \). We can choose a set of generators \( \{f_q\}_{q \in Q} \subset m_{T_2^*} \) of \( T_2^* \) indexed by \( q \in Q \) for \( Q \in Q \) over \( W \) such that (i) for \( q \in Q^- \), \( f_q \) is the image of \( U(q) - q^kU(q)^{-1} \) in \( T_Q \) and (ii) \( \{f_q\}_{q \in Q} \) gives rise to a basis of the minus part of the co-tangent space \( t_Q^* = m_{T_2^*} / (m_{T_2^*} + m_W) \).

For \( q \in Q^+ \), to form our Taylor-Wiles system, we just choose generators \( \{f_q\}_{q \in Q^+} \) in \( m_{T_2^*}^* \) whose image generate over \( \mathbb{F} \) the plus part of the co-tangent space \( t_Q^* \).

**Remark 6.5.** Out of the above choices of generators, we create the Taylor-Wiles system for each \( Q \in Q \). Since \( Q \) is infinite, we still make the system work and produces \( R_{\infty} \) (and \( R \) as before.

We note the following fact, although we have proven finer results in the above theorem.

**Lemma 6.6.** Suppose that the order of \( \varphi^- \) is either odd \( > 2 \) or larger than \( 4 \). For any \( m \geq 0 \), the ideal \( T_Q^m \) (resp. \( I_Q \)) is generated by the image \( a(l) \) of \( T(l) \) in \( T_Q^m \) (resp. \( T_Q^m \)) for primes \( l \equiv 1 \mod Cp^m \) inert in \( F/Q \) outside \( Q \) and \( N_Q(\mathbb{C}) \), where \( C = N_{F/Q}(c) \).
Proof. Let $\Sigma$ be the set of totally split primes of $\mathbb{Q}(\mu_{Cp^m})$ outside $Np$ and $Q$, and define $S \subset \Sigma$ to be the set of all primes in $\Sigma$ split in $F(\mu_{Cp^m})/\mathbb{Q}(\mu_{Cp^m})$. The set of primes of $\mathbb{Q}(\mu_{Cp^m})$ above $\Sigma$ has Dirichlet density $1$ in the set of primes of $\mathbb{Q}(\mu_{Cp^m})$. For a deformation $\rho_A : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{Cp^m})) \to \text{GL}_2(A)$ in $D^0(A)$ for a local $p$-profinite $W$-algebra $A$, if $\text{Tr}(\rho_A(Frob_l)) = 0$ for a set $S_l$ of primes $l \in \Sigma$ inert in $F(\mu_{Cp^m})/\mathbb{Q}(\mu_{Cp^m})$ such that the set of primes of $\mathbb{Q}(\mu_{Cp^m})$ above $S \cup S_l$ has Dirichlet density $1$ with respect to $\mathbb{Q}(\mu_{Cp^m})$, plainly $\text{Tr}(\rho_A \otimes \chi(Frob_l)) = \text{Tr}(\rho_A(Frob_l))$ for all $l \in S \cup S_l$. By Chebotarev density, we conclude the trace identity: $\text{Tr}(\rho_A \otimes \chi) = \text{Tr}(\rho_A)$ over $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{Cp^m}))$.

As shown in the proof of Lemma 3.2, under the assumption of the order of $\varphi^\mu$, $7$ is irreducible over $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{Cp^m}))$. Then by a theorem of Carayol–Serre (e.g., [MFG, Proposition 2.13]), we have $\rho_A \otimes \chi \cong \rho_A$ over $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{Cp^m}))$. Then by [DHI98, Lemma 3.2], $\rho_A|_{\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{Cp^m}))} \cong \text{Ind}_{F(\mu_{Cp^m})}^\mathbb{Q} \phi$ for a Galois character $\phi$. This character $\phi$ extends to $\text{Gal}(\overline{\mathbb{Q}}/F)$ as $\rho_A$ extends to $\text{Gal}(\overline{\mathbb{Q}}/F)$ and $F$ and $\mathbb{Q}(\mu_{Cp^m})$ is linearly disjoint over $\mathbb{Q}$, and we conclude that $\rho_A$ is an induced representation from $F$ over $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus $\rho_A \otimes \chi \cong \rho_A$ over $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Since the proof is the same for $I^Q$ and $I_Q$, we deal with $I^Q$. Let $I_Q$ be the ideal generated by $a(l)$ for all rational primes $l \in S \cup S_l$ as above. Then $\rho := \rho_{TQ} \mod I_Q$ satisfies $\text{Tr}(\rho_A(Frob_l)) = 0$ for the set $S \cup S_l$. Therefore by the above argument, we conclude $\rho \otimes \chi \cong \rho$. Then by Lemma 2.4, we have $I_Q \supset I^Q$.

Since $a(l) \mod I^Q \equiv 0$ if a rational prime $l$ is inert in $F$ (as $\rho_{TQ} \mod I^Q$ is an induced representation from $F$), we conclude the reverse inclusion $I^Q \supset I_Q$.\hfill\Box

7. Proof of Theorem A and local involutions

Throughout this section, we assume (h0–4) and that $\mathbb{T}^\text{imm} \neq 0$ ($\Leftrightarrow I \neq 0$); i.e. $\Omega_{T/A} \otimes \mathbb{T} \cong I/I^2 \cong Y^\mu \neq 0$ (as otherwise, we have nothing to prove).

Before starting the proof, we ask if we can extend the involutive action of $G$ on $W[[\Delta]]$ to $R_\infty$. The answer is yes if we make a good choice of the generators $T_j^\pm$ depending on $q_j \in Q$. For that, we tentatively write $*_{\epsilon}$ for an involution of $R_\infty$ ($j = 1, 2, \ldots, r$) such that $*_{\epsilon}(T_j^\pm) = (-1)^{\delta_j} T_j^\pm$ for Kronecker’s delta $\delta_j$. Plainly this involution depends on the choice of generators $f_j$ (and hence on the variable $T_j$) in the Taylor–Wiles system. Therefore, to answer the question, we need to choose generators of the Taylor-Wiles system carefully as was done in Theorem 6.4.

Our idea of extending the involution $*_{\epsilon}$ (acting on $W[[\Delta]]$) associated to $q = q_j \in Q$ is to use the local involution coming from the normalizer of $\Gamma_0(q)$. Thus we give here a description of the local component at $q \in Q^-$ of the automorphic representation arising from $\Gamma_0(q)$. For simplicity, we choose $k := 1$ (otherwise, we need to replace $q$ in the following argument by $q^k$ which does not cause any harm), and suppose that $q \equiv 1 \mod C \rho_{Cp^m}^m$ for $C = N_{F/Q}(\epsilon)$. If $f$ is a Hecke eigenform in $S_2(\Gamma_Q, \psi_k)$ whose Hecke eigenvalues gives rise to an algebra homomorphism $\lambda : \mathbb{T} \to \mathbb{T}_p$; so, $f[T(n) = \lambda(a(n))f$ for the image $a(n)$ of $T(n)$ in $\mathbb{T}$. After lifting $f$ to an adelic automorphic form on $\text{GL}_2(\mathbb{A})$ as in [MFG], the right translation of the adelic automorphic form provides an automorphic representation $\pi_f$. Since we have twisted in (2.2) the original $\rho_{TQ}$ by a global Galois character $\sqrt{\epsilon}$ to get the universal representation $\rho^{\mu}$, we need to study the twisted automorphic representation $\pi := \pi_f \otimes \sqrt{\epsilon}^{-1}$ of $\text{GL}_2(\mathbb{A})$. The corresponding automorphic form $\mathbf{f} : \text{GL}_2(\mathbb{Q}) \to \text{GL}_2(\mathbb{A}) \to \mathbb{C}$ is the minimal form of $\pi$ as described in [HMI, after Lemma 2.4.1 in page 122]. Write $\pi = \otimes \pi_i$, for the local representation $\pi_i$ of $\text{GL}_2(\mathbb{Q})$. Since $\pi_i$ belongs to a principal series, we have two characters $\alpha, \beta : \mathbb{Q}^\times_p \to \mathbb{C}^\times$ with $\pi_i \cong \pi(\alpha, \beta)$. The cusp form $\mathbf{f}$ being minimal at $q$ means that $\mathbf{f}(ux) = \alpha(a)\beta(b)f(x)$ for $u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in the Iwahori subgroup of $\text{GL}_2(\mathbb{Q})$. Here the Iwahori subgroup $I$ at $q$ is given by

$$I := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \text{GL}_2(\mathbb{Z}_q) | c \equiv 0 \mod q \mathbb{Z}_q \right\}.$$

We write $U(q)$ for the Hecke operator acting $\pi$ given by the double coset $I \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) I$ which corresponds to the classical operator $\Gamma_Q \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \Gamma_Q$ acting on $f$ (see [MFG, (3.33) for this fact]. Writing $\pi_q \in F$ for the chosen eigenvalue of $U(q)$ to define $\pi_q$, we require $\mathbf{f}(U(q) = \alpha(q)\mathbf{f}$ with $\alpha(q) \mod m_{\pi_q} = \pi_q$. As is well known, the normalizer $N(I)$ of $I$ is generated by the class of $w_q := \left(\begin{smallmatrix} 0 & -1 \\ q & 0 \end{smallmatrix}\right) \in \text{GL}_2(\mathbb{Q}_q)$. If the conductor of $\pi$ at $q$ is $q^2$; i.e., the conductor of $\alpha$ and $\beta$ are both equal to $q$ (in this case, we say that $\pi$ is $q$-new), $w_q\mathbf{f}(x) = \mathbf{f}(wx_q)$ belongs to $\pi$ and satisfies $(w_q\mathbf{f})(ux) = \beta(\alpha)\alpha(b)(w_q\mathbf{f})(x)$ for $u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in I$ and $U(q)(w_q\mathbf{f}) = \beta(q)w_q\mathbf{f}$. Define $\lambda' : \mathbb{T} \to \mathbb{T}_p$
by \( h(w_q f) = \lambda(h) w_q f \). Recall \( \rho_q \big|_{\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} = \left( \begin{smallmatrix} 0 & 1 \\ \alpha_q & \gamma_q \end{smallmatrix} \right) \) in (2.3) with two characters \( \delta_q \) and \( \delta_q' \). This shows \( w_q f \) corresponds to \( \delta_q' \) and \( \alpha = \lambda \circ \delta_q \) and \( \beta = \lambda' \circ \delta_q' \) regarding \( \alpha \) and \( \beta \) as a local Galois character by local class field theory. Then \( T_Q / (\ker(\lambda) \cap \ker(\lambda')) \) is stable under the involution \( h \mapsto w_q hw_q^{-1} \). Thus the involution induced by \( w_q \) on \( T_Q / (\ker(\lambda) \cap \ker(\lambda')) \) flips \( \alpha \) and \( \beta \) and therefore induces \( b_\eta \) on the image of \( W[\Delta_q] \) in \( T_Q / (\ker(\lambda) \cap \ker(\lambda')) \). Since \( \alpha \beta(q) = \chi(q)q \) (as we have chosen \( q \equiv 1 \mod \mathbb{Z}^m \)), the operator \( U(q) + \chi(q)qU(q)^{-1} \) has eigenvalue \( \alpha(q) + \beta(q) \) for \( f \).

Now we need to show the involution \( h \mapsto w_q hw_q^{-1} \) is well defined on \( T_Q / \ker(\lambda) \) when \( f \) is \( q \)-old. Thus we now assume that \( \pi \) is spherical at \( q \) and hence has two linearly independent \( I \)-fixed vectors. Write \( H \) (resp. \( H_I \)) for the spherical (resp. Iwahori) Hecke algebra over \( \mathbb{Z}_p \) with respect to \( GL_2(\mathbb{Z}_q) \subset GL_2(\mathbb{Q}_q) \) (resp. with respect to the Iwahori subgroup \( I \subset GL_2(\mathbb{Q}_q) \)). Let \( J \) be the Iwahori subgroup of \( PGL_2(\mathbb{Z}_q) \) (i.e., the image of \( I \) in \( PGL_2(\mathbb{Q}_p) \)) and \( H_J \) be the Iwahori Hecke algebra with respect to \( J \subset PGL_2(\mathbb{Q}_q) \) over \( \mathbb{Z}_p \). Let \( Z \subset GL_2(\mathbb{Q}_q) \) be the center. Write the image of \( x \in GL_2(\mathbb{Q}_q) \) in \( PGL_2(\mathbb{Q}_q) \) as \( \overline{x} \), and take an unramified character \( \xi : Z \to \mathbb{Z}_p^\times \). Consider the ideal \( J = J_0 \kappa \) of \( H_0 \) generated by \( S_q - \xi(q) \) for \( S_q:= I \left( \begin{smallmatrix} 0 & 0 \\ q & 1 \end{smallmatrix} \right) \). Since \( S_q \) commutes with every element in \( H_J \), the ideal \( J \) is a two-sided ideal, and \( i : H_{1/3} \cong H_J \) as \( \mathbb{Z}_p \)-modules by sending \( IxI \mod J \) to \( \overline{x} \).

Plainly \( H_J \) contains the Hecke algebra \( H_0 \) of \( J \) with respect to the maximal compact subgroup \( PGL_2(\mathbb{Z}_q) \). Since \( H_0 \) is isomorphic to the Hecke algebra of \( I \) with respect to \( GL_2(\mathbb{Z}_q) \), we may also regard \( H_0 \subset H_J \). Then for the cocharacter group \( X^* \) of the maximal split torus \( P \) of \( PGL_2 \), we have \( H_J \cong H_0 \otimes_{\mathbb{Z}_q} Z_p[X_*] \) as \( \mathbb{Z}_p \)-modules (see [HKP10, Lemma 1.7.1]). Though [HKP10] treats Hecke algebras over \( \mathbb{C} \), as long as \( q \) is a prime number, we can find the base integral domain, this type of result remains true. The group algebra \( Z_p[X_*] \) is actually a subalgebra of \( H_J \) and the generating cocharacter \( q \mapsto \left( \begin{smallmatrix} 0 & 0 \\ 1 & 1 \end{smallmatrix} \right) \) is sent to \( q^{-1}U(q) \in H_J \) (and its inverse \( q \mapsto \left( \begin{smallmatrix} 0 & 1 \\ q & 0 \end{smallmatrix} \right) \) is sent to \( qU(q)^{-1} \)). Here we have written \( U(q) \) for the double coset \( J \left( \begin{smallmatrix} 0 & 0 \\ 1 & 1 \end{smallmatrix} \right) J \).

For the center \( Z \), we have a splitting of the diagonal torus \( T \) of \( GL_2(\mathbb{Q}_q) \): \( T = Z \times PT \) given by \( \left( \begin{smallmatrix} 0 & 0 \\ 1 & 1 \end{smallmatrix} \right) \mapsto (b, \left( \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)) \). Thus \( X_* \) can be considered a subgroup of \( X_*(T) \). In this way, we have a section \( H_J \mapsto H_I \) identifying \( Z_p[X_*] \) with subalgebra of \( Z_p[X_*(T)] \subset H_I \). Therefore the isomorphism \( i \) induces an identification of \( Z_p[X_*] \cong Z_p[|q^{-1}U(q)|] \) as \( \mathbb{Z}_p \)-subalgebras of \( H_{1/3} \).

**Remark 7.1.** Keep assuming \( k = 1 \) for simplicity. We take \( \xi := \chi \big|_{\mathbb{Q}_q^\times} \), since the central character of \( \pi_q \) is \( \chi \big|_{\mathbb{Q}_q^\times} \), as long as \( q \equiv 1 \mod \mathbb{Z}/\mathbb{Z}^m \). Then \( Z_p[X_*(Z)] \) acts by the character \( \xi \) and hence the action of \( H_I \) on \( f \) factors through \( H_{1/3} \). Since \( U(q) \in H_J \) satisfies \( X^* - T(q)X + Y(q) = 0 \), \( T(q) \in H \) corresponds to \( U(q) + \chi(q)qU(q)^{-1} \in H_I \). The involution \( i : x \mapsto w_q^{-1}xw_q \) flips the diagonal entry of \( x \in T \). In \( H_{1/3} \), we have

\[
i(U(q)) = I_i((\begin{smallmatrix} 0 & 0 \\ q & 1 \end{smallmatrix})) = I((\begin{smallmatrix} 0 & 1 \\ q & 0 \end{smallmatrix})) = Iq(q^{-1}0)I = S_q U(q^{-1}) = \chi(q)q U(q^{-1}) = q U(q)^{-1} \mod p^m.
\]

Thus the involution \( i \) coincides with the involution induced from \( x \mapsto -x \) on \( Z_p[X_*] = Z_p[X_*(PT)] \) and with the involution \( S_q \mapsto -S_q \) on \( Z_p[S_q] = Z_p[X_*(Z)] \).

\[
i(U(q)) = \chi(q) \xi(U(q)) \mod p^m.
\]

Then \( H_{1/3} \) coming from \( x \mapsto w_q^{-1}xw_q \) sends \( T(q) \) to \( \chi(q)T(q) \) modulo \( p^m \).

If we replace \( qU(q) \) by \( q^k U(q) \) and take \( \xi = \chi \big|_{\mathbb{Q}_q^\times} \), the above remark remains true for general \( k \geq 1 \). We can see the content of Remark 7.1 (i.e., \( \iota(U(q)) = \chi(q)U(q)^{-1} \mod p^m \)) in an elementary matrix computation without using the theory of Iwahori Hecke algebra. To see this (still assuming \( k = 1 \)), we consider the two dimensional space \( V \) spanned by \( f \) and \( \eta f \) for \( \eta = \left( \begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix} \right) \).

We prepare two copies of \( V_0 = \mathbb{C}f \subset \pi \). Define \( i : V_0^2 \to V \) by \( (f_1, f_2) \mapsto f_1 + \eta f_2 \). As seen in [HIM, Lemma 3.13], \( U(q) \) as a matrix form on \( V_0^2 \) is given by \( U(q) = \left( \begin{smallmatrix} T(q) & -1 \\ qX(q) & 0 \end{smallmatrix} \right) \) (i.e., \( U(q)(i(f_1, f_2)) = i((f_1, f_2)U) \)). It is easy to see \( w_q f = \eta f \) and \( w_q \eta f = S_q f = \chi(q) f \) as \( w_q \) commutes with \( \eta \). Thus we have \( U^* := i(U) = \chi(q) \xi(U) \).
By Theorem 6.4, we can choose the Taylor–Wiles prime group modulo $p$ of the image of Lemma 7.2.

This eigenspace is trivial. Indeed the Iwasawa power series for $\tilde{W}$ implies two characters sending the space to the subspace on which $A_{\tilde{W}}^{\ast}$ acts on $\tilde{W}$. Making this choice of the variable $\tilde{W}$, we do not have the $\ast$ variables $X$ modulo $A_{\tilde{W}}$. If $a \neq b$ and $s_j$ for the $\ast$-eigenspace of the ray class field implies $s_j = s_k$ for $t_r$. However, we have $s_j = s_k$ for all $l$ for $s_j^l$ in Definition 4.3.

As remarked in Remark 7.1, the involution $s_j$ with the property of Lemma 7.2 makes sense only modulo $p^m$ on $R_{n,m}$ (with $0 < n \leq m$) for $q = q_j$ (in other words, $s_j \equiv q_j$ modulo $p^m$ on $W[\Delta_{Q,n}]$), and hence taking the coherent limit $R_{\infty} = \lim_{\rightarrow} R_n$ as in Remark 6.5, we have well defined $s_j$ on $R_{\infty}$. Making this choice of the variable $T_j$ (as in Theorem 6.4), we write $\ast$ for $s_j$ in Lemma 7.2 now acting on $R_{\infty}$ made via Remark 6.5 (not just on $W[\Delta]$). Thus the group $G := \prod_{j} (g_j)$ (of order $2^{-r}$) acts on $R_{\infty}$ and $\mathcal{R}$.

**Lemma 7.3.** If $p \nmid h_F$, we have $Sel_{\Delta}^1(\chi \omega) = 0$; so, $r_+ = 0$.

**Proof.** By Proposition 3.8, $Sel_{\Delta}^1(\chi \omega)$ is isomorphic to the $\mathcal{F}$-dual of the $\chi \omega$-eigenspace of the ray class group modulo $p^\infty$ of the splitting field of $\chi \omega$ (which is the maximal totally real subfield of $\mathcal{O}_F$). This eigenspace is trivial. Indeed the Iwasawa power series for $\chi \omega$ is a unit since the corresponding Kubota–Leopoldt $p$-adic L evaluated at $s = 0$ is a $p$-adic unit by $p \nmid h_F$ (see [LPL, 8.7]).

We now start the proof of Theorem A. In this proof, we give an argument which applies to $\mathcal{T}$ and $\mathcal{T}/(t - \gamma^k)$ at the same time. So we write for simplicity $A$ for either $\mathcal{T}$ or $\mathcal{T}/(t - \gamma^k)$, and put

$$B = \begin{cases} W & \text{if } A = \mathcal{T}/(t - \gamma^k), \\ A & \text{if } A = \mathcal{T}, \end{cases}$$

which is the base subalgebra of $A$. Similarly, we write $A$ for $\mathcal{R}$ or $R_{\infty}$ according as $A = \mathcal{T}$ or $A = \mathcal{T}/(t - \gamma^k)$. Plainly by Lemma 7.3, $A^{G} = \mathcal{B}[\{T_j^{-1}, \ldots, T_r^{-1}\}]^{G} = \mathcal{B}[\{T_j^{-1}, \ldots, T_r^{-1}\}]$. To make notation simple, we just write $Y_j$ for $(T_j)^{-2}$; so, $A^{G} = \mathcal{B}[\{T_j^{-1}, \ldots, T_r^{-1}\}]^{G} = \mathcal{B}[\{Y_1, \ldots, Y_r\}]$. Though, we do not have the $\ast$-eigenspace $\mathcal{T}_{\ast}$ by Lemma 7.3, our argument goes through taking the quotient of $R_{\infty}$ and $\mathcal{R}$ by the ideal $(T_{i,1}^+, \ldots, T_{i,r}^+)$. This remark possibly applies to the case of a totally real base field where $r_+$ might be positive; so, we argue in the following proof as if $r_+$ were positive (forgetting the above lemma).

Let $\tilde{\Theta}_i$ be the image of $T_i$ in $m_{\tilde{A}}$. By Proposition 3.8, the image of $\Theta_i$ (i.e., $i = 1, \ldots, r_-$) in the co-tangent space of $A$ over $A$ spans the minus part of dimension $r_-$. As $G$ acts on $\mathcal{R}$ (and $R_{\infty}$) by $\gamma_i(T_j) = (-1)^{\delta_{i,j}}T_j^\gamma$, $G$ acts non-trivially on $A$. For the cotangent space $\mathcal{T}_{A/B} = m_{\tilde{A}}/m_{\tilde{A}}^2 = \Omega_{A/B} \otimes_{F} A$, we have $G \hookrightarrow \text{Aut}(\mathcal{T}_{A/B})$, and hence $G \hookrightarrow \text{Aut}_{\mathcal{B}_{\ast}}(A)$. Let $\tilde{G} := \text{Hom}_{\text{group}}(G, \mu_2(W))$ with the identity character $1 \in \tilde{G}$, and define $\varepsilon_i \in \tilde{G}$ by $\varepsilon_i(T_j) = \varepsilon_i(b)T_j^{-\delta_{i,j}}$ for $b \in G$; so, $\tilde{G} = \prod_{i} (\varepsilon_i)$. Since $G$ acts on $A$ and $\mathcal{A}$, we can decompose $\mathcal{A} = \bigoplus_{\varepsilon \in \tilde{G}} \mathcal{A}[\varepsilon]$ and $A = \bigoplus_{\varepsilon \in \tilde{G}} A[\varepsilon]$ as direct sum of $\varepsilon$-eigenspaces $\mathcal{A}[\varepsilon]$ and $A[\varepsilon]$. Note that $A[\varepsilon]$ is free of rank 1 over $\mathcal{A}[\varepsilon] = \mathcal{A}[1]$. More generally, we write $X[\varepsilon]$ for the $\varepsilon$-eigenspace of any $p$-profinite module $X$ on which $G$ acts.
Since $A$ is reduced, $\text{Frac}(A)$ is a product of fields finite over $\text{Frac}(B)$. Therefore $b_j \in G$ either permutes some simple components of $\text{Frac}(A)$ or induces a non-trivial automorphism of some other simple components of $\text{Frac}(A)$; so, we have $(b_j) \subset \text{Aut}(A/B)$, and $b_j$ are all distinct in $\text{Aut}(A/B)$. Thus $b_1, \ldots, b_r$ generate a subgroup of $\text{Aut}(A/B)$ isomorphic to $G$. Therefore, the $\varepsilon$-eigenspace $A[\varepsilon] \neq 0$ for all $\varepsilon \in \hat{G}$, and $A[\varepsilon]$ (as a factor of the $B$-free module $A$) is free of finite rank over $B$.

The $\varepsilon$-eigenspace of $A[\varepsilon]$ is generated over $A^G$ by the lowest degree monomial $T_\varepsilon := \prod_{j \in (b_j) = -1} T_j$ such that $b(T_\varepsilon) = \varepsilon(b)T_\varepsilon$ for any $b \in G$. Therefore, $\Theta_\varepsilon := \prod_{j \in (b_j) = -1} \Theta_j$ generates $A[\varepsilon]$ over $A^G$. We have $A[\varepsilon]A[\varepsilon] \subset A[\varepsilon]$; in particular, $A[\varepsilon] = A^G \Theta_\varepsilon$ as $A^G$ contains the identity element. Since $I$ is stable under $G$, we have a decomposition $I = \bigoplus \Theta_j I[\varepsilon]$ with $I[\varepsilon] = I \cap A[\varepsilon]$ into the direct sum of $\varepsilon$-eigenspaces. Since $I$ is generated by $\Theta_j$, it contains $\Theta_e$ for all $\varepsilon \neq 1$, and hence $I[\varepsilon] = A[\varepsilon]$ for $\varepsilon \neq 1$. Thus we conclude $I = I^G \otimes \bigoplus_{\varepsilon \neq 1} A[\varepsilon]$ and $A/I = A^G/I^G$, which we write $A^\cm$ (so, $A^\cm$ is $W[[H]]/(t-\gamma^k)$ or $W[[H]]$ according as $A = \mathbb{T}/(t-\gamma^k)$ or $\mathbb{T}$).

Since $p \nmid h_F$, we have $R_\infty/(T_1, \ldots, T_r) = W[[S_1^+, \ldots, S_r^+]]$ by Propositions 1.4 and 2.6, and we also conclude $R/(T_1, \ldots, T_r) = \Lambda[[S_1^+, \ldots, S_r^+]]$. This implies

$$B[[T_1^+, \ldots, T_r^+]] = A/(T_1^-, \ldots, T_r^-) = B[[S_1^+, \ldots, S_r^+]].$$

Therefore the graded algebra $\text{gr}(A)$ with respect to $(T_1^-, \ldots, T_r^-)$ of $A$ is isomorphic to the polynomial ring $B[[S_1^+, \ldots, S_r^+]][[T_1, \ldots, T_r]]$. This implies

$$A = \lim_{n} B[[S_1^+, \ldots, S_r^+]][T_1, \ldots, T_r]/(T_1^-, \ldots, T_r^-)^n = B[[S_1^+, \ldots, S_r^+, T_1^-, \ldots, T_r^-]]$$

and hence

$$A = A/(S_1^+, \ldots, S_r^+, S_1^-, \ldots, S_r^-)
= B[[S_1^+, \ldots, S_r^+, T_1^-, \ldots, T_r^-]]/(S_1^+, \ldots, S_r^+, S_1^-, \ldots, S_r^-) = B[[T_1^+, \ldots, T_r^-]]/(S_1^+, \ldots, S_r^-).$$

In other words, we may ignore the variables $S_i^+$ (even if they exist). Thus now write $A := B[[T_1^+, \ldots, T_r^-]]$. Then we have

$$A[\varepsilon] = B[[T_1^-, \ldots, T_r^-]]^G = B[[Y_1, \ldots, Y_r]]T_\varepsilon$$

and $(S_1^-, \ldots, S_r^-)[\varepsilon] = A[\varepsilon] \cap (S_1^-, \ldots, S_r^-)$. We note a corollary of Lemma 7.2 which follows from the above argument and the definition of $S_i$ in Definition 4.3:

**Corollary 7.4.** For each $j = 1, 2, \ldots, r_-$, we have $S_j^- = f_j(Y_1, \ldots, Y_r)T_j^-$ with a power series $0 \neq f_j \in B[[Y_1, \ldots, Y_r]]$. Moreover, $f_j$ (resp. $f_j(0)$) is not a unit in $B[[Y_1, \ldots, Y_r]]$ (resp. in $B$).

**Proof.** By Lemma 7.2 and the choice of $T_j^-$, $T_j^-$ and $S_j^-$ belong to the same eigenspace $A[\varepsilon]$ for all $\varepsilon \in \hat{G}$ since $A[\varepsilon] = A^G T_j^- = B[[Y_1, \ldots, Y_r]]$-free of rank 1, we find $S_j^- = f_j T_j^-$ for $0 \neq f_j \in B[[Y_1, \ldots, Y_r]] = A^G$. If $f_j$ is a unit, $S_j^- \mod m^2_A$ and $T_j^- \mod m^2_A$ generates the equal one dimension subspace of the coset $T_\varepsilon [T_\varepsilon]$ in which $S_j^- = 0$. This is a contradiction as $T_j^- \neq 0 \mod m^2_A$ by Lemma 6.2. Thus $f_j$ is a non-unit. Hence $f_j(0)$ cannot be a unit in $B$.

There is another argument showing the non-unit property. Here it is: By Proposition 3.8, the $-1$ eigenspace dimension $d_Q^-$ of the tangent space of $T_Q$ and $\mathbb{T}Q$ is independent of $Q$. If one of $f_i$ is a unit, then the $d_0^- < d_Q^-$, a contradiction. Thus $f_j (j = 1, 2, \ldots, r_-)$ are all non-unit.

Defining the $\varepsilon$-projection for $\varepsilon \in \hat{G}$ by $\pi[\varepsilon](x) = \sum_{b \in G} \varepsilon(b)b(x)$ (so $X[\varepsilon] = \pi[\varepsilon](X)$ for any profinite module $X$ on which $G$ acts), if $b(x_i) = \varepsilon_i(b)x_i$ for all $b \in G$ (i.e., $x_i = y_i T_\varepsilon^-$ with $y_i \in A^G$), we have

$$\pi[\varepsilon](\sum_i a_i x_i) = \sum_i \sum_b b(a_i)x_i(\varepsilon(b)) = \sum_i \sum b(a_i)x_i \varepsilon(\varepsilon(b)) = \sum_i \pi[\varepsilon][\varepsilon](a_i)x_i.$$
Since \( x_i = y_i T_{i}^{-} \) with \( y_i \in \mathcal{A}^G \), we have
\[
(x_1, \ldots, x_r)[c] = (y_1 T_{i}^{-} T_{i}^{\varepsilon}, \ldots, y_r T_{i}^{-} T_{r}^{\varepsilon}) \mathcal{A}^G.
\]
If \( \varepsilon(b_i) = 1 \) (i.e., \( \varepsilon \) does not contain \( \varepsilon_i \)), we have \( T_{i}^{-} T_{i}^{\varepsilon} = (T_{i}^{-})^2 T_{i} = Y_i T_{i} \), and if \( \varepsilon(b_i) = -1 \) (i.e., \( \varepsilon \) does contain \( \varepsilon_i \)), we have \( T_{i}^{-} T_{i}^{\varepsilon} = T_{i} \). This shows
\[
I[\varepsilon] = (T_{i}^{-}, \ldots, T_{r}^{-})[\varepsilon] = (T_{i}^{\varepsilon})_{A^G}
\]
and hence \( I[\varepsilon] = (T_{i})_{A^G} = \mathcal{A}[\varepsilon] \) if \( \varepsilon \neq 1 \), \( I^G = (Y_1, \ldots, Y_r) \).

Similarly, for \( \mathfrak{A} = (S_1^{-}, \ldots, S_r^{-}) \), its \( \varepsilon \)-eigenspace is given by
\[
\mathfrak{A}[\varepsilon] = T_\varepsilon a_\varepsilon \text{ for } a_\varepsilon := \left( \sum_{j: \varepsilon(b_j) = -1} f_j \mathcal{A}^G + \sum_{i: \varepsilon(b_i) = 1} Y_i f_i \mathcal{A}^G \right).
\]

Note here \( a_\varepsilon \) is an ideal of \( \mathcal{A}^G \). We have, if \( \varepsilon \neq 1 \),
\[
\mathcal{A}[\varepsilon] = \frac{B[[Y_1, \ldots, Y_r]T_{\varepsilon}]}{(S_1^{-}, \ldots, S_r^{-})[\varepsilon]} = \frac{I[\varepsilon]}{T_\varepsilon a_\varepsilon} \cong \frac{\mathcal{A}^G}{a_\varepsilon},
\]
and
\[
\mathcal{A}^G = \frac{B[[T_{i}^{-}]_2^2 \cdots T_{r}^{-}]}{(T_{i}^{-})_2 f_1, \ldots, (T_{r}^{-})_2 f_r}_{A^G} \cong \frac{B[[Y_1, \ldots, Y_r]]}{(Y_1 f_1(Y), \ldots, Y_r f_r(Y))_{A^G}},
\]
where the last identity is under the identification of \( B[[T_{i}^{-}]_2^2 \cdots T_{r}^{-}] \) with \( B[[Y_1, \ldots, Y_r]] \) under \( (T_{j}^{-})^2 \sim Y_j \). Thus \( \mathcal{A}^G \) is a complete intersection, and \( f_\varepsilon := \{ f_j(Y) \}_{j: \varepsilon(b_j) = -1} \cup \{ Y_i f_i(Y) \}_{i: \varepsilon(b_i) = 1} \) is a regular sequence of \( B[[Y_1, \ldots, Y_r]] \) since \( \mathcal{A}[\varepsilon] \) is free of finite rank over \( B \) (see [CRT, Theorem 17.4]). Since \( \mathcal{A}[\varepsilon] = \mathcal{A}^G T_{\varepsilon} \), we have a surjective morphism of \( \mathcal{A}^G \)-modules:
\[
\varpi_\varepsilon : \frac{B[[Y_1, \ldots, Y_r]]}{(Y_1 f_1(Y), \ldots, Y_r f_r(Y))_{A^G}} \to \mathcal{A}[\varepsilon] \cong \frac{B[[Y_1, \ldots, Y_r]]}{\sum_{j: \varepsilon(b_j) = -1} f_j \mathcal{A}^G + \sum_{i: \varepsilon(b_i) = 1} Y_i f_i \mathcal{A}^G}
\]
sending \( g \mapsto g \theta_\varepsilon \), whose kernel is given by
\[
\text{Ker}(\varpi_\varepsilon) = \frac{\sum_{j: \varepsilon(b_j) = -1} f_j \mathcal{A}^G + \sum_{i: \varepsilon(b_i) = 1} Y_i f_i \mathcal{A}^G}{(Y_1 f_1(Y), \ldots, Y_r f_r(Y))} = \text{Ann}_{A^G}(\theta_\varepsilon) = \sum_{j: \varepsilon(b_j) = -1} \text{Ann}_{A^G}(\theta_j).
\]
Here \( \text{Ann}_{A^G}(\theta_j) \) is the annihilator \( \mathcal{A}^G \)-ideal of \( \theta_j \). Thus \( \text{Ker}(\varpi_\varepsilon) \) is isomorphic to
\[
\frac{\sum_{j: \varepsilon(b_j) = -1} f_j(Y) \mathcal{A}^G + \sum_{i: \varepsilon(b_i) = 1} Y_i f_i(Y) \mathcal{A}^G}{(Y_1 f_1(Y), \ldots, Y_r f_r(Y)) \cap \sum_{j: \varepsilon(b_j) = -1} f_j(Y) \mathcal{A}^G} \cong \frac{\sum_{j: \varepsilon(b_j) = -1} f_j(Y) \mathcal{A}^G}{(Y_1 f_1(Y), \ldots, Y_r f_r(Y)) \cap \sum_{j: \varepsilon(b_j) = -1} f_j(Y) \mathcal{A}^G}.
\]

Let \( \mathfrak{D}_\varepsilon := \sum_{i: \varepsilon(b_i) = 1} T_i^\varepsilon \mathcal{A} \) and \( \mathfrak{a}_\varepsilon := \{ \sum_{j: \varepsilon(b_j) = -1} f_j \mathcal{A} + \sum_{i: \varepsilon(b_i) = 1} Y_i f_i \mathcal{A} \} \) as \( \mathcal{A} \)-ideals. Then we have
\[
\mathfrak{a}_\varepsilon := (S_1^{-}, \ldots, S_r^{-}) = (T_1^{-} f_1(Y), \ldots, T_r^{-} f_r(Y)) \subset \mathfrak{D}_\varepsilon.
\]

Similarly put \( \mathfrak{B}_\varepsilon := \sum_{i: \varepsilon(b_i) = 1} Y_i f_i \mathcal{A}^G + \sum_{j: \varepsilon(b_j) = 1} Y_j \mathcal{A}^G \). In the same way, we have
\[
\mathfrak{B} := (Y_1 f_1(Y), \ldots, Y_r f_r(Y))_{A^G} \subset \mathfrak{B}_\varepsilon.
\]

**Lemma 7.5.** Let \( \underline{g} := \{ f_j(Y) \}_{j: \varepsilon(b_j) = 1} \cup \{ Y_i \}_{i: \varepsilon(b_i) = 1} \) (resp. \( \underline{g}' := \{ f_j(Y) \}_{j: \varepsilon(b_j) = 1} \cup \{ T_i^{-} \}_{i: \varepsilon(b_i) = 1} \) which is a minimal set of generators of \( \mathfrak{B}_\varepsilon \) (resp. \( \mathfrak{D}_\varepsilon \)). Then \( \underline{g} \) and \( \underline{g}' \) is a regular sequence in \( \mathcal{A}^G \) and \( \mathcal{A} \), respectively. Moreover \( \mathfrak{B}_\varepsilon = \bigcap_{\varepsilon} \mathfrak{B}_\varepsilon, \mathfrak{a}_\varepsilon = \bigcap_{\varepsilon} \mathfrak{a}_\varepsilon, \mathfrak{a}_\varepsilon' = \bigcap_{\varepsilon} \mathfrak{a}_\varepsilon' \subset \mathfrak{D}_\varepsilon, \mathcal{A}^G/\mathfrak{B}_\varepsilon \) and \( \mathcal{A}^G/\mathfrak{B}_\varepsilon \) are \( B \)-free of finite rank for all \( \varepsilon \).

Since the proof is the same for \( \mathfrak{B} \) and \( \mathfrak{a}_\varepsilon \), we shall give a proof for \( \mathfrak{B}_\varepsilon \).

**Proof.** Since \( \mathfrak{B}_\varepsilon \) contains \( \mathfrak{B} \) and \( \mathcal{A}^G = \mathcal{A}/\mathfrak{B} \) is free of finite rank over \( B \), for any system \( \{ a_1, \ldots, a_j \} \subset \mathfrak{m}_B \) of parameters of \( B \) (so \( j = 1 \) or 2 according as \( B = W \) or \( \Lambda \) ), \( \mathfrak{B}_\varepsilon \) is a finite ring; so, \( \text{height}(\mathfrak{B}_\varepsilon + (a_1, \ldots, a_j)) = \dim \mathcal{A} \), and by [CRT, Theorem 17.4 (3)], \( \underline{g} \cup \{ a_1, \ldots, a_j \} \) is a system of parameters of \( \mathcal{A} \). In particular \( \underline{g}_B \) is a regular sequence of \( \mathcal{A} \) by [CRT, Theorem 17.4 (1)].

Pick a minimal prime ideal \( P \supset \mathfrak{B}_\varepsilon = (Y_1 f_1(Y), \ldots, Y_r f_r(Y)) \). Then \( P \) contains either \( Y_j \) or \( f_j \). Then choose \( \varepsilon \in \hat{G} \) so that \( \varepsilon(b_j) = 1 \Leftrightarrow Y_j \not\in P \). By definition \( P \supset \mathfrak{B}_\varepsilon \). Thus any minimal
prime of $A^G$ contains $\mathfrak{B}' := (\cap_i \mathfrak{B}_i)/\mathfrak{B}$. In other words, $\mathfrak{B}'$ is nilpotent as $\cap_i \mathfrak{B}_i$ is the nilradical of $\mathfrak{B}$ (e.g., [CRT, §3]). Since $A^G = A^G/\mathfrak{B}$ is reduced, we find $\mathfrak{B} = \cap_i \mathfrak{B}_i$. We claim that $A^G/\mathfrak{a}_c$ is reduced. Indeed, if $a \in \sqrt{\mathfrak{a}_c}$ but $a \notin \mathfrak{a}_c$, then $a^n \notin \mathfrak{a}_c$ for $n > 0$. Thus $(a\Theta_e)^n = a^n\Theta_e^n \subset \mathfrak{a}_c \Theta_e^n = \{0\}$ as $\mathfrak{a}_c = \text{Ann}_{A^G}(\Theta_e)$, and hence $a\Theta_e$ is nilpotent. Since $A$ is reduced, we find $a\Theta_e = 0$; so, $a = \text{Ann}_{A^G}(\Theta_e)$. This shows reducedness of $A^G/\mathfrak{a}_c$. Then, by the same argument as above, since $\mathfrak{a}_c = (\sum_{i \in (b_j) = -1} f_j A^G + \sum_{i \in (b_j) = 1} Y_f(Y,A^G)$, $\mathfrak{a}_c = \cap_{\epsilon_c(b_j) = \epsilon(b_j) = 1} \mathfrak{B}_c$.

Since $\{Y_f(Y),...,Y_{-r_f(Y)}(Y)\}$ is a regular sequence, $P$ is of height $r_-$ by [CRT, Theorems 17.4 and 17.6] and [BCM, IV.1.4.2]. Since $A^G = A^G/\mathfrak{B}$ is free of finite rank over $B$, if $p \in P$, $P$ is of height $r_- + 1$, a contradiction. Thus the residue field of $P$ is of characteristic 0. Taking $B = W$, $A^G/\mathfrak{B}_c \leftarrow \prod_{p \in \mathfrak{B}_c, p \text{ minimal prime}} A^G/\mathfrak{P}$ is $p$-torsion-free; so, $B$-free. If $B = \Lambda$, we have $(A^G/\mathfrak{B}_c)/(t-\gamma)$ is $W$-free of finite rank $m$ by the above argument. By Nakayama’s lemma, $A^G/\mathfrak{B}_c$ is generated by $m$ elements as a $\Lambda$-module. Therefore we have a surjective $\Lambda$-algebra homomorphism $\pi : A^m \to A^G/\mathfrak{B}_c$. We can vary $k \geq 2$, and rank$_W(A^G/\mathfrak{B}_c)/(t-\gamma)$ is independent of $k$. Then we conclude $\text{Ker}(\pi) \subset \cap_{k \geq 2} (t-\gamma)A^m = 0$; so, $\pi$ is an isomorphism, and $A^G/\mathfrak{B}_c$ is $\Lambda$-free of rank $m$.

Since $A^G$ is $B$-free of finite rank, by the exact sequence $\mathfrak{B}_c/\mathfrak{B} \leftarrow A^G \to A^G/\mathfrak{B}_c$, $B$-freeness of $A^G/\mathfrak{B}_c$ tells us that $\mathfrak{B}_c/\mathfrak{B}$ is $B$-free of finite rank. \hfill \Box

\textbf{Lemma 7.6.} Let the notation be as above, and put $A^c := A/I$. The characteristic element in $B$ of the $B$-torsion module $\Omega_{A/B} \otimes_B A^c$ is given by $\prod_{i=1}^\infty f_j(0) \in B$. In particular, $f_j(0)$ is non-zero and non-unit in $B$ (i.e., the sequences $\{f_j, Y_1,...,Y_r\}$ and $\{f_j, T_{i_1}^{-1},...,T_{i_r}^{-1}\}$ for any single $j$ are regular sequences in $A$ of height $r_- + 1$). More generally, for $1 \neq \epsilon \in \widetilde{G}$, $\{f_j : j \in (b_j) = -1 \cup \{f_{k}\}_{k \in (b_k) = 1}$ and $\{f_j : j \in (b_j) = -1 \cup \{f_{k}\}_{k \in (b_k) = 1}$ are regular sequence in $A$ of length $r_- + 2$, where $i$ is any one index with $\epsilon_i = 1$.

\textbf{Proof.} By Corollary 7.4, $f_j(0)$ cannot be a unit. Write $A^{ncm} = A/\mathfrak{a}$ (so, $\mathfrak{a} = (A^{ncm} \oplus 0) \cap A$). Then the annihilator of $I = A(\sigma - 1)A$ regarded as an ideal of $A^{ncm}$ is the zero ideal (since $A^{ncm} \otimes_B \text{Frac}(B) = I \otimes_B \text{Frac}(B)$). Again we have a decomposition $A^{ncm} = \bigoplus_{\epsilon \in \widetilde{G}} A^{ncm}[\epsilon]$ into the sum of the $\epsilon$-eigenspaces $A^{ncm}[\epsilon]$ under the action of $G$. Since $I = (\Theta_1,...,\Theta_{r_-})$ and $A^{ncm}[\epsilon] = A[\epsilon] = I[\epsilon]$ as long as $\epsilon \neq 1$ as already remarked, we have $I^G = \bigoplus_j A^{ncm}[1](\Theta_j)\epsilon^2$ and $I = (\bigoplus_j A^{ncm}[1](\Theta_j)\epsilon^2) \oplus \bigoplus_{\epsilon \neq 1} A[\epsilon].$

Since $I = (\Theta_1,...,\Theta_{r_-})$, we have $I^2 = (\Theta_1,\Theta_j)(\epsilon) \epsilon^2 \supset \bigoplus_j A^{ncm}[1](\Theta_j)\epsilon^2 = I^G$. If $\#|\epsilon| \geq 2$ writing $|\epsilon| := \{j\in(b_j) = -1\}$, decomposing $\epsilon = \epsilon_1\epsilon_2$ with non-empty and disjoint $|\epsilon_j|$ ($j = 1, 2$), the $\epsilon$-eigenspace $(I^2)[\epsilon]$ contains $\Theta_\epsilon = \Theta_{\epsilon_1}\Theta_{\epsilon_2}$ and hence $A[\epsilon] = I[\epsilon] = (I^2)[\epsilon]$. If $\#|\epsilon| = 1$, we have $(I^2)[\epsilon] = I^G A[\epsilon]$. Thus we conclude

\begin{equation}
I/I^2 = \bigoplus_{\epsilon : \#|\epsilon| = 1} (I/I^2)[\epsilon] = \bigoplus_{\epsilon : \#|\epsilon| = 1} A[\epsilon]/I^G A[\epsilon].
\end{equation}

Recall that $\epsilon_i \in \widetilde{G}$ is the dual of $b_i$ (i.e., $\epsilon_i(b_j) = (-1)^{\delta_{ij}}$ for the Kronecker delta $\delta_{ij}$). From the exact sequence

\begin{equation}
0 \to (S_j)_{j/\mathfrak{a}}/(S_j)^2 = \bigoplus_j A \cdot dS_j \to \bigoplus_j A \cdot dT_j \to \Omega_{A/B} \to 0,
\end{equation}

tensoring with $B \cong A^{ncm}$ over $A$ and taking $\epsilon_j$-eigenspace, we get another exact sequence

\begin{equation}
0 \to B \cdot dS_j \to B \cdot dT_j \to (\Omega_{A/B} \otimes_B A^{ncm})[\epsilon] = (I/I^2)[\epsilon] \to 0.
\end{equation}

Note that $A/(T_{i_1},...,T_{i_r}) = A/A(\sigma - 1)A = A/A(\sigma - 1)A = B = A^{ncm}$. Since $S_j = f_j T_j$ for $f_j \in \mathfrak{B}$, $A^{G} = B[[Y_1,...,Y_r]]$, for the constant term $f_j(0)$ of $f_j(Y)$, under the notation of (7.3), we have

\begin{equation}
(I/I^2)[\epsilon] = \frac{B \cdot dT_j}{B \cdot dS_j} = \frac{f_j(0) dT_j}{f_j(0) dS_j} + \frac{T_j \cdot dT_j - f_j(Y_1,...,Y_r)}{|T_j - 0_1,...,r_\epsilon|}. \frac{B \cdot dT_j}{f_j(0) dS_j}.
\end{equation}

Thus we have $(I/I^2)[\epsilon] \cong B/(f_j(0))$. This shows that $B(\Omega_{A/B} \otimes_B A^{ncm}) = \prod f_j(0)$ which is non-zero as $A$ is reduced and free of finite rank over $B$ (and $A \neq A^{ncm}$ by our non-triviality assumption).

In particular, $f_j(0) \neq 0$, and the principal ideal $(f_j(Y)) \subset B[[Y_1,...,Y_r]]$ is prime to $Y_1$, and hence $\{f_j, Y_1,...,Y_r\}$ is a regular sequence in $A^G = B[[Y_1,...,Y_r]]$. Since $Y_j = (T_j)^2$, we also conclude that $\{f_j, T_{i_1},...,T_{i_r}\}$ is a regular sequence in $A$.\hfill \Box
We now prove the general case. Pick \( \varepsilon \not= 1 \), and recall \( a'_\varepsilon := (\sum_{j:\varepsilon(b_j) = -1} f_j A + \sum_{k:\varepsilon(b_k) = 1} T_k^- f_k A) \) and \( \mathcal{D}_\varepsilon := \sum_{j:\varepsilon(b_j) = -1} f_j A + \sum_{k:\varepsilon(b_k) = 1} T_k^- A \). Then \( G \) acts on \( A' = A/a'_\varepsilon \) faithfully. Since \( A' \) is a \( B \)-module of finite type, \( \Omega_{A'/B} \) is a \( B \)-torsion module of finite type. We have the following exact sequence

\[
0 \rightarrow a'_\varepsilon / a'^2 \rightarrow A' \cdot df_j / dT^- \rightarrow A' \cdot d(T^- f_k) \rightarrow A' \cdot d(T^-) \rightarrow \Omega_{A'/B} \rightarrow 0.
\]

Tensoring with \( B' := A/\mathcal{D}_\varepsilon \) and taking \( \varepsilon_i \)-eigenspace for \( i \) with \( \varepsilon(b_i) = 1 \),

\[
(a'_\varepsilon / a'^2)_{\varepsilon_i} = \frac{B' \cdot d(T^-)}{B' \cdot dS_i} = \frac{B' \cdot dT^-}{f_j dT^- + T_j df_j} = \frac{B' \cdot dT^-}{f_j dT^-}
\]

where \( \pi = (x \mod \mathcal{D}_\varepsilon) \). This is because \( T_j = 0 \). Since \( B' / f_j B' \) is \( B \)-torsion and \( B' \) is \( B \)-free of finite rank (by Lemma 7.5), the multiplication by \( f_j \) on \( B' \) is injective. Therefore \( \{f_j\}_{j: \varepsilon(b_j) = -1} \cup \{f_i\} \cup \{T_j\}_{\varepsilon(b_k) = 1} \) is a regular sequence of length \( r_+ - 1 \) in \( A \). This implies that \( \{f_j\}_{j: \varepsilon(b_j) = -1} \cup \{f_i\} \cup \{T_j\}_{\varepsilon(b_k) = 1} \) is a regular sequence of length \( r'_+ + 1 \) in \( A^G \).

\[ \square \]

Though we do not need the following result in the sequel, we just record it here:

**Corollary 7.7.** We have

\[ \text{Frac}(A^G) = \text{Frac}(A^G / \mathfrak{B}) = \bigoplus \text{Frac}(A^G / \mathfrak{B}_i) \quad \text{and} \quad \text{Frac}(A) = \text{Frac}(A / \mathfrak{A}) = \bigoplus \varepsilon \text{Frac}(A / \mathcal{D}_\varepsilon). \]

Again we prove the assertion only for \( \mathfrak{B} \).

**Proof.** Let \( P \) be a minimal prime ideal containing \( \mathfrak{B} \). Then as in the proof of Lemma 7.5, \( P \) determines \( \varepsilon \in G \) so that \( \varepsilon(b_k) = 1 \) if and only if \( y_k \in P \), and hence \( P \) contains \( \mathfrak{B}_i \). We first show that \( f_i \not\in P \) if \( \varepsilon(b_i) = 1 \). Indeed, if \( f_i \in P \), \( P \) contains \( \{f_j\}_{j: \varepsilon(b_j) = -1} \cup \{f_i\} \cup \{T_j\}_{\varepsilon(b_k) = 1} \), which is a regular sequence of length \( r_+ - 1 \) in \( A^G \). Thus \( P \) has height \( r_+ - 1 \) and hence cannot be a minimal prime containing \( \mathfrak{B} \) generated by a regular sequence of length \( r_+ \) (see [CRT, Theorem 17.6] and [BCM, IV.1.4.2]). Write \( \min(\mathfrak{a}) \) for the set of minimal primes containing an \( A^G \)-ideal \( \mathfrak{a} \). From this, for each minimal prime \( P \) of \( A^G \) containing \( \mathfrak{B} \), we have a unique \( \mathfrak{B}_i \), such that \( P \supseteq \mathfrak{B}_i \) for any other \( \mathfrak{a}' \not= \mathfrak{a} \). Since \( \text{Frac}(A^G / \mathfrak{B}) = \bigoplus_{P \in \min(\mathfrak{B})} \text{Frac}(A^G / P) \) and \( \text{Frac}(A^G / \mathfrak{B}_i) = \bigoplus_{P \in \min(\mathfrak{B}_i)} \text{Frac}(A^G / P) \), we conclude \( \text{Frac}(A^G / \mathfrak{B}) = \bigoplus \text{Frac}(A^G / \mathfrak{B}_i) \). \[ \square \]

By definition, we have \( A^\text{cm}[1] = A^G / \mathfrak{B}_1 \cong A / \mathcal{D}_1 = A^\text{cm} \cong B \). Write \( A^\text{ncm}[1] = A^\text{cm},[1] = (A^G / \mathfrak{B}_1)^\perp \) for the image of \( A^G \) in \( \bigoplus_{\varepsilon \not= 1} \text{Frac}(A^G / \mathfrak{B}_i) \). We have \( A^\text{ncm}[1] = T_+^\text{cm} \) or \( T_+^\text{ncm} \) according as \( B = A \) or \( B = W \). We want to compute the congruence module

\[ C_0 := A^\text{ncm}[1] \otimes_{A^G} A^\text{cm}[1] = (A^G / \mathfrak{B}_1)^\perp \otimes_{A^G} (A^G / \mathfrak{B}_1)^\perp \cong (A^G / \mathfrak{B}_1)^\perp \otimes_{A^G} B \]

and its relation to \( C_\varepsilon := (A^G / \mathfrak{B}_i) \otimes_{A^G} (A^G / \mathfrak{B}_1)^\perp \) for \( \varepsilon \not= 1 \). Here the identity at \((*)\) is because we identify \( A^\text{cm} \) and \( B \) by the \( B \)-algebra structure of \( A^\text{cm} \).

**Corollary 7.8.** Let the notation be as above. Then we have \( C_0 \cong B / \bigcap_{j=-1}^r (f_j(0)) \), \( C_{\varepsilon_1} \cong B / (f_j(0)) \) and \( C_{\varepsilon} = B / (f_j(0))_{j: \varepsilon(b_j) = -1} \), where \( (f_j(0))_{j: \varepsilon(b_j) = -1} \) is the \( B \)-ideal generated by \( f_j(0) \) for all \( j \) with \( \varepsilon(b_j) = -1 \). In particular \( \text{Spec}(C_{\varepsilon_1}) \) contains \( \text{Spec}(C_\varepsilon) \) as long as \( \varepsilon(b_j) = -1 \).

**Proof.** Recall \( \mathfrak{B}_i := \sum_{j: \varepsilon(b_j) = -1} f_j A^G + \sum_{i: \varepsilon(b_i) = 1} Y_i A^G \). Since

\[ \text{Spec}(C_{\varepsilon}) = \text{Spec}(A^G / \mathfrak{B}_1) \cap \text{Spec}(A^G / \mathfrak{B}_i) = \text{Spec}(A^G / \mathfrak{B}_1) \times_{\text{Spec}(A^G)} \text{Spec}(A^G / \mathfrak{B}_i), \]

we have \( C_{\varepsilon} = B / (f_j(0))_{j: \varepsilon(b_j) = -1} \) as \( \text{Spec}(C_{\varepsilon}) \) is the locus of \( Y_i = 0 \) for all \( i \) and \( f_j = 0 \) for \( j \) with \( \varepsilon(b_j) = -1 \). Since \( \mathfrak{B} = \bigcup \mathfrak{B}_i \) by Lemma 7.5, we have an inclusion \( A^G = A^G / \mathfrak{B} \hookrightarrow \bigcup \mathfrak{B}_i A^G / \mathfrak{B}_i \), which implies \( \text{Spec}(A^G) = \bigcup \text{Spec}(A^G / \mathfrak{B}_i) \) and \( \text{Spec}(A^\text{ncm}[1]) = \bigcup_{\varepsilon \not= 1} \text{Spec}(A^G / \mathfrak{B}_i) \). Thus we have \( \text{Spec}(C_0) = \bigcup_{\varepsilon \not= 1} \text{Spec}(C_{\varepsilon}) \) and

\[ \text{Spec}(C_0) = \text{Spec}((A^G / \mathfrak{B}_1)^\perp) \cap \text{Spec}(A^G / \mathfrak{B}_1) = \text{Spec}((A^G / \mathfrak{B}_1)^\perp) \times_{\text{Spec}(A^G)} \text{Spec}(A^G / \mathfrak{B}_1). \]
Thus \( \text{Spec}(C_z) \hookrightarrow \text{Spec}(C_0) \) is a closed immersion. On the other hand, \( C_{z_j} = B/(f_j(0)) \) and hence \( \text{Spec}(C_{z_j}) \) contains \( \text{Spec}(C_z) \) as long as \( \varepsilon(b_j) = -1 \). Thus we conclude \( C_0 = B/\bigcap_j(f_j(0)) \) as \( \text{Spec}(C_0) = \bigcup_j \text{Spec}(C_{z_j}) \). \\
\( \square \)

**Corollary 7.9.** If \( B = \Lambda \), then \( \Lambda/(f_i(0), f_j(0)) \) is a finite ring as long as \( i \neq j \).

**Proof.** We compute \( C_0 \) different way. Define \( \text{Spec}((A/I)^{\perp}) = \pi^{-1}(\text{Spec}((A^G/I^G)^{\perp})) \subset \text{Spec}(A) \) for the projection \( \pi : \text{Spec}(A) \to \text{Spec}(A^G) \). Then \( \text{Frac}(A) = \text{Frac}(A/I) \oplus \text{Frac}((A/I)^{\perp}) \). Since \( A^{cm} := A/I \cong A^G/I^G \) as \( I^G = (Y_1, \ldots, Y_n) \), the isomorphism \( \text{Spec}(A/I) \cong \text{Spec}(A^G/I^G) \) induced by \( \pi \) gives rise to \( C_0 \cong A/I \otimes_A (A/I)^{\perp} \) or equivalently \( \text{Spec}(C_0) \cong \text{Spec}(A/I) \times_{\text{Spec}(A)} \text{Spec}((A/I)^{\perp}) \).

We use this expression to compute \( C_0 \) differently.

Recall \( A^{nmc} = A/a \). Thus we have \( C_0 \cong A^{cm}/a \cong A^{cm} \otimes_A A^{nmc} \cong A^{nmc}/I = A^{nmc}[1]/I^G \).

By Corollary 7.8, we conclude \( C_0 \cong A^{cm}/a \cong \prod_{p \mid h_F} A^{cm} \). Different primes \( f_i(0) \) and \((f_j(0))\) are co-prime in \( \Lambda \) if \( i \neq j \), hence \( \Lambda/(f_i(0), f_j(0)) \) is finite. \\
\( \square \)

The following corollary conclude the proof of Theorem A:

**Corollary 7.10.** Assume (h0–4). Let the notation be as above. Then we have

\[
\Omega_{A/B} \otimes_A A^{cm} \cong \bigoplus_j B\Theta_j \cong \bigoplus_j B/(f_j(0)),
\]

and if \( B = \Lambda \), \( \Omega_{A/B} \otimes_A A^{cm} \) is pseudo isomorphic to \( \Lambda/\bigcap_{j=1}^n(f_j(0)) \).

**Proof.** From (7.4) combined with (7.2), we conclude that \( I/I^2 = \bigoplus_j B\Theta_j \cong \bigoplus_j B/(f_j(0)) \). Then by Corollary 7.9, \( f_j(0) \) are mutually prime each other if \( B = \Lambda \), and by Chinese reminder theorem, \( \Omega_{A/B} \otimes_A A^{cm} \cong I/I^2 \) is pseudo isomorphic to \( \Lambda/(\bigcap_{j=1}^n f_j(0)) \). \\
\( \square \)

8. CYCLICITY FOR A \( \mathbb{Z}_p \)-EXTENSION \( K/F \)

Let \( F_\infty \subset \mathbb{F}_{\mu_{p^\infty}} \) be the cyclotomic \( \mathbb{Z}_p \)-extension of \( F \). Then \( F_\infty := F_\infty^+F^- \) is the unique \( \mathbb{Z}_p^2 \)-extension of \( F \). Take a \( \mathbb{Z}_p \)-extension \( K/F \) inside \( F_\infty \); so, \( F_\infty/K \) is also a \( \mathbb{Z}_p \)-extension.

Let

\[
L_\infty/F_\infty(F(\phi)), \ L_\infty^+/F_\infty^+(F(\phi)), \ L_\infty^-/F_\infty^-(F(\phi)), \ L_\infty^K/K(F(\phi))
\]

be the maximal \( p \)-abelian extension unramified outside \( p \). Define

\[
Y = \text{Gal}(L_\infty/F_\infty(F(\phi))), \ Y_\pm = \text{Gal}(L_\infty^+/F_\infty^+(F(\phi))), \ Y_K = \text{Gal}(L_\infty^K/K(F(\phi))).
\]

Via canonical splitting

\[
\text{Gal}(F_\infty F(\phi)/F) = \Gamma_F \times \text{Im}(\phi),
\]

\[
\text{Gal}(F_\infty^{\pm} F(\phi)/F) = \Gamma_\pm \times \text{Im}(\phi) \text{ and } \text{Gal}(K F(\phi)/F) = \Gamma_K \times \text{Im}(\phi)
\]

for \( \Gamma_\pm = \text{Gal}(F_\infty^{\pm}/F) \) and \( \Gamma_K = \text{Gal}(K/F) \), we define

\[
Y(\phi) = Y \otimes_{\mathbb{Z}_p, \text{Im}(\phi), \phi} W, \ Y_\pm(\phi) = Y \otimes_{\mathbb{Z}_p, \text{Im}(\phi), \phi} W, \ Y_K(\phi) = Y_K \otimes_{\mathbb{Z}_p, \text{Im}(\phi), \phi} W.
\]

Write \( \mathbb{H}/F \) for the Hilbert class field over \( F \), and put \( \mathbb{H}(\phi) = \mathbb{H}/F(\phi) \) (the composite of \( \mathbb{H} \) and \( F(\phi) \)). Let \( L_\infty/F_\infty \mathbb{H}(\phi) \) (resp. \( L_\infty^+/F_\infty^+ \mathbb{H}(\phi), L_\infty^-/F_\infty^- \mathbb{H}(\phi), L_\infty^K/K \mathbb{H}(\phi) \)) be the maximal \( p \)-abelian extension unramified outside \( p \). Put

\[
Y = \text{Gal}(L_\infty/F_\infty \mathbb{H}(\phi)), \ Y_\pm = \text{Gal}(L_\infty^+/F_\infty^+ \mathbb{H}(\phi)), \ Y_K = \text{Gal}(L_\infty^K/K \mathbb{H}(\phi)).
\]
Lemma 8.1. Assume $p 
parallel h_F$. Lifting the character $\varphi^-$ to $\text{Gal}(\mathbb{H}(\varphi^-)/F)$ for the composite $\mathbb{H}(\varphi^-) = \mathbb{H} F(\varphi^-)$, we have

$$Y^-(\varphi^-) \cong Y^- \otimes_{\mathbb{Z}_p[\text{Gal}(\mathbb{H}(\varphi^-)/F)]} W, \quad Y(\varphi^-) \cong Y \otimes_{\mathbb{Z}_p[\text{Gal}(\mathbb{H}(\varphi^-)/F)]} W$$

and

$$Y(\varphi^-) \cong Y \otimes_{\mathbb{Z}_p[\text{Gal}(\mathbb{H}(\varphi^-)/F)]} W, \quad Y_K(\varphi^-) \cong Y_K \otimes_{\mathbb{Z}_p[\text{Gal}(\mathbb{H}(\varphi^-)/F)]} W.$$

Proof. This follows from that fact that $\mathbb{H}(\varphi^-)$ is linearly disjoint from $L_\infty$ over $F(\varphi^-)$, since $[\mathbb{H}(\varphi^-) : F]$ is prime to $p$ by (h0) and $p \nmid h_F$. Indeed, as $[\mathbb{H}(\varphi^-) : F(\varphi^-)]$ is prime to $p$, we have $\text{Gal}(L_\infty/F(\varphi^-)) = \text{Gal}(\mathbb{H}(\varphi^-)/F(\varphi^-)) \rtimes \text{Gal}(L_\infty/\mathbb{H}(\varphi^-))$, and hence $L_\infty = L_\infty^{\text{Gal}(\mathbb{H}(\varphi^-)/F(\varphi^-))}$, which implies the identity

$$Y(\varphi^-) \cong Y \otimes_{\mathbb{Z}_p[\text{Gal}(\mathbb{H}(\varphi^-)/F)]} W.$$

Replacing $(\mathcal{L}_\infty, L_\infty)$ by $(\mathcal{L}_\infty^K, L_\infty^K)$, respectively, we get

$$Y_K(\varphi^-) \cong Y_K \otimes_{\mathbb{Z}_p[\text{Gal}(\mathbb{H}(\varphi^-)/F)]} W$$

by the same argument. This implies the other two identities (as the first and the third is special cases of the identity for $K$ taking $K := F_\infty^p$).

Let $a_\pm = \text{Ker}(W[[T_F]] \rightarrow W[[\Gamma_\pm]])$ and $a_K = \text{Ker}(W[[T_F]] \rightarrow W[[\Gamma_K]])$. Then we have a natural $W[[T_F]]$-linear maps

$$\pi_+: Y/a_+Y \rightarrow Y^+, \quad \pi_K: Y/a_KY \rightarrow Y_K$$

and

$$\pi_-: Y/a_-Y \rightarrow Y^-.$$

If either $F_\infty/K$ is unramified outside $p$ ($\iff p$ fully ramifies in $K/F$) or $\varphi^- \neq 1$, by Rubin [Ru91, Theorem 5.3 (i)-(ii)], we have $\text{Ker}(\pi_K) = \text{Ker}(\pi_\pm) = 0$ and $\text{Coker}(\pi_\pm) \cong \mathbb{Z}_p \cong \text{Coker}(\pi_K)$. Thus we get

Theorem 8.2. Suppose $p \nmid h_F$ and $\varphi^- \neq 1$. Let $K/F$ be a $\mathbb{Z}_p$-extension. Then $\pi_\pm$ and $\pi_K$ are all surjective. If either $F_\infty/K$ is unramified outside $p$ or $\varphi^-$ is non-trivial on $\text{Gal}(\mathbb{H}_p/\mathbb{Q}_p)$, we have

$$Y(\varphi^-)/a_-Y(\varphi^-) \cong Y^-(\varphi^-)$$

and

$$Y(\varphi^-)/a_KY(\varphi^-) \cong Y_K(\varphi^-)$$

as $W[[T_F]]$-modules.

Proof. Under the assumption of the theorem, by Rubin [Ru91, Theorem 5.3 (i)-(ii)], the corresponding assertions hold between $Y(\varphi^-)$ and $Y_K(\varphi^-)$. This is equivalent to the assertion of the theorem by Lemma 8.1.

Corollary 8.3. Assume $p \nmid h_F$ and (h0–4). If either $F_\infty/K$ is unramified outside $p$ or $\varphi^-$ is non-trivial on $\text{Gal}(\mathbb{H}_p/\mathbb{Q}_p)$, then cyclicity for $Y_K(\varphi^-)$ over $W[[\Gamma_K]]$, cyclicity of $Y^-(\varphi^-)$ over $W[[\Gamma_-]]$ and cyclicity of $Y(\varphi^-)$ over $W[[T_F]]$ are all equivalent. If $\varphi^- \neq 1$, then cyclicity of $Y(\varphi^-)$ over $W[[T_F]]$ implies cyclicity $Y_K(\varphi^-)$ of $W[[\Gamma_K]]$.

Proof. By Nakayama’s lemma applied to $W[[T_F]]$, as long as $Y(\varphi^-)/a_KY(\varphi^-) \cong Y_K(\varphi^-)$, cyclicity of $Y(\varphi^-)$ over $W[[T_F]]$ is equivalent to that of $Y_K(\varphi^-)$. This holds in particular for $K = F_\infty$ as $F_\infty/F_\infty^p$ is unramified everywhere. Then the first assertion follows from the above theorem.

If $Y(\varphi^-)$ is cyclic over $W[[T_F]]$, cyclicity $Y_K(\varphi^-)$ over $W[[\Gamma_K]] = W[[T_F]]/a_K$ follows from the surjectivity the projection: $Y(\varphi^-)/a_KY(\varphi^-) \rightarrow Y_K(\varphi^-)$. Thus again the second assertion follows from the above theorem.

9. Degree of CM components over the Iwasawa algebra

We continue to assume that $F$ is imaginary. Let $\text{Spec}(\mathbb{T})$ be the connected component containing a CM component coming from $F$. As seen in [H15, Section 5] (and Corollary 2.5), under (h0–4), any CM component of $\text{Spec}(\mathbb{T})$ is contained in $\text{Spec}(W[[H]])$ (and $T = W[[H]] \leftrightarrow L_p \in W[[H]]^\times$).

Since $\iota : Z \cong H$ by (1.6), $H$ canonically contains $\iota(\Gamma)$ for $\Gamma = 1 + p\mathbb{Z}_p$ embedded into $O_p^\times$. We identify $\Gamma$ and $\iota(\Gamma) \subset H$. Thus decomposing $H = \Gamma_+ \times \Delta$ for the torsion-free subgroup $\Gamma_+ \supset \Gamma$ and a finite group $\Delta$, each irreducible CM component is isomorphic to $\text{Spec}(W[[\Gamma_-]])$. Since $\Gamma_- \cong \mathbb{Z}_p$, we find that $\dim_k \text{Frac}(W[[\Gamma_-]]) = [\Gamma_- : \Gamma] = p^m$ for some $m \geq 0$. Recall $C := \text{Gal}(F_p/F)$ for the maximal $p$-abelian extension $F_p/F$ of conductor dividing $cp$. Since the image $\Gamma_-/\Gamma \hookrightarrow C$ and $C \hookrightarrow \text{Cl}_F$ (under (h0)) for the class group $\text{Cl}_F$ of $F$, if $h_F = p^k \eta$ ($h, \eta \in \mathbb{Z}$) with $p \nmid \eta$ for the class
number $h_F = |C_F|$, we have $0 \leq m \leq h$. If we find an $O$-ideal $a$ prime to $p$ such that $\alpha_p^n = (\alpha)$ with $\alpha \in O$ (for $0 \leq n \leq h$) with $\alpha_p^{n-1} \neq 1 \mod p^2$, we find that $m \geq n$. Thus we get

**Proposition 9.1.** Let the notation be as above. Assume $(h_0 \cdot 4)$. For a CM component $I$ of $h$, we have $\dim \text{Frac}(I) = p^m$ with $0 \leq m \leq h$. If we find an $O$-ideal $a$ prime to $p$ such that $\alpha_p^{n-1} = (\alpha)$ with $\alpha \in O$ (for $0 \leq n \leq h$) with $\alpha_p^{n-1} \neq 1 \mod p^2$, we find that $m \geq n$.

By the last assertion of the above proposition, we can easily create many examples of CM components with $\text{Frac}(I) \not\subseteq \mathbb{K}$. An interesting point is that the dimension $\dim \text{Frac}(I)$ is a $p$-power, while non CM component we studied earlier often satisfies $\dim \text{Frac}(I) = 2$. As shown in [KhR15], there are also examples of non CM component with arbitrary large degree over $\Lambda$.

Take an irreducible component $\text{Spec}(I)$ of $\text{Spec}(\mathbb{T})$, and write its complementary (reduced) component as $\text{Spec}(I^\perp)$. Thus we have $\text{Spec}(\mathbb{T}) = \text{Spec}(I) \cup \text{Spec}(I^\perp)$, and $\text{Spec}(I \otimes \mathbb{T}^\perp) = \text{Spec}(I) \cap \text{Spec}(I^\perp)$ has codimension $\geq 1$ in $\text{Spec}(\mathbb{T})$. Suppose that $I$ is Gorenstein. This is true for CM components as it is isomorphic to the regular ring $W[[\Gamma_\alpha]]$. If $\mathbb{T}^\text{ncm}$ is non-trivial and integral, $I = \mathbb{T}^\text{ncm}$ is Gorenstein (as we proved that $\mathbb{T}^\text{ncm}$ is Gorenstein in Theorem 5.4 (1)); so, again this property is satisfied for many non CM components. Then as indicated in [EAI, Section 3.1, page 88], $I \otimes \mathbb{T}^\perp = I/(L_p(\text{Ad}(p_0)))$ for a $p$-adic $L$-function $L_p(\text{Ad}(p_0)) \in I$ interpolating $L(1, \text{Ad}(p_0))$ divided the canonical period for $P$ running through arithmetic points of $\text{Spec}(I)(\overline{\mathbb{Q}}_p)$.

Suppose that $I$ is a CM component. Since $\Omega_p[I/H]/\Lambda$ is a $p$-torsion module, we expect to have $pL_p(\text{Ad}(p_0))$ if $H \neq \Gamma_\alpha$ (see [MFG, §5.3.4]). The decomposition $\text{Ad}(\text{Ind}_F^\mathbb{T} \phi) \cong \chi \otimes \text{Ind}_F^\mathbb{T} \phi$ for $\varphi^{-1} = \varphi(\tau)\varphi(\tau/c-1)$ for a complex conjugation, we have $L_p(\text{Ad}(p_0)) = h_F \cdot L_p(I)$ for the projection $L_p(I)$ of the Katz $p$-adic $L$-function $L_p$ under $W[[H]] \to I$ (see [H15, Section 5]). Thus we get $h_F \cdot L_p(\text{Ad}(p_0)) \in I$. This gives a plenty of examples of positivity of the $\mu$-invariant of $L_p(\text{Ad}(p_0))$. One can then ask if the $\mu$-invariant of $L_p(\text{Ad}(p_0))$ vanishes for non CM components $I$. One can produce some non CM component with $L_p(\text{Ad}(p_0))$ having positive $\mu$ if $p = 2$. Thus for this question to be affirmative, we need to assume $p > 2$.

**10. Divisibility of the adjoint $p$-adic $L$-function**

We continue to assume that $F$ is imaginary. Recall our assumption $p \geq 5$. Picking an irreducible component $\text{Spec}(I)$ of $\text{Spec}(\mathbb{T})$ and writing $\overline{\mathbb{T}}$ for the normalization of $I$ (i.e., $\overline{\mathbb{T}}$ is the integral closure of $I$ in $\text{Frac}(I)$), we put $\mathbb{T} = \mathbb{T} \otimes \overline{\mathbb{T}}$. Write $\pi : \mathbb{T} \to I$ for the projection inducing the inclusion $\text{Spec}(I) \hookrightarrow \text{Spec}(\mathbb{T})$. Since $\text{Hom}_\Lambda(\mathbb{T}, \Lambda) \cong \mathbb{T}$, we have

$$\mathbb{T} \cong \text{Hom}_\Lambda(\mathbb{T}, \Lambda) \otimes \overline{\mathbb{T}} \cong \text{Hom}_\Lambda(\mathbb{T} \otimes \overline{\mathbb{T}}, \overline{\mathbb{T}}).$$

(10.1)

This follows from the fact that $\overline{\mathbb{T}}$ is $\Lambda$-free of finite rank (as any reflexive module of finite type over a regular local domain of dimension 2 is free; see [H88a, Lemma 3.1] and [H88b, (5,5.9)]). We fix the identification (10.1). Decompose $\text{Frac}(\mathbb{T}) = \text{Frac}(I) \oplus S$ as a $\mathbb{K}$-algebra direct sum, and define $I_\perp$ for the image of $\mathbb{T}$ in $S$, where $\lambda : \mathbb{T} \to \text{Frac}(I)$ is induced by the projection $\mathbb{T} = \mathbb{T} \otimes \overline{\mathbb{T}}$ given by $t \otimes \overline{t} = \pi(t)\overline{t} \in I$. Regarding $\lambda : \mathbb{T} \to I$, we take adjoint $\lambda^* : I \otimes \mathbb{T} \to \text{Hom}_\mathbb{K}(I, \mathbb{T}) \to \text{Hom}_\mathbb{K}(\mathbb{T}, \mathbb{T}) = \mathbb{T}$. Then define $L_p(\text{Ad}(p_0)) := \lambda \circ \lambda^* \in \text{Hom}_\mathbb{K}(I, \mathbb{T})$. As shown in [H86c, Lemma 1.6] (or [MFG, §5.3.3]), we have $G_0(\lambda, \overline{\mathbb{T}}) := I_\perp \otimes \overline{\mathbb{T}} \cong I/(L_p(\text{Ad}(p_0)))$ as $I$-modules. This $L_p(\text{Ad}(p_0))$ interpolates the adjoint $L$-values $L(1, \text{Ad}(p_0))/\Omega_{p}$ for arithmetic points $P$ for the canonical period $\Omega_{p}$ written as $U_{\infty}(f_\text{1})U_{\text{1}}(f_\text{1})$ in [H88b, Theorem 0.1] and coincides with the one introduced in the previous section if $I$ is Gorenstein (i.e., $L_p(\text{Ad}(p_0))$ is contained in $I$ if $I$ is Gorenstein).

In [H88b, Theorem 0.1], some restrictive assumptions [H88b, (0.8a,b,c)] are made. However, these assumptions are not necessary as long as $h$ is reduced (for example, $N$ is cube-free; see [H13, Section 1]). To see this, consider the jacobian variety $J_1(Np^r)$ of the modular curve $X_1(Np^r)$ over $\mathbb{Q}$. Then by the Albanese functoriality applied to the tower of modular curves:

$$\cdots \to X_1(Np^{r+1}) \to X_1(Np^r) \to \cdots \to X_1(Np),$$

we have the projective system of the ordinary parts of the $p$-adic Tate modules $\{T_pJ_1(Np^{r+1})\}_r$. Let $L := \lim_{\to} T_pJ_1(Np^{r+1})$. Then as shown in [H86b] (see also [H14, Sections 4–5]), $L$ is naturally an $h$-module and is also $\Lambda$-free of finite rank. As explained in [H13, Section 4] from the work of
Ohta (and an earlier work by the author [H86b]), we have the following canonical exact sequence of $h$-modules:

\[(10.2) \quad 0 \to h \to L \to h^{\nu} \to 0.\]

When [H88b] was written, this sequence is only known under the one of the three conditions [H88b, (0.8a,b,c)]. This is the only point we used to prove [H88b, Theorem 0.1]; so, the result is valid without assuming these conditions (i.e., [H88b, Conjecture 0.2] is now known to be true; see [H16, §5.5] for more details of this).

We want to prove

**Theorem 10.1.** Suppose $p \geq 5$, let $\text{Spec}(\overline{I})$ be an irreducible non CM component of $\text{Spec}(T)$ satisfying (h0–4), and write $\overline{I}$ be the normalization of $I$ in $\text{Frac}(I)$. Then, under the equivalent conditions of Theorem 5.4, we have

1. If $\text{Spec}(\overline{I})$ is a CM component of $\text{Spec}(T)$ and $\varphi$ ramifies at $p$, then the ideal $(L_p(\text{Ad}(\rho_I)))$ of $\overline{I}$ is generated by the $\varphi^-$-branch of the anticyclotomic Katz $p$-adic $L$-function times the $p$-part $h_F$ of the class number of $F$.

2. Suppose $p \nmid h_F$ and Conjecture 5.6. Then we have $\sqrt{L_p(\varphi^-)} \in \overline{I}$, $\text{rank}^p_{\Lambda} \overline{I} \geq 2$, the $p$-adic $L$-function $L_p(\text{Ad}(\rho_I))$ is a non-unit in $\overline{I}$, and $\sqrt{L_p(\varphi^-)}$ divides $(L_p(\text{Ad}(\rho_I)))$ in $\overline{I}$. If further $\text{rank}^p_{\Lambda} T_{\text{necm}} = 2$, then $\overline{I} = \Lambda[\sqrt{L_p(\varphi^-)}]$ and $(L_p(\text{Ad}(\rho_I))) = (\sqrt{L_p(\varphi^-)})$.

The example given in [H85, (10a,b)] shows the case (2) in the above theorem actually occurs, and indeed, in this case, $T = \Lambda[\sqrt{L_p}]$ and $(L_p)_{\Lambda}$ has a unique zero of multiplicity one in the unit disk $p\mathbb{Z}_p$.

**Proof.** The assertion (1) is a restatement of [H15, Proposition 7.10]. So we prove the other two assertions. We deal with (2). Write the composite map $\overline{T} = T \otimes_{\Lambda} \overline{I} \to I \otimes_\Lambda \overline{I} \to \overline{I}$ as $\lambda$, where the right most arrow is the multiplication ($a \otimes \overline{I} \mapsto ab$). Since $\overline{T} = T \otimes_{\Lambda} \overline{I}$ surjects down to $I \otimes_\Lambda \overline{I}$, we have $\text{Spec}(\overline{I}) \subset \text{Spec}(I \otimes_\Lambda \overline{I}) \subset \text{Spec}(T)$. Consider the congruence modules (see [MFG, §5.3.3] for congruence modules)

$$C_0(\lambda; \overline{I}) := \overline{I} \otimes_{\overline{T}, \lambda} \overline{I} \quad \text{and} \quad C_0(m; \overline{I}) = \theta \otimes_{\overline{T}, m} \overline{I}$$

for $\theta$ given by $\text{Spec}(\vartheta') = \text{Spec}(I \otimes_\Lambda \overline{I})$ (i.e., $\text{Spec}(\vartheta')$ is the complementary component of $\text{Spec}(\overline{I})$ in $\text{Spec}(I \otimes_\Lambda \overline{I})$). Note that $C_0(\lambda; \overline{I}) = \overline{I} \otimes_T \overline{I} \cong \overline{I}/(L_p(\text{Ad}(\rho_I)))$ by definition. Thus we have the surjective $I$-linear map $C_0(\lambda; \overline{I}) = \overline{I}/(L_p(\text{Ad}(\rho_I))) \to C_0(m; \overline{I})$ as $\text{Spec}(\vartheta') \cap \text{Spec}(\overline{I}) \subset \text{Spec}(\vartheta') \cap \text{Spec}(\overline{I})$.

Note that the projection: $T \to I$ factors through $T_{\text{necm}}$. Write $\lambda'$ for the composite $T_{\text{necm}} \otimes_{\overline{I}} \overline{I} \to \overline{I}$ and define an $I$-ideal $a$ by $C_0(\lambda'; \overline{I}) = \overline{I}/a$. By Theorem 5.4 (2), $T_{\text{necm}} = T_{\text{necm}} \oplus T_{\text{necm}} \theta'$ with $\theta^2 \in T_{\text{necm}}$, and by (5.2), $\overline{I}/a = W[[H]]/(L_p)$ with $(L_p(\text{Ad}(\rho_I))) = (h_F L_p(\varphi^-)) = (L_p(\varphi^-))$ as $p \nmid h_F$. By projecting $\theta$ down to $d \in I$, we find $(d^2) \cap \Lambda = (L_p(\varphi^-))$; so, $\sqrt{L_p(\varphi^-)} \in I$ (no need to extend $W$ as $W \supset W(\overline{F}_p)$). Since divisibility just follows from localization, we may localize at height one primes $P||L_p(\varphi^-)$ of $\Lambda$. Thus $\overline{I}/p$ is a semi-local normal ring finite flat over the valuation ring $\Lambda_p$. Therefore, it is a regular ring (in particular, it is complete intersection); so, writing $C_0(m; \overline{I}) = \overline{I}/p$ and $\partial_p$ is the different of $\overline{I}/\Lambda_p$ (cf. [MFG, Lemma 5.21]). Since $\overline{I}/p \supset \Lambda_p[\sqrt{L_p(\varphi^-)}]$, its different $(\sqrt{L_p(\varphi^-)})$ is a factor of the different $\partial_p$ of $I_p/\Lambda_p$, which is in turn a factor of $(L_p(\varphi^-))$ (as $C_0(\lambda'; \overline{I})$ surjects down to $C_0(m; \overline{I})$).

If further $T_{\text{necm}} = I$ and $\text{rank}^p_{\Lambda} T_{\text{necm}} = 2$, then $\overline{I} = \Lambda[\sqrt{L_p(\varphi^-)}]$, and by the semi-simplicity conjecture, $\overline{I}$ is integrally closed; so, $\overline{I} = I$. Then, from $W[[H]]/(L_p(\varphi^-)) \cong I/(\sqrt{L_p(\varphi^-)})$, we find that

$$T = \{(x, y) \in W[[H]] \oplus I : x \mod (L_p(\varphi^-))W[[H]] = y \mod \sqrt{L_p(\varphi^-)}I\},$$

where on the right-hand-side, we regard $L_p(\varphi^-) \in \Lambda \subset I$. From this, we can easily compute $C_0(\lambda; I) = I/(\sqrt{L_p(\varphi^-)}) = I/(L_p(\text{Ad}(\rho_I)))$, which finishes the proof. □
11. Dualizing modules

We describe purely ring theoretic results we have used in the paper. The theory of dualizing modules is initiated by Grothendieck [SGA 2.IV–V] and is developed by Hartshorne [RDD] and Kleiman [Kl80]. Let $S$ be a base local ring. For any $S$-module $M$, we define $M^! := \text{Hom}_S(M, S)$.

**Lemma 11.1.** Let $S$ be a $p$-profinite Gorenstein local ring and $A$ be a local $S$-algebra. Suppose that $A$ is a local Cohen–Macaulay ring with $\dim A = \dim S$. If $A$ is an $S$-module of finite type, the following conditions are equivalent:

1. The local ring $A$ is Gorenstein;
2. $A^! \cong A$ as $A$-modules.

**Proof.** Since $S$ is Gorenstein, it has canonical module $\omega_S \cong S$ (as $S$-modules; see [CMA, §21.3]). Then by [CMA, Theorem 21.15], $A$ itself has its dualizing module $\omega_A$ given by $\text{Hom}_S(A, \omega_S)$. By [CMA, §21.3], a local ring $R$ is Gorenstein if and only if $\omega_R \cong R$ as $R$-modules for the dualizing module $\omega_R$ of $R$. Since $\omega_S \cong S$, we find $\omega_A \cong A^!$, and hence $A$ is Gorenstein if and only if $A^! \cong A$.

Let $A$ be a Gorenstein local $S$-algebra for a Gorenstein local ring $S$. Suppose that $A$ is reduced and free of finite rank over $S$ and $S$ is $W$-free of finite rank. Let $\sigma \in \text{Aut}(A)$ be an $S$-algebra involution. We allow the case where $\sigma$ acts non-trivially on $S$. Put $A_{\pm} := \{ x \in A | \sigma(x) = \pm x \}$. Then by Lemma 11.1, we get $A^! \cong A$ as $A$-modules. Since $\sigma$ acts by duality on $A^!$, we have $A_{\pm}^! = (A^!)_{\mp} := \{ x \in A^! | \sigma(x) = \pm x \}$. Note that $A^!_{\pm} \cong \text{Hom}_S(A_{\pm}, S)$. Thus $\sigma$ acts on $\text{Hom}_A(A^!, A)$ and $\text{Isom}_A(A^!, A)$ just by $\phi \mapsto \phi^\sigma := \sigma \circ \phi \circ \sigma$. Indeed, by a computation: $\phi^\sigma(ax) = \sigma(\phi(\sigma(ax))) = \sigma(\sigma(a)\phi(\sigma(x))) = a\sigma(\phi(\sigma(x))) = a\phi^\sigma(x)$ for $a \in A$, we conclude $\phi^\sigma$ is $A$-linear. We then consider the $\pm$-eigenspace $\text{Hom}_A(A^!, A)^{\pm}$ for $a \in A$ and $\text{Isom}_A(A^!, A)^{\pm} := \text{Hom}_A(A^!, A)^{\pm} \cap \text{Isom}_A(A^!, A)$. Here $\text{Isom}_A \subset \text{Hom}_A$ is made up of $A$-linear isomorphisms. The set $\text{Isom}_A(A^!, A)^{\pm}$ could be empty.

If $\sigma$ fixes $S$ point by point, we have $(A^!)_\pm = (A_{\pm})^!$, which we just write $A_{\pm}^!$.

**Lemma 11.2.** Let $A$ be a noetherian Gorenstein local $S$-algebra for a $p$-profinite Gorenstein local ring $S$ (for a prime $p > 2$). Suppose that $A$ is reduced and free of finite rank over $S$. Let $\sigma \in \text{Aut}_S(A)$ be an algebra involution fixing $S$ point by point.

1. At least for one sign $\varepsilon = \pm$, the set $\text{Isom}_A(A^!, A)^\varepsilon$ is non-empty.
2. If either ranks $A_{+} > \text{rank}_S A_{-}$ or $\text{Isom}_A(A^!, A)^+ \neq \emptyset$, we have $A_{+} \cong (A_{+})^!$ (i.e., $A_{+}$ is Gorenstein). Moreover we have $\text{Isom}_A(A^!, A)^{-} = \emptyset$ if $\text{rank}_S A_{+} > \text{rank}_S A_{-}$.
3. If $\text{rank}_S A_{+} = \text{rank}_S A_{-}$ and $\text{Isom}_A(A^!, A)^{+} \neq \emptyset$, we have $A_{+} \cong A_{+}[c]$.
4. Suppose that $S$ is a domain. Then we have $\text{rank}_S A_{+} \geq \text{rank}_S A_{-}$.

**Proof.** Since $A$ is Gorenstein, we have $A^! \cong A$ as $A$-modules by Lemma 11.1. Thus we conclude $\text{Isom}_A(A^!, A) \neq \emptyset$. Pick $\phi \in \text{Isom}_A(A^!, A)$. Let $\phi^\pm = \phi \pm \phi^\sigma$. Then for $a \in A$, we have

$$\phi^\pm(ax) = \phi(ax) \pm \sigma(\phi(\sigma(ax))) = a\phi(x) \pm \sigma(\phi(\sigma(x))) = a\phi(x) \mp a\sigma(\phi(\sigma(x))) = a\phi^\pm(x).$$

Then $\phi^+ - \phi^- = 2\phi$. If $\phi^\varepsilon$ or $\phi^\varepsilon$ is not onto, we conclude $\text{Im}(\phi^\varepsilon) \subset A$ is a proper $A$-submodule of $A$; so, $\text{Im}(\phi^\varepsilon) \subset m_A$. This shows $\phi^\varepsilon = 2\phi - \phi^\sigma \equiv 2\phi \mod m_A$, which implies $\phi^\varepsilon$ is onto (as $p > 2$). Identifying $A^!$ with $A$, we can iterate $\Phi := \phi^{-\varepsilon}$, and $\text{Ker}(\Phi^n)$ is an ascending sequence of $A$-ideals. Since $A$ is noetherian, for some $n > 0$, we have $\text{Ker}(\Phi^n) = \text{Ker}(\Phi^{n+1})$. Thus we conclude $\Phi : A = \text{Im}(\Phi^n) = A/\text{Ker}(\Phi^n) \xrightarrow{\Phi} A/\text{Ker}(\Phi^{n+1}) = \text{Im}(\Phi^{n+1}) = A$ and hence $\phi^{-\varepsilon}$ is an isomorphism.

If $\text{rank}_S A_{+} > \text{rank}_S A_{-}$, by $A_+$-indecomposability of $A_+$ as $A_-$-modules, the Krull-Schmidt theorem tells us $A_+^! \cong A_+$ and hence $A_+^! \cong A_-$. Moreover the decomposition $A = A_+ \oplus A_-$ is a unique decomposition of the $A_+$-module $A$ into the sum of the indecomposable $A_+$ of the largest $S$-rank and an $A_-$-submodule $A_-$ of less $S$-rank. Therefore, any $\phi \in \text{Isom}_A(A^!, A)$ is forced to preserve $A_+$ and $A_-$; so, we have $\text{Isom}_A(A^!, A)^+ = \emptyset$ and $\text{Isom}_A(A^!, A)^- = \emptyset$. Thus we get $A_+^! \cong A_+$ as $A_+$-modules (i.e., $A_+$ is Gorenstein).

Now suppose $\text{rank}_S A_{+} = \text{rank}_S A_{-}$ and $\text{Isom}_A(A^!, A)^+ \neq \emptyset$. Thus $A_{+} \cong (A_{+})^!$ as $A_+$-modules, and $\text{Isom}_A(A^!, A)^+ \neq \emptyset$ implies $A_{+}^! \cong A_+$ as $A_+$-modules (i.e., $A$ is Gorenstein). Similarly $\text{Isom}_A(A^!, A)^- = \emptyset$ implies $\text{Isom}_A(A^!, A)^- \neq \emptyset$ by (1), and $A_{-}^! \cong A_-$ as $A_-$-modules.
Since Frac(A) is a product of fields, for each simple component K of Frac(A), either σ acts non-trivially or σ fixes K element by element. Since $A_\pm$ is a direct summand of the S-free module A of finite rank, $A_\pm$ is S-free of finite rank as S is a local ring. Thus we get

$$\text{rank}_S A_+ = \dim_{\text{Frac}(S)} A_+ \otimes_S \text{Frac}(S) \geq \dim_{\text{Frac}(S)} A_- \otimes_S \text{Frac}(S) = \text{rank}_S A_-,$$

proving (4).

We now study relative dualizing modules and show that a Gorenstein local domain quadratic over a Gorenstein subalgebra is generated by a single element over the subalgebra. Let B be a commutative p-profinite local ring for a prime $p > 2$. Consider a local B-algebra A finite over B with $B \hookrightarrow A$. Write $\omega_{A/B}$ for the dualizing module for the finite (hence proper) morphism $X := \text{Spec}(A) \xrightarrow{f} \text{Spec}(B) := Y$ if it exists (in the sense of [Kl80, (6)]). For the dualizing functor $f^!$ from quasi coherent Y-sheaves into quasi coherent X-sheaves defined in [Kl80, (2)], we have $\text{Hom}_A(F, f^!N) = \text{Hom}_B(f_*F, N)$ for any quasi-coherent sheaves F over X and N over Y; so, if $\omega_{A/B}$ exists (i.e., $f^!(N) = N \otimes_B \omega_{A/B}$), taking $F = A$ and $N = B$, we have $\omega_{A/B} = f^!(O_Y) = \text{Hom}_B(A, B)$ as $A$-modules. As shown in [Kl80, (21)], Spec(A) $\xrightarrow{f} \text{Spec}(B)$ has dualizing module if and only if f is Cohen Macaulay (e.g., if B is regular and A is free of finite rank over B). Even if we do not have dualizing module $\omega_{A/B}$, we just define $\omega_{A/B} := \text{Hom}_B(A, B)$ generally.

Suppose that we have an involution $\sigma \in \text{Aut}(A/B)$. Let $A_+ = A^\sigma$ for the order 2 subgroup $G$ of $\text{Aut}(A/B)$ generated by $\sigma$. Under the following four conditions:

1. $B$ is a regular local ring,
2. $A$ is free of finite rank over B,
3. $A$ and $A_+$ are Gorenstein rings,
4. $A/B$ is generically etale (i.e., Frac(A) is reduced separable over Frac(B)),

in [RDF, §3.5.a], the module of regular differentials $\omega_{\square/\triangle}$ for $(\square, \triangle) = (A, B), (A, A_+), (A_+, B)$ is defined as fractional ideals in $\text{Frac}(\square)$. By (1) and (2), $A/B$ and $A_+/B$ are Cohen Macaulay; so, $\omega_{A/B}$ and $\omega_{A_+/B}$ as above are the dualizing modules.

We now identify the dualizing module with more classical “inverse different” (realized as a fractional ideal). Let $C \supset B$ be reduced algebras. By abusing notation, write $\omega_{C/B} := \text{Hom}_B(C, B)$ in general. Suppose that $\text{Frac}(C)/\text{Frac}(B)$ is étale; so, we have a well defined trace map $\text{Tr} : \text{Frac}(C) \to \text{Frac}(B)$, and $\omega_{\text{Frac}(C)/\text{Frac}(B)} = \text{Frac}(C)\text{Tr}$ by the trace pairing $(x, y) \mapsto \text{Tr}(xy)$. We define an $C$-fractional ideal by

$$d_{C/B}^{-1} := \{ x \in C | \text{Tr}(xC) \subset B \}.$$

In other words, $\omega_{C/B} = \text{Hom}_B(C, B) \hookrightarrow \text{Hom}_{\text{Frac}(B)}(\text{Frac}(C), \text{Frac}(B)) = \text{Frac}(C)\text{Tr}$ has image $d_{C/B}^{-1}$; $\text{Tr}$. Thus we have $d_{C/B}^{-1} \cong \omega_{C/B}$. If $C = B[\delta]$ is free of rank 2 over B with an $B$-basis 1, $\delta$ with $\delta^2 \in B$, we have $d_{C/B}^{-1} = \delta^{-1}C$ for $\delta^{-1} \in \text{Frac}(C)$. Here is a version of Dedekind’s formula of transitivity of inverse differenten proven in [KDF, Proposition G.13] (see also [RDP, Theorem 8.6], [Kl80, (26) (vii)] and [Hu89]):

**Proposition 11.3.** Let B be a regular p-profinite local ring. Suppose that $D/C/B$ is generically étale finite extensions of reduced algebras such that D and C are B-flat, $\omega_{C/B} \cong B$ as B-modules (i.e., B is Gorenstein) and that Frac(D) is Frac(C)-free. Then we have $d_{D/C}^{-1} \cong \omega_{C/B}$ and $\omega_{D/C} \cong \omega_{C/B}$.

Let A be a reduced noetherian algebra with an involution $\sigma$. Put $A_\pm = A := \{ x \in A | \sigma(x) = \pm x \}$ and write $G$ for the subgroup of $\text{Aut}(A)$ of order 2 generated by $\sigma$; so, $A^+ = A^\sigma = H^0(G, A)$.

**Lemma 11.4.** Let S be a p-profinite Gorenstein integral domain for a prime $p > 2$ and A be a reduced local S-algebra free of finite rank over S. Suppose

1. $A$ and $A_+$ are Gorenstein,
2. $\text{Frac}(A)/\text{Frac}(A_+)$ is an étale extension,
3. $\text{Frac}(A)$ is free of rank 2 over $\text{Frac}(A_+)$,
4. $d_{A/A_+} \subset m_A$ or $A$ is flat over $A_+$ or $A_-$ is generated by one element over $A_+$.

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

**Proof:**
For $A_+$-module $M$, we write $M^*$ for the $A_+$-dual $\text{Hom}_{A_+}(M, A_+)$. 

**Proof.** From Lemma 11.1, we conclude $A^* \cong \omega_{A/A_+} \cong A$. Thus we conclude 

$$\omega_{A/A_+} \cong \mathcal{O}_{A/A_+}^{-1} = A^{-1}$$

with a non-zero divisor $\theta \in A$. Similarly $\mathcal{O}_{A_+/S}^{-1} = A_+^{-1}/S$ and $\mathcal{O}_{A_+/S} = \theta_{A_+/S}^{-1}A_+$. We may assume that $\theta_{A_+/S} = \theta_{A/S}$ by Proposition 11.3. Define $[x, y] := \text{Tr}_{A_+/A}(\theta^{-1}xy)$, which induces the self $A_+$-duality on $A$. If $\theta \in A_+$, we have $\text{Tr}_{A_+/A}(\theta^{-1}xy) = \theta^{-1}\text{Tr}_{A_+/A}(xy)$; so, 

$$A_+ = [A, A] = \text{Tr}_{A_+/A}(\theta^{-1}A) = \theta^{-1}\text{Tr}_{A_+/A}(A) = \theta^{-1}A_+.$$

Thus $\theta$ is a unit. The multiplication of $\theta$ gives rise to $\text{Isom}_A(A^*, A) \cong \text{Isom}_A(\mathcal{O}_{A/A_+}^{-1}, A)$.

Suppose $\mathcal{O}_{A/A_+} \subset m_A$. Then $\theta$ cannot be a unit. We conclude $\theta \notin A_+$; so, $\text{Isom}_A(A^*, A)^+ = \emptyset$. Thus by Lemma 11.2, $\text{Isom}_A(A^*, A)^- \neq \emptyset$. In other words, writing $f(x)$ for the minimal monic quadratic polynomial of $\theta$ in $A_+[x]$, we have $\mathcal{O}_{A/A_+} = A\delta$ with $\delta = f'(\theta) = \theta - \sigma(\theta)$ (i.e., the multiplication of $\delta$ gives rise to an element in $\text{Isom}_A(A^*, A)^-$. Indeed, by the trace pairing $[x, y] = \text{Tr}_{A_+/A}(xy)$, we have the identity $\mathcal{O}_{A/A_+} \cong A^* = A_+^* \oplus A^*$ and $A_+^* \cong A_+\delta^{-1}$ under this isomorphism. Thus flatness of $A$ over $A_+$, plainly by (3), $A_-$ is generated by a single element $\delta$. The assertion is plain in the case where $A_- = A_+\theta$. \hfill $\square$

**Remark 11.5.** By Corollary 7.9, we can show that the non-flat locus of $\text{Spec}(\mathbb{T}^\text{ncm})$ over $\text{Spec}(\mathbb{T}^\text{ncm})$ has codimension 2. For any height 1 prime $F$ of $A$, the localization $\mathbb{T}_{F}^\text{ncm}$ is therefore flat over $\mathbb{T}_{F_+}^\text{ncm}$. Thus by Lemma 11.4, we get $\mathbb{T}_{F}^\text{ncm} = \mathbb{T}_{F_+}^\text{ncm}(\delta_F)$ for $\delta_F \in \mathbb{T}_{F_+}^\text{ncm}$. This fact gives an alternative argument proving Theorem A.

**References**

**Books**


**Articles**


ANTICYCLOTOMIC CYCLICITY CONJECTURE


Department of Mathematics, UCLA, Los Angeles, CA 90095-1555, U.S.A.
E-mail address: hida@math.ucla.edu