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 of an induced representation of a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$. As an application, we prove cyclicity of the Iwasawa module with an anti-cyclotomic branch character over $\mathbb{Z}_p$-extensions of F under mild conditions.

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

Cyclotomic cyclicity conjecture: *Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the unique $\mathbb{Z}_p$-extension. Let $X_\pm$ be the Galois group of the maximal p-abelian extension everywhere unramified over $\mathbb{Q}(\mu_{p^\infty})$ on which complex conjugation acts by ± 1. For an odd character $\psi : \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}_\infty) \to \mu_{p-1}(\mathbb{Z}_p)$, define $X_-(\psi) := X_- \otimes_{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}_\infty)],\psi} \mathbb{Z}_p$ (the ψ-eigenspace of X). Then identifying $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \mathbb{Z}_p^\times = \mu_{p-1} \times \Gamma$ and regarding $X_-(\psi)$ as $\mathbb{Z}_p[[\Gamma]]$-module naturally, if $X_-(\psi) \neq 0$, $X_-(\psi)$ is pseudo isomorphic to $\mathbb{Z}_p[[\Gamma]]/(f_\psi)$ for a power series f_ψ prime to $p\mathbb{Z}_p[[\Gamma]]$.*

This conjecture asserts the cyclicity (up to finite error) of $X_-(\psi)$ as an Iwasawa module. Under the assumption that $X_+ = 0$ (the Kummer–Vandiever conjecture), Iwasawa proved (along with his main conjecture) pure cyclicity without finite pseudo-null error [CPI, No.48]. The fact $p \nmid f_\psi$ is a combination of the vanishing of the μ-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 results towards this conjecture via Galois deformation theory (e.g. [Ku93], [O03], [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–Vandiver conjecture (which sometimes fails) and a conjecture of Greenberg.

Let F be an imaginary quadratic field inside a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ with discriminant $-D$ and integer ring O. Assume that the prime (p) splits into $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in O with $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Let F_∞^-/F be the anti-cyclotomic $\mathbb{Z}_p$-extension with Galois group $\Gamma_- := \mathrm{Gal}(F_\infty^-/F)$; so, $c\sigma c = \sigma^{-1}$ for complex conjugation c and $\sigma \in \Gamma_- \cong \mathbb{Z}_p$. Fix a Witt vector ring $W = W(\mathbb{F})$ with finite residue field $\mathbb{F}$ of characteristic p, and take a branch character $\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to W^\times$. Regard it as a finite order idele character $\phi : F_\mathbb{A}^\times/F^\times \to W^\times$. Most of the time, we suppose that ϕ is anticyclotomic; so, $\phi(x^c) = \phi^{-1}(x)$. For an anticyclotomic ϕ, we always find a finite order character φ of $F_\mathbb{A}^\times/F^\times$ such that $\phi = \varphi^-$ for φ^- given by $\varphi^-(x) = \varphi(x)\varphi(x^c)^{-1}$ (e.g., [HMI, Lemma 5.31]). However, controlling the conductor of φ is a difficult task. Consider the anticyclotomic Iwasawa algebra $W[[\Gamma_-]] = \varprojlim_n W[\Gamma_-/\Gamma_-^{p^n}]$. Let $F(\phi)/F$ be the abelian extension cut out by ϕ (i.e., $F(\phi) = \overline{\mathbb{Q}}^{\mathrm{Ker}(\phi)}$). Let Y^- be the Galois group of the maximal p-abelian extension unramified outside $\mathfrak{p}$ over the composite $F_\infty^-(\phi) := F_\infty^- F(\phi)$. When we impose total $\mathfrak{p}^c$-splitting condition in addition to unramifiedness outside $\mathfrak{p}$, we add subscript/superscript "*sp*" (i.e., we write Y_{sp}^- instead Y^-), though often unramifiedness at $\mathfrak{p}^c$ implies splitting (see Proposition 7.1). Since $\mathrm{Gal}(F(\phi)/F)$ acts on Y^- naturally as a factor of $\mathrm{Gal}(F_\infty^-(\phi)/F)$, we have the ϕ-eigenspace $Y^-(\phi) = Y^- \otimes_{\mathbb{Z}_p[\mathrm{Gal}(F(\phi)/F)],\phi} \mathbb{Z}_p(\phi)$, where $\mathbb{Z}_p(\phi)$ is the W-free module of rank 1 on which $\mathrm{Gal}(F(\phi)/F)$ acts via ϕ.

Anticyclotomic cyclicity conjecture: *Assume $\phi \neq 1$ and that the conductor ϕ is a product of split primes over $\mathbb{Q}$. If the class number of F is prime to p and $Y^-(\phi) \neq 0$, then the $W[[\Gamma_-]]$-module $Y^-(\phi)$ is pseudo isomorphic to $W[[\Gamma_-]]/(f_\phi^-)$ as $W[[\Gamma_-]]$-modules for an element $f_\phi^- \in W[[\Gamma_-]]$ prime to $pW[[\Gamma_-]]$.*

We prove in this paper:

2010 *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 $\phi = \varphi^-$ for the Teichmüller lift φ of a modulo p Galois character $\overline{\varphi}$ of prime-to-p conductor $\mathfrak{c}$, and let $N = DN_{F/\mathbb{Q}}(\mathfrak{c})$. Suppose*

(h0) *$p > 3$ is prime to $N\prod_{l|N}(l-1)$ for prime factors l of N,*
(h1) *$\mathfrak{c}$ is prime to D, and $N_{F/\mathbb{Q}}(\mathfrak{c})$ is square-free (so, N is cube-free),*
(h2) *$\overline{\varphi} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathbb{F}^\times$ is unramified outside $\mathfrak{c}\mathfrak{p}$ with Teichmüller lift φ (so, writing $C(\det(\overline{\rho}))$ for the conductor of $\det(\overline{\rho})$ for $\overline{\rho} := \mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}$, we have $N|C(\det(\overline{\rho}))|Np$),*
(h3) *φ^- has at least order 3,*
(h4) *$\varphi^-(\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p))$ is not trivial,*

If the class numbers of F and $F(\varphi^-)$ are both prime to p, then the Iwasawa module $Y^-(\varphi^-)$ is isomorphic to $W[[\Gamma_-]]/(f_\phi^-)$ as $W[[\Gamma_-]]$-modules for an element $f_\phi^- \in W[[\Gamma_-]]$ prime to $pW[[\Gamma_-]]$.

The proof of this theorem is technical, ring theoretic tools applied to a local ring of the big Hecke algebra. To give an outline of our argument without going into technicality, let us state a theorem which describe ring-theoretic properties of the Hecke algebra equivalent to anti-cyclotomic cyclicity (i.e., without pseudo-null error) of $Y^-(\varphi^-)$. As a base ring of the Galois deformation theory, we take the Witt vector ring flat over the p-adic integer ring $\mathbb{Z}_p$. Here $\mathbb{C}_p$ is the p-adic completion of a fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ under its norm $|\cdot|_p$ normalized so that $|p|_p = \frac{1}{p}$. We identify the Iwasawa algebra $\Lambda = W[[\Gamma]]$ with the one variable power series ring $W[[T]]$ by $\Gamma \ni \gamma = (1+p) \mapsto t = 1+T \in \Lambda$. Take a Dirichlet character $\psi : (\mathbb{Z}/Np\mathbb{Z})^\times \to W^\times$, and consider the big ordinary Hecke algebra $\mathbf{h}$ (over Λ) of prime-to-p level N and the character ψ whose definition (including its CM components) will be recalled in the following section. We just mention here the following three facts

(1) $\mathbf{h}$ is an algebra flat over Λ interpolating p-ordinary Hecke algebras of level Np^{r+1}, of weight $k+1 \geq 2$ and of character $\epsilon\psi\omega^{-k}$ for the Teichmüller character ω, where $\epsilon : \mathbb{Z}_p^\times \to \mu_{p^r}$ ($r \geq 0$) and $k \geq 1$ vary. If N is cube-free, $\mathbf{h}$ is a reduced algebra [H13, Corollary 1.3];
(2) Each prime $P \in \mathrm{Spec}(\mathbf{h})$ has a unique (continuous) Galois representation $\rho_P : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\kappa(P))$ for the residue field $\kappa(P)$ of P;
(3) ρ_P restricted to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ (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 $\overline{\rho} = \rho_{\mathfrak{m}_\mathbb{T}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F})$ for the residue field $\mathbb{F} = \mathbb{T}/\mathfrak{m}_\mathbb{T}$. If $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}$ for the reduction $\overline{\varphi}$ modulo p of φ, we have an involution $\sigma \in \mathrm{Aut}(\mathbb{T}/\Lambda)$ such that $\sigma \circ \rho_P \cong \rho_P \otimes \chi$ for $\chi := \left(\frac{F/\mathbb{Q}}{}\right)$. For a subscheme $\mathrm{Spec}(A) \subset \mathrm{Spec}(\mathbb{T})$ stable under σ, we put $A_\pm := \{x \in A | \sigma(x) = \pm x\}$. Then $A_+ \subset A$ is a subring and A_- is an A_+-module.

Let Q be a finite set of rational primes in $F/\mathbb{Q}$ prime to Np. Let Q^+ be the subset of primes in Q split in F. Write K_Q for the ray class field over F of conductor $\mathfrak{C}p^\infty\prod_{q\in Q^+} q$ for $\mathfrak{C} := \mathfrak{c} \cap \mathfrak{c}^c$, and let K_Q^-/F (resp. $K_{\mathfrak{C}_Q}^-$) be the maximal p-abelian anticyclotomic sub-extension of K_Q/F (resp. the intersection of K_Q^- with the ray class field over F of conductor $\mathfrak{C}p\prod_{q\in Q^+} q$). Put $H_Q = \mathrm{Gal}(K_Q^-/F)$ and $C_Q = \mathrm{Gal}(K_{\mathfrak{C}_Q}^-/F)$. When Q is empty, we drop the subscript Q (so, $H = H_\emptyset$). Note here $H_Q = H_{Q^+}$ by definition. Moreover the fixed points $\mathrm{Spec}(\mathbb{T})^{\sigma=1}$ is known to be canonically isomorphic to $\mathrm{Spec}(W[[H]])$, and $Y^-(\varphi^-) \neq 0$ if and only if σ is non-trivial on $\mathbb{T}$ (and hence $\mathbb{T} \neq W[[H]]$; see Corollary 2.5). The ring $\mathbb{T}$ is reduced (if N is cube-free), and for the kernel $I = \mathbb{T}(\sigma-1)\mathbb{T} = \mathrm{Ker}(\mathbb{T} \twoheadrightarrow W[[H]])$, the I-span $X := I \cdot \mathrm{Frac}(\Lambda)$ in $\mathbb{T} \otimes_\Lambda \mathrm{Frac}(\Lambda)$ is a ring direct summand X complementary to $\mathrm{Frac}(W[[H]])$. We write $\mathbb{T}^{\mathrm{ncm}}$ for the image of $\mathbb{T}$ in the ring direct summand X (and call it the non-CM component of $\mathbb{T}$). Plainly $\mathbb{T}^{\mathrm{ncm}}$ is stable under σ.

Theorem B: *Let* $\mathrm{Spec}(\mathbb{T})$ *be a connected component of* $\mathrm{Spec}(\mathbf{h})$ *associated to the induced Galois representation $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}$ for the reduction $\overline{\varphi}$ modulo p of φ satisfying $(U(p) \mod \mathfrak{m}_\mathbb{T}) = \overline{\varphi}_{\overline{\mathfrak{p}}}(\mathrm{Frob}_p)$. 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 $\mathbb{T}^{\mathrm{ncm}}$ and $\mathbb{T}_+^{\mathrm{ncm}}$ are both local complete intersections free of finite rank over Λ.*
(2) *The ideal $I = \mathbb{T}(\sigma-1)\mathbb{T} \subset \mathbb{T}^{\mathrm{ncm}}$ is generated by a non-zero-divisor $\theta \in \mathbb{T}_-^{\mathrm{ncm}}$ with $\theta^2 \in \mathbb{T}_+^{\mathrm{ncm}}$ (i.e., θ generates a free $\mathbb{T}^{\mathrm{ncm}}$-module $\mathbb{T}_-$), and $\mathbb{T}^{\mathrm{ncm}} = \mathbb{T}_+^{\mathrm{ncm}}[\theta]$ is free of rank 2 over $\mathbb{T}_+^{\mathrm{ncm}}$.*
(3) *The Iwasawa module $Y^-(\varphi^-)$ is cyclic over $W[[\Gamma_-]]$.*
(4) *The Iwasawa module $Y^-(\varphi^-\omega)$ is cyclic over $W[[\Gamma_-]]$.*

Under these equivalent conditions, the ring $\mathbb{T}_+$ is a local complete intersection.

Write Cl_X for the class group of a number field X and put $h_X = |Cl_X|$ (the class number). The condition $p \nmid h_F h_{F(\varphi^-)}$ 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 may replace $Y^-(\varphi^-)$ in Theorem A by $Y^-_{sp}(\varphi^-)$, as $Y^-(\varphi^-) = Y^-_{sp}(\varphi^-)$; see Proposition 7.1).

We will prove the assertion (4) in Theorem B at the end of Section 6 and hence a slightly stronger version of Theorem A (Theorem 6.3) asserting cyclicity over $W[[H]]$ without assuming $p \nmid h_F$. Therefore if $p|h_F$, $Y^-(\phi)$ for $\phi = \varphi^-, \varphi^-\omega$ may not be cyclic over $W[[\Gamma_-]]$ unless $H = \Gamma_-$. The fact that f^-_ϕ in the conjecture is prime to $pW[[\Gamma_-]]$ follows from the vanishing of the μ-invariant of the anti-cyclotomic Katz p-adic L-function [H10] (and [EAI, Theorem 3.37]) and the proof of the main conjecture by Rubin [Ru88], [Ru91], 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). In Section 7, we extend the cyclicity to non-anticyclotomic $\mathbb{Z}_p$-extensions of F via Rubin's control theorem (see Corollary 7.4). 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 10). The Taylor–Wiles system is made of the deformation rings R_Q of $\overline{\rho}$ and the corresponding local rings $\mathbb{T}_Q$ of the Hecke algebras (of level $N_Q := N\prod_{q\in Q} q$) allowing ramification at primes in Q (for a suitably chosen infinite sequence of finite sets Q of primes q with $q \equiv 1 \mod p$; see Section 4 and [TW95]).

Here is a sketch of the proof of the equivalence of (2) ⇔ (3) in Theorem B. For any commutative ring A, we write Frac(A) for the total quotient ring of A (i.e., Frac(A) is the ring of fractions inverting all non-zero-divisors of A). We simply write $\mathbb{K}$ for Frac(Λ). As is well known, under (h1), Frac($\mathbb{T}$) can be decomposed as an algebra direct sum $\mathrm{Frac}(W[[H]]) \oplus X$ in a unique way. Write $\mathbb{T}^{\mathrm{ncm}}$ for the projected image of $\mathbb{T}$ in X. Then we have $I \hookrightarrow \mathbb{T}^{\mathrm{ncm}}$, and via the deformation theoretic technique of Mazur–Tilouine [MT90] (see also [H16, §6.3.6]), we show that $Y^-(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W$ is isomorphic to I/I^2 (by an old formula in [H86c, Lemma 1.1]). Assume that the class number h_F of F is prime to p. Then the projection of H to Γ_- 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 φ^- giving the characteristic ideal of $Y^-(\varphi^-)$, we have $W[[\Gamma_-]]/(L^-_p(\varphi^-)) \cong \mathbb{T}^{\mathrm{ncm}}/I$ (which also shows that the generator of I is a non zero-divisor of $\mathbb{T}^{\mathrm{ncm}}$). Since I is principal generated by a non-zero divisor, we have $I/I^2 \cong \mathbb{T}^{\mathrm{ncm}}/I \cong W[[\Gamma_-]]/(L^-_p(\varphi^-))$, getting the anticyclotomic cyclicity conjecture. If $H \twoheadrightarrow \Gamma_-$ has non-trivial kernel (which implies $p|h_F$), Theorem 5.4 tells us that $Y^-(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W$ is not cyclic over $W[[\Gamma_-]]$.

To reach (2) ⇔ (4) in Theorem B, following the techniques of [H98] and [CV03], we construct an involution σ of $\mathbb{T}$ (Corollary 2.3). By Taylor–Wiles [TW95], $\mathbb{T}$ is known to be a local complete intersection over Λ (so, is Gorenstein over Λ). Adding to the data of the Taylor–Wiles system the involution σ coming from the twist by $\chi = \left(\frac{F/\mathbb{Q}}{}\right)$, 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 Λ with the induced involution σ, and the ring $\mathcal{R}_+$ fixed by involution is proven to be Gorenstein. By the theory of dualizing modules/sheaves for Gorenstein covering $X \to Y$ (studied by A. Grothendieck [SGA 2.VI–V], R. Hartshorne [RDD] and S. Kleiman [Kl80]), this is close to the cyclicity of $\mathcal{R}_- = \{x \in \mathcal{R} | \sigma(x) = -x\}$ over $\mathcal{R}_+$ (see Lemma 10.4), 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 $\mathbb{T}_- = \{x \in \mathbb{T} | \sigma(x) = -x\}$ 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) ⇔ (2).

The Gorenstein-ness of the rings $\mathbb{T}^{\mathrm{ncm}}_+$ and $\mathbb{T}^{\mathrm{ncm}}$ (i.e., (1)) implies (2) by Lemma 10.4 in the theory of dualizing modules). The identity $\mathbb{T}^{\mathrm{ncm}}/(\theta) \cong \mathbb{T}^{\mathrm{ncm}}_+/(\theta^2) \cong W[[H]]/(L^-_p(\varphi^-))$ tells us that $\mathbb{T}^{\mathrm{ncm}}_+$ and $\mathbb{T}^{\mathrm{ncm}}$ are actually local complete intersections; so, (2) ⇒ (1).

The same ring theoretic analysis can be done for a real quadratic field F, as the conditions (h0–4) 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 $\mathbb{T} \neq \Lambda$ 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, (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 (h3) implies an assumption for "$R = T$" theorems of Wiles et al [Wi95] and [TW95]:

(W) $\overline{\rho}$ restricted to $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$ for $M = \mathbb{Q}[\sqrt{(-1)^{(p-1)/2}p}]$ is absolutely irreducible,

and the main reason for us to assume (h3) is the use of the "$R = T$" theorem for the minimal deformation ring R of $\overline{\rho}$ (see Theorem 2.1) though we need this condition for some other purposes. The condition (W) is equivalent to the condition that the representation $\overline{\rho}$ is not of the form $\mathrm{Ind}_M^{\mathbb{Q}}\,\xi$ for a character $\xi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \mathbb{F}^\times$ by Frobenius reciprocity. The implication: (h3) $\Rightarrow$ (W) follows from [H15, Proposition 5.2]. Actually (W) also follows from the following condition:

(h5) $\overline{\varphi}^-$ ramifies at a prime factor $l|N$.

Indeed, if $\overline{\rho} = \mathrm{Ind}_K^{\mathbb{Q}}\,\xi$ for another quadratic field $K \neq F$, by [H15, Proposition 5.2 (2)], KF is uniquely determined degree 4 extension of $\mathbb{Q}$ by $\overline{\rho}$, and the prime l in (h5) ramifies in KF/F as $\overline{\rho}|_{I_l} = \overline{\epsilon}_l \oplus \overline{\delta}_l$ for the inertia group $I_l \subset \mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ with unramified $\overline{\delta}_l$. This is impossible if $K = M$ as only p ramifies in $M/\mathbb{Q}$. Instead assuming (h5), we hope to eliminate the condition (h3) in our future work. By (h2), writing $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \cong \overline{\epsilon} \oplus \overline{\delta}$ with $\overline{\delta} = \overline{\varphi}_{\overline{\mathfrak{p}}}$ unramified, we conclude from (h4)

(Rg) $\overline{\delta} \neq \overline{\epsilon}$.

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 $\mathbf{h}^Q$ of auxiliary Q-level used to construct Taylor–Wiles systems and its CM components $W[[H_Q]]$ as their residue rings. In Section 2, we recall the original $R = \mathbb{T}$ theorem proven by Taylor–Wiles, and in Section 3, we recall some technical details of the Taylor–Wiles argument and prove that $r_- = \dim_{\mathbb{F}} \mathrm{Hom}_{W[[\Gamma_-]]}(Y^-(\varphi^-\omega), \mathbb{F})$ gives an upper bound of the number of generators of $\mathcal{R}_-$ over $\mathcal{R}_+$ (see (3.9)). In Section 4, we prove a sufficient condition for the local intersection property of the subring $\mathbb{T}_+$ of $R = \mathbb{T}$ fixed by the involution σ, employing the method of Taylor–Wiles adding the datum of the involution (Theorem 4.10). In the following Section 5, we prove a finer version of Theorem B (Theorem 5.4), applying the result of Section 4 to a residual representation induced from an imaginary quadratic field. By a Selmer group computation, we show that the number r_- is equal to the number of such inert primes in Q and in turn is equal to the minimum number of generators of $Y^-(\varphi^-)$ over the Iwasawa algebra. In Section 6, we prove $r_- \leq 1$ via classical Kummer's theory applied to units in $F(\varphi^-)$ and hence a finer version (Theorem 6.3) of Theorem A from Theorem B. In Section 7, we show by a control theorem of Rubin that cyclicity of $Y^-(\varphi^-)$ implies cyclicity of the Iwasawa module over K with branch character φ^- and $\varphi^-\omega$ for any $\mathbb{Z}_p$-extension K/F. In Section 8, 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 Λ. In Section 9, 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 $\overline{\mathbb{Q}}$ (resp. $\overline{\mathbb{Q}}_p$) for an algebraic closure of $\mathbb{Q}$ (resp. $\mathbb{Q}_p$) and fix embeddings $\overline{\mathbb{Q}}_p \xleftarrow{i_p} \overline{\mathbb{Q}} \xrightarrow{i_\infty} \mathbb{C}$. We write $\mathbb{C}_p$ for the p-adic completion of $\overline{\mathbb{Q}}_p$. A number field is a subfield of $\overline{\mathbb{Q}}$ by a fixed embedding. We assume $\mathfrak{p} := \{x \in O : |x|_p < 1\}$. For each local ring A, we write $\mathfrak{m}_A$ for the maximal ideal of A. For any profinite abelian group G, we write $W[G]$ for its group algebra, and put $W[[G]] = \varprojlim_H W[G/H]$ for H running over all open subgroups of G; so, $W[[G]] = W[G]$ is G is finite. For a character $\phi : \mathrm{Gal}(F(\phi)/F) \to W^\times$ and $A = W, \mathbb{F}$, we put

$$(Cl_{F(\phi)} \otimes_{\mathbb{Z}} A)[\phi] = \{x \in Cl_{F(\phi)} \otimes_{\mathbb{Z}} A | x^\tau = \phi(\tau)x \text{ for all } \tau \in \mathrm{Gal}(F(\phi)/F)\}.$$

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

We recall the theory of $\mathbf{h}$ 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 $\mathbb{T}/\mathfrak{m}_{\mathbb{T}}$ for the maximal ideal of the connected component $\mathrm{Spec}(\mathbb{T})$ (of our interest) in $\mathrm{Spec}(\mathbf{h})$.

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 $W(\overline{\mathbb{F}}_p)$ 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

$$\begin{aligned} \Gamma_0(Np^r) &:= \{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) | c \equiv 0 \mod Np^r\}, \\ \Gamma_1(Np^r) &:= \{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(Np^r)) | d \equiv 1 \mod Np^r\}. \end{aligned} \tag{1.1}$$

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 ψ as defined in [IAT, (3.5.4)].

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

$$\begin{aligned} \Gamma_0(Q) &:= \{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) | c \equiv 0 \mod q \text{ for all } q \in Q\}, \\ \Gamma_1(Q) &:= \{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(Q)) | d \equiv 1 \mod q \text{ for all } q \in Q\}. \end{aligned} \tag{1.2}$$

Let $\Gamma^{(p)}_Q$ be the subgroup of $\Gamma_0(Q)$ containing $\Gamma_1(Q)$ such that $\Gamma_0(Q)/\Gamma^{(p)}_Q$ 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

$$\Gamma_{Q,r} := \Gamma^{(p)}_Q \cap \Gamma_0(Np^r), \tag{1.3}$$

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

$$\Delta_Q := (\Gamma_0(Np^r) \cap \Gamma_0(Q))/\Gamma_{Q,r}, \tag{1.4}$$

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 $q \not\equiv 1 \mod p$ for all $q \in Q$, we have $\Gamma_1(N_Q p^r) \subset \Gamma_{Q,r} = \Gamma_0(N_Q p^r)$ for $N_Q := N \prod_{q \in Q} q$.

Let the ring $\mathbb{Z}[\psi] \subset \mathbb{C}$ and $\mathbb{Z}_p[\psi] \subset \overline{\mathbb{Q}}_p$ be generated by the values ψ 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 $T(n)$:

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

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 Γ containing $\Gamma_1(Np^r)$, we write $h_k(\Gamma,\psi;W)$ for the Hecke algebra on Γ with coefficients in W acting on $S_{k+1}(\Gamma,\psi;W)$. The algebra $h_k(\Gamma,\psi;W)$ can be also realized as $W[T(n)|n=1,2,\cdots] \subset \mathrm{End}_W(S_{k+1}(\Gamma,\psi;W))$. 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 $\mathbf{h}_{Q,k,\psi/W} \subset h_{Q,k,\psi/W}$ is the maximal ring direct summand on which $U(p)$ is invertible. If $Q=\emptyset$, we simply write $\mathbf{h}_{k,\psi/W}$ for $\mathbf{h}_{\emptyset,k,\psi/W}$. We write e for the idempotent of $\mathbf{h}_{Q,k,\psi/W}$, 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 $S_{k+1}(\Gamma_{Q,r},\psi)$ (as e descends from $S_{k+1}(\Gamma_{Q,r},\psi,\overline{\mathbb{Q}}_p)$ to $S_{k+1}(\Gamma_{Q,r},\psi,\overline{\mathbb{Q}})$). We write the image $M^{\mathrm{ord}} := e(M)$ of the idempotent attaching the superscript "ord" (e.g., S^{ord}_{k+1}).

Fix a character ψ_0 modulo Np, and assume now $\psi_0(-1)=-1$. Let ω 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 $\Lambda = W[[\Gamma]] = \varprojlim_n W[\Gamma/\Gamma^{p^n}]$ 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 $\mathbf{h}^Q$ (of level $\Gamma_{Q,\infty}$). We write $\mathbf{h}$ for $\mathbf{h}^\emptyset$.

Since $Np = DN_{F/\mathbb{Q}}(\mathfrak{c})p \geq Dp > 4$, the algebra $\mathbf{h}^Q$ 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) $\mathbf{h}^Q$ is free of finite rank over Λ equipped with $T(n)\in\mathbf{h}^Q$ 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,

$$\mathbf{h}^Q/(t-\epsilon(\gamma)\gamma^k)\mathbf{h}^Q \cong \mathbf{h}_{Q,k,\epsilon\psi_k}\ (\gamma=1+p) \text{ for } \psi_k := \psi_0\omega^{-k},$$

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 $\mathbf{h}^Q$ is flat over $\Lambda[\Delta_Q]$ with $\mathbf{h}^Q/\mathfrak{A}_{\Delta_Q}\mathbf{h}^Q \cong \mathbf{h}^\emptyset$ 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 $\mathbf{h}_{Q,k,\epsilon\psi_k} := \mathbf{h}^Q/(t-\epsilon(\gamma)\gamma^k)\mathbf{h}^Q$ which acts on p-ordinary p-adic cusp forms of weight k and of Neben character $\epsilon\psi_k$. By the above lemma, $\mathbf{h}_{Q,k,\epsilon\psi_k}$ is free of finite rank d over $W[\Delta_Q]$ whose rank over $W[\Delta_Q]$ is equal to $\mathrm{rank}_W\,\mathbf{h}_{\emptyset,k,\epsilon\psi_k}$ (independent of Q).

Since N_Q is cube-free, by [H13, Corollary 1.3], $\mathbf{h}^Q$ is reduced. Let $\mathrm{Spec}(\mathbb{I})$ be an irreducible component of $\mathrm{Spec}(\mathbf{h}^Q)$. 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 $\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ 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 ϵ_P. If P is arithmetic, by (C2), we have a Hecke eigenform $f_P\in S_{k+1}(\Gamma_{Q,r(P)+1},\epsilon\psi_k)$ such that its eigenvalue for $T(n)$ is given by $a_P(n) := P(a(n))\in\overline{\mathbb{Q}}$ for all n. Thus $\mathbb{I}$ gives rise to a family $\mathcal{F}=\{f_P|\text{arithmetic } P\in\mathrm{Spec}(\mathbb{I})\}$ of Hecke eigenforms. We define a *p-adic analytic family of slope* 0 (with coefficients in $\mathbb{I}$) to be the family as above of Hecke eigenforms associated to an irreducible component $\mathrm{Spec}(\mathbb{I})\subset\mathrm{Spec}(\mathbf{h}^Q)$. We call this family slope 0 because $|a_P(p)|_p=1$ for the p-adic absolute value $|\cdot|_p$ of $\overline{\mathbb{Q}}_p$ (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 $\mathrm{Spf}(\mathbb{I})$. Identify $\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ with $\mathrm{Hom}_{W\text{-alg}}(\mathbb{I},\overline{\mathbb{Q}}_p)$ so that each element $a\in\mathbb{I}$ gives rise to a "function" $a:\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)\to\overline{\mathbb{Q}}_p$ whose value at $(P:\mathbb{I}\to\overline{\mathbb{Q}}_p)\in\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ is $a_P := P(a)\in\overline{\mathbb{Q}}_p$. Then a is an analytic function of the rigid analytic space associated to $\mathrm{Spf}(\mathbb{I})$. Taking a finite covering $\mathrm{Spec}(\widetilde{\mathbb{I}})$ of $\mathrm{Spec}(\mathbb{I})$ with surjection $\mathrm{Spec}(\widetilde{\mathbb{I}})(\overline{\mathbb{Q}}_p)\twoheadrightarrow\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$, abusing slightly the definition, we may regard the family $\mathcal{F}$ as being indexed by arithmetic points of $\mathrm{Spec}(\widetilde{\mathbb{I}})(\overline{\mathbb{Q}}_p)$, where arithmetic points of $\mathrm{Spec}(\widetilde{\mathbb{I}})(\overline{\mathbb{Q}}_p)$ are made up of the points above arithmetic points of $\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$. The choice of $\widetilde{\mathbb{I}}$ is often the normalization of $\mathbb{I}$ or the integral closure of $\mathbb{I}$ in a finite extension of the quotient field of $\mathbb{I}$.

Each irreducible component $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbf{h}^Q)$ has a 2-dimensional semi-simple (actually absolutely irreducible) continuous representation $\rho_{\mathbb{I}}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with coefficients in the quotient field of $\mathbb{I}$ (see [H86b]). The representation $\rho_{\mathbb{I}}$ 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]), $\rho_{\mathbb{I}}$ is unramified outside $N_Q p$ and satisfies

$$\text{(Gal)} \qquad \mathrm{Tr}(\rho_{\mathbb{I}}(\mathrm{Frob}_l)) = a(l) \ \ (l \nmid Np), \ \rho_{\mathbb{I}}([\gamma^s, \mathbb{Q}_p]) \sim \left(\begin{smallmatrix} t^s & * \\ 0 & 1 \end{smallmatrix}\right) \text{ and } \rho_{\mathbb{I}}([p, \mathbb{Q}_p]) \sim \left(\begin{smallmatrix} * & * \\ 0 & a(p) \end{smallmatrix}\right),$$

where $\gamma^s = (1+p)^s = \sum_{n=0}^{\infty} \binom{s}{n} p^n \in \mathbb{Z}_p^\times$ for $s \in \mathbb{Z}_p$ and $[x, \mathbb{Q}_p]$ is the local Artin symbol. As for primes in $q \in Q$, if $q \equiv 1 \mod p$ and $\overline{\rho}(\mathrm{Frob}_q)$ has two distinct eigenvalues, we have

$$(\mathrm{Gal}_q) \qquad \rho_{\mathbb{I}}([z, \mathbb{Q}_q]) \sim \begin{pmatrix} \alpha_q(z) & 0 \\ 0 & \beta_q(z) \end{pmatrix} \text{ with characters } \alpha_q \text{ and } \beta_q \text{ of } \mathbb{Q}_q^\times \text{ for } z \in \mathbb{Q}_q^\times,$$

where one of α_q and β_q is unramified (e.g., [MFG, Theorem 3.32 (2)] or [HMI, Theorem 3.75]). For each prime ideal P of $\mathrm{Spec}(\mathbb{I})$, writing $\kappa(P)$ for the residue field of P, we also have a semi-simple Galois representation $\rho_P : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\kappa(P))$ unramified outside $N_Q p$ such that $\mathrm{Tr}(\rho_P(\mathrm{Frob}_l))$ is given by $a(l)_P$ for all primes $l \nmid N_Q p$. If P is the maximal ideal $\mathfrak{m}_{\mathbb{I}}$, we write $\overline{\rho}$ for ρ_P which is called the residual representation of $\rho_{\mathbb{I}}$. The residual representation $\overline{\rho}$ is independent of $\mathbb{I}$ as long as $\mathrm{Spec}(\mathbb{I})$ belongs to a given connected component $\mathrm{Spec}(\mathbb{T})$ of $\mathrm{Spec}(\mathbf{h}^Q)$. Indeed, $\mathrm{Tr}(\rho_P) \mod \mathfrak{m}_{\mathbb{I}} = \mathrm{Tr}(\overline{\rho})$ for any $P \in \mathrm{Spec}(\mathbb{T})$. If P is an arithmetic prime, we have $\det(\rho_P) = \epsilon_P \psi_k \nu_p^k$ for the p-adic cyclotomic character ν_p (regarding ϵ_P and ψ_k 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 $\mathbb{I}$ is called a *CM component* if there exists a nontrivial character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{I}^\times$ such that $\rho_{\mathbb{I}} \cong \rho_{\mathbb{I}} \otimes \chi$. We also say that $\mathbb{I}$ has *complex multiplication* if $\mathbb{I}$ 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 $\mathbb{I}$ with $\rho_{\mathbb{I}} \cong \rho_{\mathbb{I}} \otimes \chi$, then χ is a quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which cuts out an imaginary quadratic field F, i.e., $\chi = \left(\frac{F/\mathbb{Q}}{}\right)$. Write $\widetilde{\mathbb{I}}$ for the integral closure of Λ inside the quotient field of $\mathbb{I}$. The following three conditions are known to be equivalent:

(CM1) *$\mathcal{F}$ has CM with $\rho_{\mathbb{I}} \cong \rho_{\mathbb{I}} \otimes \left(\frac{F/\mathbb{Q}}{}\right)$ ($\Leftrightarrow \rho_{\mathbb{I}} \cong \mathrm{Ind}_F^{\mathbb{Q}} \widehat{\lambda}$ for a character $\widehat{\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \widetilde{\mathbb{I}}^\times$);*

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

(CM3) *For some arithmetic P of* $\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$*, f_P is a binary theta series of the norm form of $F/\mathbb{Q}$.*

Indeed, (CM1) is equivalent to $\rho_{\mathbb{I}} \cong \mathrm{Ind}_F^{\mathbb{Q}} \widehat{\lambda}$ for a character $\widehat{\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{Frac}(\mathbb{I})^\times$ unramified outside Np (e.g., [DHI98, Lemma 3.2] or [MFG, Lemma 2.15]). Since the characteristic polynomial of $\rho_{\mathbb{I}}(\sigma)$ has coefficients in $\mathbb{I}$, its eigenvalues fall in $\widetilde{\mathbb{I}}$; so, the character $\widehat{\lambda}$ has values in $\widetilde{\mathbb{I}}^\times$ (see, [H86c, Corollary 4.2]). Then by (Gal), $\widehat{\lambda}_P = P \circ \widehat{\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \overline{\mathbb{Q}}_p^\times$ for an arithmetic $P \in \mathrm{Spec}(\widetilde{\mathbb{I}})(\overline{\mathbb{Q}}_p)$ is a locally algebraic p-adic character, which is the p-adic avatar of a Hecke character $\lambda_P : F_{\mathbb{A}}^\times / F^\times \to \mathbb{C}^\times$ of type A_0 of the quadratic field $F_{/\mathbb{Q}}$. Then by the characterization (Gal) of $\rho_{\mathbb{I}}$, f_P is the theta series with q-expansion $\sum_{\mathfrak{a}} \lambda_P(\mathfrak{a}) q^{N(\mathfrak{a})}$, where $\mathfrak{a}$ 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 $\Leftrightarrow k = 0$; cf., [MFM, §4.8]). This shows (CM1)$\Rightarrow$(CM2)$\Rightarrow$(CM3). If (CM2) is satisfied, we have an identity $\mathrm{Tr}(\rho_{\mathbb{I}}(\mathrm{Frob}_l)) = a(l) = \chi(l) a(l) = \mathrm{Tr}(\rho_{\mathbb{I}} \otimes \chi(\mathrm{Frob}_l))$ with $\chi = \left(\frac{F/\mathbb{Q}}{}\right)$ for all primes l outside Np. By Chebotarev density, we have $\mathrm{Tr}(\rho_{\mathbb{I}}) = \mathrm{Tr}(\rho_{\mathbb{I}} \otimes \chi)$, and we get (CM1) from (CM2) as $\rho_{\mathbb{I}}$ is semi-simple. If a component $\mathrm{Spec}(\mathbb{I})$ contains an arithmetic point P with theta series f_P as above of $F/\mathbb{Q}$, either $\mathbb{I}$ is a CM component or otherwise P is in the intersection in $\mathrm{Spec}(\mathbf{h}^Q)$ of a component $\mathrm{Spec}(\mathbb{I})$ 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 [H86a, §7]). The latter case cannot happen as two distinct components never cross at an arithmetic point in $\mathrm{Spec}(\mathbf{h}^Q)$ (i.e., the reduced part of the localization $\mathbf{h}_P^Q$ is étale over Λ_P for any arithmetic point $P \in \mathrm{Spec}(\Lambda)(\overline{\mathbb{Q}}_p)$; 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 $\mathbf{h}^Q$ whose Galois representation is 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 $\mathrm{Gal}(F/\mathbb{Q})$ (even if F is real). Let $\mathfrak{c}$ be the prime-to-p conductor of a character $\overline{\varphi}$ as in Theorem B in the introduction (allowing real F). Put $\mathfrak{C} = \mathfrak{c} \cap \mathfrak{c}^c$. By (h1), $\mathfrak{c}$ is a square free integral ideal of F with $\mathfrak{c} + \mathfrak{c}^c = O$ (for complex conjugation c). Since Q is outside N, Q is a finite set of rational primes unramified in $F/\mathbb{Q}$ prime to $\mathfrak{C}p$. Let Q^+ be the subset in Q made up of primes split in F. We choose a prime factor $\mathfrak{q}$ of q for each $q \in Q^+$ (once and for all), and put $\mathfrak{Q}^+ := \prod_{q\in Q^+} \mathfrak{q}$. We study some ray class groups isomorphic to H_Q. We put $\mathfrak{C}_{Q^+} := \mathfrak{C}\prod_{q\in Q^+} q$. We simply write $\mathfrak{C}$ for $\mathfrak{C}_\emptyset$. Consider the ray class group $Cl(\mathfrak{a}) = Cl_F(\mathfrak{a})$ (of F) modulo $\mathfrak{a}$ for an integral ideal $\mathfrak{a}$ of O, and put

$$Cl(\mathfrak{c}\mathfrak{Q}^+\mathfrak{p}^\infty) = \varprojlim_r Cl(\mathfrak{c}\mathfrak{Q}^+\mathfrak{p}^r), \quad \text{and} \quad Cl(\mathfrak{C}_{Q^+}p^\infty) = \varprojlim_r Cl(\mathfrak{C}_{Q^+}p^r). \tag{1.5}$$

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

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

$$\pi : \mathfrak{Z}_{Q^+} \twoheadrightarrow Z_{Q^+} \ \text{ and } \ \pi^- : \mathfrak{Z}_{Q^+} \to Z^-_{Q^+}.$$

Recall $p > 3$; so, the projection π^- induces an isomorphism $\mathfrak{Z}^{1-c}_{Q^+} = \{zz^{-c} | z \in \mathfrak{Z}_{Q^+}\} \to Z^-_{Q^+}$. Thus π^- induces an isomorphism between the p-profinite groups $Z^-_{Q^+}$ and $\mathfrak{Z}^{1-c}_{Q^+}$. Similarly, π induces $\pi : \mathfrak{Z}^{1-c}_{Q^+} \cong Z_{Q^+}$. Thus we have for the Galois group H_Q as in the introduction

$$\iota : Z_{Q^+} \cong Z^-_{Q^+} \cong H_Q \tag{1.6}$$

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

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

1. Φ is unramified outside $\mathfrak{c}\mathfrak{Q}^+\mathfrak{p}$,
2. $\Phi(\mathrm{Frob}_\mathfrak{l}) = \varphi(\mathrm{Frob}_\mathfrak{l})[\mathfrak{l}]$ for each prime $\mathfrak{l}$ outside $N\mathfrak{p}$ and $\mathfrak{Q}^+$, where $[\mathfrak{l}]$ is the projection to Z_{Q^+} of the class of $\mathfrak{l}$ in $Cl(\mathfrak{c}\mathfrak{Q}^+\mathfrak{p}^\infty)$.

When F is real, all groups Z_{Q^+}, $Z^-_{Q^+}$ and H_Q are finite groups; so, $W[[Z_{Q^+}]] = W[Z_{Q^+}]$ for example. The character Φ 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 $\overline{\varphi}(\mathrm{Frob}_\mathfrak{q}) \neq \overline{\varphi}(\mathrm{Frob}_{\mathfrak{q}^c})$ for all $\mathfrak{q}|\mathfrak{Q}^+$. Then we have a surjective Λ-algebra homomorphism $\mathbf{h}^{Q^+} \twoheadrightarrow W[[Z_{Q^+}]]$ such that*

1. *$T(l) \mapsto \Phi(\mathfrak{l}) + \Phi(\mathfrak{l}^c)$ if $l = \mathfrak{l}\mathfrak{l}^c$ with $\mathfrak{l} \neq \mathfrak{l}^c$ and $l \nmid N_{Q^+}p$;*
2. *$T(l) \mapsto 0$ if l remains prime in F and is prime to $N_{Q^+}p$;*
3. *$U(q) \mapsto \Phi(\mathfrak{q}^c)$ if $\mathfrak{q}$ is a prime ideal with $\mathfrak{q}|\mathfrak{Q}^+\mathfrak{c}$;*
4. *$U(p) \mapsto \Phi(\mathfrak{p}^c)$.*

If F is real, the above homomorphism factors through the weight 1 Hecke algebra $\mathbf{h}^{Q^+}/(t^{p^m} - 1)\mathbf{h}^{Q^+}$ 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 $f|T(q) = a_q f$ for $q \notin Q^+$ and two roots α, β 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 $f_x|U(q) = x f_x$ for $x = \alpha, \beta$. This tells us that if we choose a set $\Sigma^- := \{\overline{\alpha}_q | q \in Q^-\}$ of mod p eigenvalues of $\overline{\rho}(\mathrm{Frob}_q)$ for $q \in Q^- := Q - Q^+$, we have a unique local ring $\mathbb{T}^Q$ of $\mathbf{h}^Q$ and a surjective algebra homomorphism $\mathbb{T}^Q \twoheadrightarrow W[[Z_{Q^+}]]$ factoring through $\mathbf{h}^{Q^+} \twoheadrightarrow W[[Z_{Q^+}]]$ such that $U(q) \mod \mathfrak{m}_{\mathbb{T}^Q} = \overline{\alpha}_q$ for all $q \in Q^-$. For $q \in Q^-$, if f is a theta series of F, we have $a_q = 0$; so, the residual class (modulo $\mathfrak{m}_{\mathbb{T}^Q}$) of α and β in $\mathbb{Z}_p[\alpha, \beta] \subset \overline{\mathbb{Q}}_p$ are distinct (because of $p > 2$). Therefore if we change Σ^-, the local ring $\mathbb{T}^Q$ will be changed accordingly. We record this fact as

Corollary 1.3. *Suppose that $\overline{\varphi}(\mathrm{Frob}_{\mathfrak{q}}) \neq \overline{\varphi}(\mathrm{Frob}_{\mathfrak{q}^c})$ for all $\mathfrak{q}|\mathfrak{Q}^+$ and that W is sufficiently large so that we can choose a set $\Sigma^- = \{\overline{\alpha}_q \in \mathbb{F} | q \in Q^-\}$ of mod p eigenvalues of $\overline{\rho}(\mathrm{Frob}_q)$ for $q \in Q^- = Q - Q^+$ in the residue field $\mathbb{F}$ of W. Then we have a unique local ring $\mathbb{T}^Q$ of $\mathbf{h}^Q$ such that we have a surjective Λ-algebra homomorphism $\mathbb{T}^Q \twoheadrightarrow W[[Z_{Q^+}]]$ characterized by the following conditions:*

1. *$T(l) \mapsto \Phi(\mathfrak{l}) + \Phi(\mathfrak{l}^c)$ if $l = \mathfrak{l}\mathfrak{l}^c$ with $\mathfrak{l} \neq \mathfrak{l}^c$ and $l \nmid N_Q p$;*
2. *$T(l) \mapsto 0$ if l remains prime in F and is prime to $N_Q p$;*
3. *$U(q) \mapsto \Phi(\mathfrak{q}^c)$ if $\mathfrak{q}$ is a prime ideal with $\mathfrak{q}|\mathfrak{Q}^+\mathfrak{c}$;*
4. *$U(q) \mapsto \pm\Phi(\mathfrak{q})$ if $q \in Q^-$, where the sign is determined by $\pm\Phi(\mathfrak{q}) \mod \mathfrak{m}_{\mathbb{T}^Q} = \overline{\alpha}_q$;*
5. *$U(p) \mapsto \Phi(\mathfrak{p}^c)$.*

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

We will later show that the quotient $\mathbb{T}^Q \twoheadrightarrow W[[Z_Q]]$ 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 $\Sigma^- = \{\overline{\alpha}_q \in \mathbb{F} | q \in Q^-\}$, we put

$$\mathbb{T}_Q = \mathbb{T}^Q/(t - \gamma^k)\mathbb{T}^Q. \tag{1.7}$$

The choice of $\mathfrak{q}|\mathfrak{Q}^+$ can be also considered to be the choice $\Sigma^+ := \{\overline{\varphi}(\mathrm{Frob}_{\mathfrak{q}^c}) \in \mathbb{F} : \mathfrak{q}|\mathfrak{Q}^+\}$ of the eigenvalue of $U(q)$. Thus the local rings $\mathbb{T}^Q$ and $\mathbb{T}_Q$ are considered to be defined with respect to the choice $\Sigma = \Sigma^+ \sqcup \Sigma^-$ of one of the mod p eigenvalues of $U(q)$ for each $q \in Q$. In other words, $\mathbb{T}_Q$ is a local factor of $\mathbf{h}_{Q,k,\psi_k}$ with the prescribed mod p eigenvalues Σ of $U(q)$ for $q \in Q$. Note that $\mathbb{T}_Q$ 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 $\mathcal{Q}^+ = \{\mathfrak{Q}^+_m | m = 1, 2, \dots\}$ of r_+-sets $\mathfrak{Q}^+_m$ of primes $\mathfrak{q}$ of O such that $N(\mathfrak{q}) \equiv 1 \mod p^m$. We assume that $\mathfrak{Q}^+_m$ is made of primes split in $F/\mathbb{Q}$ outside $\mathfrak{c}p$ and that $\mathfrak{q} \mapsto \mathfrak{q} \cap \mathbb{Z}$ induces a bijection between $\mathfrak{Q}^+_m$ and $Q^+_m := \{\mathfrak{q} \cap \mathbb{Z} | \mathfrak{q} \in \mathfrak{Q}^+_m\}$. We regard Q^+_m as a set of rational primes. We write $\mathfrak{Q}^+_m$ sometimes for the product $\prod_{\mathfrak{q} \in Q^+_m} \mathfrak{q}$. Then the inclusion $\mathbb{Z} \hookrightarrow O$ induces a natural isomorphism $\prod_{q \in Q^+_m} (\mathbb{Z}/q\mathbb{Z})^\times \cong (O/\mathfrak{Q}^+_m)^\times$. 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 $\Delta_{\mathfrak{q}} \cong \Delta_q$ of $(O/\mathfrak{q})^\times \cong (\mathbb{Z}/q\mathbb{Z})^\times$. For the ray class group $Cl(\mathfrak{c}\mathfrak{Q}^+_m\mathfrak{p}^n)$, we have a natural exact sequence of abelian groups

$$(O/\mathfrak{Q}^+_m)^\times \xrightarrow{i} Cl(\mathfrak{c}\mathfrak{Q}^+_m\mathfrak{p}^n) \to Cl(\mathfrak{c}\mathfrak{p}^n) \to 1,$$

which induces the exact sequence of its maximal p-abelian quotients:

$$1 \to \Delta_{Q^+_m} \to Cl(\mathfrak{c}\mathfrak{Q}^+_m\mathfrak{p}^n)_p \to Cl(\mathfrak{c}\mathfrak{p}^n)_p \to 1,$$

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

$$1 \to \Delta_{Q^+_m} \to Z_{Q^+_m} \to Z_\emptyset \to 1. \tag{1.8}$$

We consider the group algebra $W[[Z_{Q^+_m}]]$ which is an algebra over $W[\Delta_{Q^+_m}]$. We choose a generator δ_q of the cyclic group $\Delta_{\mathfrak{q}}$ and put Δ^+_n to be the quotient of $\Delta_{Q^+_m}$ by the subgroup generated by $\{\delta_q^{p^n}\}_{q \in Q^+_m}$ for $0 < n \leq m$; thus, $\Delta^+_n \cong (\mathbb{Z}/p^n\mathbb{Z})^{r_+}$. This include the ordering $Q^+_m = \{q_1, \dots, q_{r_+}\}$

so that the above isomorphism sends $\Delta_{q_j}/\langle\delta_{q_j}^{p^n}\rangle$ to the j-th factor $\mathbb{Z}/p^n\mathbb{Z}$. In this way, we fix the identification of Δ_n^+ with $(\mathbb{Z}/p^n\mathbb{Z})^{r_+}$ for all n and m once and for all. Thus, writing $W_n := W/p^nW$, we get a projective system

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

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

$$W[[S_1,\dots,S_{r_+}]] \cong \varprojlim_n W_n[\Delta_n^+]$$

sending $s_j = 1 + S_j$ to the image of δ_{q_j} in Δ_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 $\mathbb{Z}_p^\times \cong O_\mathfrak{p}^\times$ induces a group morphism $\mathbb{Z}_p^\times \to Cl(\mathfrak{c}\mathfrak{p}^\infty)$, which induces an isomorphism $\Gamma = 1 + p\mathbb{Z}_p \cong Z_\emptyset$. 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 $m \geq n$:

$$\begin{tikzcd}
W_{n'}[[\Gamma]][\Delta_{n'}^+] \cong W[[Z_{Q_{m'}^+}]]/\mathfrak{A}_{n'} \arrow[r, "\twoheadrightarrow"] \arrow[d, "\pi_n^{n'}"'] & W_{n'}[[Z_\emptyset]] \arrow[d, "\text{onto}"'] \\
W_n[[\Gamma]][\Delta_n^+] \cong W[[Z_{Q_m^+}]]/\mathfrak{A}_n \arrow[r, "\twoheadrightarrow"] & W_n[[Z_\emptyset]],
\end{tikzcd}$$

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

$$\{W[[Z_{Q_{m'}^+}]]/\mathfrak{A}_{n'} \xrightarrow{\pi_n^{n'}} W[[Z_{Q_m^+}]]/\mathfrak{A}_n\}_{n'>n}.$$

By this map, $W[[Z_{Q_m^+}]]/\mathfrak{A}_n$ is naturally a Λ-algebra via the canonical splitting $Z_{Q_m^+} = \Delta_{Q_m^+} \times Z_\emptyset$, and hence a $\Lambda[[S_1,\dots,S_{r_+}]]$-algebra. Since $Z_\emptyset = \Gamma$, we get $\varprojlim_n W[[Z_{Q_m^+}]]/\mathfrak{A}_n \cong \Lambda[[S_1,\dots,S_{r_+}]]$. 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 $\varprojlim_n W[[H_{Q_m^+}]]/\mathfrak{A}_n$ is isomorphic to $\Lambda[[S_1,\dots,S_{r_+}]]$.*

This follows from the above argument, after identifying $Z_{Q_m^+}$ with $H_{Q_m^+}$ and identifying Λ 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 $\mathcal{Q}^+$ of r_+-sets $\mathfrak{Q}_m^+$ of split primes in F outside N such that $N(\mathfrak{q}) \equiv 1 \mod p^m$ with $Q_m^+ := \{(q) = \mathfrak{q} \cap \mathbb{Z} | \mathfrak{q} \in \mathfrak{Q}_m^+\}$ with an ordering. We still have the following exact sequence (1.8):

$$1 \to \Delta_{Q_m^+} \to Z_{Q_m^+} \xrightarrow{\pi_{Q_m^+}} Z_\emptyset \to 1.$$

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 Γ_F. The projection $\pi_{Q_m^+}$ identifies the maximal torsion-free quotient of $Z_{Q_m^+}$ with Γ_F. Write $Z_{Q_m^+,tor} : \mathrm{Ker}(Z_{Q_m^+} \to \Gamma_F)$ (the maximal torsion subgroup of Z_{Q^+}). Note that $\Delta_{Q_m^+} \hookrightarrow Z_{Q_m^+,tor}$. For m running over integers with $m \geq n$, the isomorphism classes of the set of cokernels $\{Z_{Q_m^+,tor}/\Delta_{Q_m^+}^{p^n}\}_{m\geq n}$ of pairs of abelian groups is finite. Here $Z_{Q_m^+,tor}/\Delta_{Q_m^+}^{p^n}$ and $Z_{Q_{m'}^+,tor}/\Delta_{Q_{m'}^+}^{p^n}$ are isomorphic if the following diagram for $m' > m$ is commutative:

$$\begin{tikzcd}
\Delta_{Q_m^+}/\Delta_{Q_m^+}^{p^n} \arrow[r, "\hookrightarrow"] \arrow[d, "\wr"', "i_{m,m'}"] & Z_{Q_m^+,tor}/\Delta_{Q_m^+}^{p^n} \arrow[d, "\wr"'] \\
\Delta_{Q_{m'}^+}/\Delta_{Q_{m'}^+}^{p^n} \arrow[r, "\hookrightarrow"] & Z_{Q_{m'}^+,tor}/\Delta_{Q_{m'}^+}^{p^n}.
\end{tikzcd}$$

Here $i_{m,m'}$ is induced by sending the generator $\delta_{q_j}\Delta_{Q_m^+}^{p^n}$ for $Q_m^+ = \{q_1,\dots,q_{r_+}\}$ to the generator $\delta_{q'_j}\Delta_{Q_{m'}^+}^{p^n}$ writing $Q_{m'}^+ = \{q'_1,\dots,q'_{r_+}\}$ according to our choice of ordering. Starting with $n = 1$, we have an isomorphism class $\mathcal{I}_1$ in $\{Z_{Q_m^+,tor}/\Delta_{Q_m^+}^p\}_{m\geq1}$ with infinite elements. Suppose that we have constructed a sequence $\mathcal{I}_n \to \mathcal{I}_{n-1} \to \cdots \to \mathcal{I}_1$ of isomorphism classes $\mathcal{I}_j$ in $\{Z_{Q^+_m,tor}/\Delta^{p^j}_{Q^+_m}\}_{m\geq j}$ such that $Z_{Q^+_m,tor}/\Delta^{p^j}_{Q^+_m} \in \mathcal{I}_j$ is sent onto to $Z_{Q^+_m,tor}/\Delta^{p^{j-1}}_{Q^+_m}$ in $\mathcal{I}_{j-1}$ for all $j = 2, 3, \ldots, n$. Since

$$\mathcal{I}'_{n+1} := \{Z_{Q^+_m,tor}/\Delta^{p^{n+1}}_{Q^+_m} | (Z_{Q^+_m,tor}/\Delta^{p^n}_{Q^+_m}) \in \mathcal{I}_n\}_{m\geq n+1}$$

is an infinite set, we can choose an isomorphism class $\mathcal{I}_{n+1} \subset \mathcal{I}'_{n+1}$ with $|\mathcal{I}_{n+1}| = \infty$. Thus by induction on n, we find an infinite sequence $\cdots \to \mathcal{I}_n \to \mathcal{I}_{n-1} \to \cdots \to \mathcal{I}_1$ as above. Then we define $m(n)$ for each n to be the minimal m appearing $\mathcal{I}_n$. Thus we have a projection $\pi^n_{n+1,tor}$: $Z_{Q^+_{m(n+1)},tor}/\Delta^{p^{n+1}}_{Q^+_{m(n+1)}} \to Z_{Q^+_{m(n)},tor}/\Delta^{p^n}_{Q^+_{m(n)}}$ and a projective system of groups

$$\begin{tikzcd}
Z_{Q^+_{m(n+1)},tor}/\Delta^{p^{n+1}}_{Q^+_{m(n+1)}} \arrow[r, hook] \arrow[d, "\pi^n_{n+1,tor}"'] & Z_{Q^+_{m(n+1)}}/\Delta^{p^{n+1}}_{Q^+_{m(n+1)}} \arrow[r, two heads] \arrow[d, "\pi^n_{n+1}"'] & \Gamma_F \arrow[d, "\Vert"'] \\
Z_{Q^+_{m(n)},tor}/\Delta^{p^n}_{Q^+_{m(n)}} \arrow[r, hook] & Z_{Q_{m(n)}}/\Delta^{p^n}_{Q^+_{m(n)}} \arrow[r, two heads] & \Gamma_F.
\end{tikzcd}$$

Passing to the limit, we have an exact sequence:

$$1 \to \varprojlim_n Z_{Q^+_{m(n)},tor}/\Delta^{p^n}_{Q^+_{m(n)}} \to \varprojlim_n Z_{Q_{m(n)}}/\Delta^{p^n}_{Q^+_{m(n)}} \to \Gamma_F \to 1.$$

Note here the subgroup $\Delta_\infty := \varprojlim_n \Delta_{Q^+_{m(n)}}/\Delta^{p^n}_{Q^+_{m(n)}} \cong \mathbb{Z}_p^{r_+}$ with $W[[\Delta_\infty]] = W[[S_1, \ldots, S_{r_+}]]$ for the variable chosen as in Proposition 1.4 and $W[[Z_S]]$ for $Z_S := \varprojlim_n Z_{Q^+_{m(n)},tor}/\Delta^{p^n}_{Q^+_{m(n)}}$ is an algebra free of finite rank over $W[[\Delta_\infty]]$. We write $\Gamma_S = Z_S/Z_{S,tor}$ for the maximal torsion subgroup $Z_{S,tor}$ of Z_S. Choose a splitting of the exact sequence $Z_{S,tor} \hookrightarrow Z_S \twoheadrightarrow \Gamma_S$ so that Γ_S as a subgroup of Z_S contains Δ_∞. Then $W[[Z_S]] = W[[\Gamma_S]][Z_{S,tor}] \cong W[[\Gamma_S]][Z_S/\Gamma_S]]$. By splitting the projection $Z_\infty := \varprojlim_n Z_{Q_{m(n)}}/\Delta^{p^n}_{Q^+_{m(n)}} \twoheadrightarrow \Gamma_F$, 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 $H_{Q^+_m}$ with $Z_{Q^+_m}$ by (1.6). Then there is a subsequence $\{\mathfrak{Q}_{m(n)}\}_{n=1,2,\ldots} \subset \mathcal{Q}^+$ such that $\{W[[H_{Q^+_{m(n)}}]]/\mathfrak{A}_n\}_n$ forms a projective system of finite rings and that the limit ring $\varprojlim_n W[[H_{Q^+_m}]]/\mathfrak{A}_n$ is isomorphic to the profinite group algebra $W[[\Gamma_F \times \Gamma_S]][Z_\infty/\Gamma_S]$, and Γ_S (resp. Γ_F) contains Δ_∞ (resp. Γ) as a subgroup of finite index. In particular, $\varprojlim_n W[[H_{Q^+_m}]]/\mathfrak{A}_n$ is free of finite rank over $\Lambda[[S_1, \ldots, S_{r_+}]]$ and is a local complete intersection over Λ.*

2. The $R = \mathbb{T}$ 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 $\mathbb{F} = \mathbb{T}/\mathfrak{m}_{\mathbb{T}}$. For the moment, we only assume (h0–3) for a fixed connected component $\mathrm{Spec}(\mathbb{T})$ of $\mathrm{Spec}(\mathbf{h})$ for $\mathbf{h} := \mathbf{h}^\emptyset$ and its residual representation $\overline{\rho}$ of the form $\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$ for a Galois character $\overline{\varphi} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathbb{F}$.

We fix a weight $k \geq 0$ and pick a Hecke character $\varphi_k : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to W^\times$ of conductor at most $\mathfrak{c}\mathfrak{p}$ with p-type $-ki_p|_F$ for the identity embedding $i_p|_F : F \hookrightarrow \overline{\mathbb{Q}}_p$ such that $\varphi_k \equiv \varphi \mod \mathfrak{m}_W$. Let $\theta(\varphi_k) \in S_{k+1}(\Gamma_0(Np), \psi_k)$ for the corresponding theta series. Then ψ_k is determined by φ_k (i.e., $\psi_k = \chi\varphi_k|_{\mathbb{A}^\times}\nu_p^k$ regarding φ_k and ψ_k as idele characters; see [HMI, Theorem 2.71]). When F is imaginary (that is usually the case), we assume that $k \geq 1$.

Recall the identity $\psi_k\nu_p^k \mod \mathfrak{m}_W = \det(\overline{\rho})$ for the p-adic cyclotomic character ν_p; so, ψ_0 is the Teichmüller lift of $\det(\overline{\rho})$. Hereafter, we simply write ψ for $\psi_0 = \psi_k\omega^k$. Writing $\mathfrak{c}$ for the prime-to-p conductor of $\overline{\varphi}$, by (h2), $N_{F/\mathbb{Q}}(\mathfrak{c})D = N$ for the discriminant D of F (cf. [GME, Theorem 5.1.9]). By (h1), the conductor $\mathfrak{c}$ is square-free and only divisible by split primes in $F/\mathbb{Q}$. Since $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$, for $l|Np$, the prime l either splits in F or ramified in F. Write $\mathfrak{l}$ for the prime factor of (l) in F. If (l) splits into $\mathfrak{l}\overline{\mathfrak{l}}$ and $l|N$, we may assume that the character $\overline{\varphi}$ ramifies at $\mathfrak{l}$ and is unramified at $\overline{\mathfrak{l}}$, and hence $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)} \cong \overline{\varphi}_{\mathfrak{l}} \oplus \overline{\varphi}_{\overline{\mathfrak{l}}}$. If $l = p$, for the fixed prime $\mathfrak{p}$, we have $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ and $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \cong \overline{\varphi}_{\mathfrak{p}} \oplus \overline{\varphi}_{\overline{\mathfrak{p}}}$. If $(l) = \mathfrak{l}^2$ ramifies in F, we have $\overline{\rho}|_{I_l} \cong 1 \oplus \chi$ for the quadratic character $\chi = \left(\frac{F/\mathbb{Q}}{}\right)$. Here I_l is the inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$.

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

$$\mathcal{D}(A) = \mathcal{D}^{\emptyset}(A) := \{\rho : \mathrm{Gal}(\mathbb{Q}^{(Np)}/\mathbb{Q}) \to \mathrm{GL}_2(A) : \text{a representation satisfying (D1–4)}\}/\cong .$$

Here are the conditions (D1–4):

(D1) $\rho \mod \mathfrak{m}_A \cong \overline{\rho}$ (i.e., there exists $a \in \mathrm{GL}_2(\mathbb{F})$ such that $a\overline{\rho}(\sigma)a^{-1} = (\rho(\sigma) \mod \mathfrak{m}_A)$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$).

(D2) $\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \cong \left(\begin{smallmatrix} \epsilon & * \\ 0 & \delta \end{smallmatrix}\right)$ with δ unramified and $(\delta(\mathrm{Frob}_p) \mod \mathfrak{m}_A) = \overline{\varphi}_{\overline{\mathfrak{p}}}(\mathrm{Frob}_p)$.

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

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

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

$$\mathcal{D}^Q(A) := \{\rho : \mathrm{Gal}(\mathbb{Q}^{(QNp)}/\mathbb{Q}) \to \mathrm{GL}_2(A) : \text{a representation satisfying (D1–4) and (UQ)}\}/\cong,$$

where

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

We may also impose another condition if necessary:

(det) $\det(\rho) = \iota_A \circ \nu_p^k\psi_k$ for the p-adic cyclotomic character ν_p,

and consider the functor

$$\mathcal{D}_{Q,k,\psi_k}(A) := \{\rho : \mathrm{Gal}(\mathbb{Q}^{(QNp)}/\mathbb{Q}) \to \mathrm{GL}_2(A) : \text{a representation satisfying (D1–4) and (det)}\}/\cong .$$

The condition (det) implies that if deformation is modular and satisfies (D1–4), then it is associated to a weight $k+1$ cusp form of Neben character ψ_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 $\mathcal{D}_{k,\psi_k}$ for $\mathcal{D}_{\emptyset,k,\psi_k}$ when Q is empty. For each prime q, we write $\mathcal{D}^q_{Q,k,\psi_k}$ for the deformation functor of $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)}$ satisfying the local condition (D2–4) which applies to q.

By our choice of $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}$, we have $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q})} \cong \begin{pmatrix} \overline{\epsilon}_q & 0 \\ 0 & \overline{\delta}_q \end{pmatrix}$ for two local characters $\overline{\epsilon}_q, \overline{\delta}_q$ for all $q \in Q$. If $\overline{\delta} \neq \overline{\epsilon}$ (i.e., (Rg) and (h4)) and $\overline{\epsilon}_q(\mathrm{Frob}_q) \neq \overline{\delta}_q(\mathrm{Frob}_q)$ for all $q \in Q$, $\mathcal{D}$, $\mathcal{D}^Q$, $\mathcal{D}_{k,\psi_k}$ and $\mathcal{D}_{Q,k,\psi_k}$ are representable by universal objects $(R, \boldsymbol{\rho}) = (R^{\emptyset}, \boldsymbol{\rho}^{\emptyset})$, $(R^Q, \boldsymbol{\rho}^Q)$, $(R_{\emptyset}, \boldsymbol{\rho}_{\emptyset})$ and $(R_Q, \boldsymbol{\rho}_Q)$, 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 $\mathcal{D}$. It is easy to check the deformation functor $\mathcal{D}^{\mathrm{ord}}$ 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 $\det\overline{\rho}$ (h2) and p is unramified in $F/\mathbb{Q}$, if l is a prime factor of N, writing $\rho|_{I_l}^{ss}$ for its semi-simplification of ρ over I_l, we see from (h0) that $(\rho|_{I_l})^{ss} = \epsilon_l \oplus \delta_l$ for two characters ϵ_l and δ_l (of order prime to p) with δ_l unramified and $\epsilon_l \equiv \psi|_{I_l} \mod \mathfrak{m}_A$. Thus by the character $\epsilon_N := \prod_{l|N}\epsilon_l$ of $I_N = \prod_{l|N} I_l$, A is canonically an algebra over the group algebra $W[I_N]$. Then R is given by the maximal residue ring of R^{ord} on which I_N acts by $\psi_{1,N} = \prod_{l|N}\psi|_{I_l}$; so, $R = R^{\mathrm{ord}} \otimes_{W[I_N],\psi_{1,N}} W$, where the tensor product is taken over the algebra homomorphism $W[I_N] \to W$ induced by the character $\psi_{1,N}$. Since $\overline{\rho}$ is an induced representation, $\overline{\rho}|_{I_l}$ is semi-simple and $\overline{\rho}|_{I_l} = \overline{\epsilon}_l \oplus \overline{\delta}_l$ with $\overline{\epsilon}_l = \epsilon_l \mod \mathfrak{m}_A$. Similarly one can show the representability of $\mathcal{D}^Q$ and $\mathcal{D}_{Q,k,\psi_k}$.

Let $\mathbb{T}$ be the local ring of $\mathbf{h} = \mathbf{h}^{\emptyset}$ as in Theorem B whose residual representation is $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}$ with $(U(p) \mod \mathfrak{m}_{\mathbb{T}}) = \overline{\varphi}_{\overline{\mathfrak{p}}}(\mathrm{Frob}_p)$. The ring $\mathbb{T}$ is uniquely determined by (h1–2) as the unramified quotient of $\overline{\rho}$ at each $l|N$ and quotient of $\overline{\rho}$ with specified value at Frob_p at p is unique. Because of the existence of companion forms, if φ is unramified at p, we need to specify the "quotient" character of $\overline{\rho}$ to be given by $\overline{\varphi}_{\overline{\mathfrak{p}}}$ at p.

Since $\overline{\rho}$ is irreducible, by the technique of pseudo-representation, we have a unique representation

$$\rho_{\mathbb{T}} : \mathrm{Gal}(\mathbb{Q}^{(Np)}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$$

up to isomorphisms such that $\mathrm{Tr}(\rho_{\mathbb{T}}(\mathrm{Frob}_l)) = a(l) \in \mathbb{T}$ for all prime $l \nmid Np$ (e.g., [HMI, Proposition 3.49]), where $a(l)$ is the image of $T(l)$ in $\mathbb{T}$. This representation is a deformation of $\overline{\rho}$ in $\mathcal{D}^{\emptyset}(\mathbb{T})$. Thus by universality, we have projections $\pi : R = R^{\emptyset} \to \mathbb{T}$. such that $\pi \circ \boldsymbol{\rho} \cong \rho_{\mathbb{T}}$. Here is the "$R = T$" theorem of Taylor, Wiles ét al specialized to our case:

Theorem 2.1. *Assume* (h0–4). *Then the morphism $\pi : R \to \mathbb{T}$ is an isomorphism, and $\mathbb{T}$ is a local complete intersection over Λ.*

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 $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/M)}$ for $M = \mathbb{Q}[\sqrt{p^*}]$ with $p^* := (-1)^{(p-1)/2}p$. Note that (W) follows from (h3), 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 $\mathbb{T}/I \cong W[[H]]$ (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 $\mathbb{Z}_p[\varphi^-][[\Gamma_-]]/(f^-_{\varphi^-})$ with $f^-_{\varphi^-} \in \mathbb{Z}_p[\varphi^-][[\Gamma_-]]$, it has an injection into the cyclic module with finite cokernel.*

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

$$0 \to \bigoplus_i R dS_i = (S_1, \dots, S_r)/(S_1, \dots, S_r)^2 \to \bigoplus_i R dT_i \to \Omega_{R/\Lambda} \to 0.$$

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

$$0 \to \bigoplus_i \Lambda dS_i \to \bigoplus_i \Lambda dT_i \to \Omega_{R/\Lambda} \otimes_R \Lambda \to 0.$$

By a theorem of Mazur (cf. [MT90], [HT94, §3.3], [HMI, 3.89, 5.33] and [H16, §6.3.6]), under (h0) and (h2), we have $\Omega_{R/\Lambda} \otimes_R \Lambda \cong Y^-(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W$. Thus we get a Λ-free resolution of length 2 of the Iwasawa module, and hence it has homological dimension 1.

Suppose that we have a pseudo-isomorphism $i : Y^-(\varphi^-) \to \mathbb{Z}_p[\varphi^-][[\Gamma_-]]/(f^-_{\varphi^-})$. Then i is an injection as $Y^-(\varphi^-)$ does not have any pseudo-null submodule non-null, and $\mathrm{Coker}(i)$ is finite. □

Since $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$, for $\chi = \left(\frac{F/\mathbb{Q}}{}\right)$, $\overline{\rho} \otimes \chi \cong \overline{\rho}$. By assumption, p splits in F; so, χ is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ for prime factors l of $pN_{F/\mathbb{Q}}(\mathfrak{c})$ and ramified quadratic on $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ for $l|D$. Thus $\rho \mapsto \rho \otimes \chi$ is an automorphism of the functor $\mathcal{D}^Q$ and $\mathcal{D}_{Q,k,\psi_k}$, and $\rho \mapsto \rho \otimes \chi$ induces automorphisms σ_Q of R_Q and R^Q.

We identify R and $\mathbb{T}$ now by Theorem 2.1; in particular, we have an automorphism $\sigma = \sigma_\emptyset \in \mathrm{Aut}(\mathbb{T})$ as above. We could think about $\mathbf{h}_{/W_0}$ defined over a smaller complete discrete valuation ring $W_0 \subset W$ (the smallest possible ring is the ring $\mathbb{Z}_p[\psi]$ generated over $\mathbb{Z}_p$ by the values of ψ). After extending scalar from W_0 to W, we get an involution. We may assume that $W = W(\mathbb{F})$ (the Witt vector ring of $\mathbb{F} = \mathbb{T}/\mathfrak{m}_{\mathbb{T}}$). Since σ fixes W as it is an identity on $\mathbb{F}$, we know that σ preserves $\mathbb{T}$ 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 $\mathbb{Z}_p[\psi]$, we have an involution $\sigma \in \mathrm{Aut}(\mathbb{T}_{/W_0})$ with $\sigma \circ \rho_{\mathbb{T}} \cong \rho_{\mathbb{T}} \otimes \chi$.*

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

We now study the closed subscheme $\mathrm{Spec}(\mathbb{T})^{\mathcal{G}}$ fixed by $\mathcal{G} := \langle \sigma \rangle \subset \mathrm{Aut}(\mathbb{T}_{/\Lambda})$. Consider the functor $\mathcal{D}_F, \mathcal{D}_F^\infty : CL_W \to SETS$ defined by

$$\mathcal{D}_F(A) = \{\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to A^\times | \lambda \equiv \overline{\varphi} \mod \mathfrak{m}_A \text{ has conductor a factor of } \mathfrak{cp}\},$$

and

$$\mathcal{D}_F^\infty(A) = \{\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to A^\times | \lambda \equiv \overline{\varphi} \mod \mathfrak{m}_A \text{ has conductor a factor of } \mathfrak{cp}^\infty\}.$$

Let $F_{\mathfrak{cp}}$ be the maximal abelian p-extension of F inside the ray class field of conductor $\mathfrak{cp}$. Put $C = C_\emptyset := \mathrm{Gal}(F_{\mathfrak{cp}}/F)$. Similarly, write $F_{\mathfrak{cp}^\infty}$ for the maximal p-abelian extension inside the ray class field over F of conductor $\mathfrak{cp}^\infty$. Put $H := \mathrm{Gal}(F_{\mathfrak{cp}^\infty}/F)$. Note that $F_{\mathfrak{cp}^\infty}/F$ is a finite extension if F is real. Then $\mathcal{D}_F$ is represented by $(W[C], \Phi)$ where $\Phi(x) = \varphi(x)x$ for $x \in C$, where φ is the Teichmüller lift of $\overline{\varphi}$ with values in $W^\times$. Similarly $\mathcal{D}_F^\infty$ is represented by $W[[H]] = \varprojlim_{H' \subset H, \mathrm{open}} W[H/H']$. 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 $\mathrm{Gal}(K^-/F)$ of the Galois group of the ray class field K of conductor $(\mathfrak{c} \cap \mathfrak{c}^c)p^\infty$. The present definition is a bit different from the one given there. However, the present H is isomorphic to the earlier $\mathrm{Gal}(K^-/F)$ by sending τ to $\tau^{(1-c)/2} = \sqrt{\tau c \tau^{-1} c^{-1}}$ 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 $\lambda \mapsto \mathrm{Ind}_F^{\mathbb{Q}} \lambda$ induces an isomorphism $\mathcal{D}_F \cong \mathcal{D}_T^{\mathcal{G}}$ and $\mathcal{D}_F^\infty \cong \mathcal{D}^{\mathcal{G}}$, where*

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

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

Proof. Since the proof is essentially the same for the two cases, we only deal with $\mathcal{D}_F^\infty \cong \mathcal{D}^{\mathcal{G}}$. By [DHI98, Lemma 3.2], we have $\rho \otimes \chi \cong \rho$ for $\rho \in \mathcal{D}(A)$ is equivalent to having $\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to A^\times$ such that $\rho \cong \mathrm{Ind}_F^{\mathbb{Q}} \lambda$. We can choose λ so that λ has conductor a factor of $\mathfrak{cp}^\infty$ by (D4) and $C(\det(\rho)) | Np^\infty$. Then λ is unique by (D2–3) and (h0). Thus we get the desired isomorphism. □

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

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

In the proof of Theorem 2.1, Taylor and Wile considered an infinite set $\mathcal{Q}$ made up of a series of finite sets Q of primes $q \equiv 1 \mod p$ outside Np such that $\overline{\rho}(\mathrm{Frob}_q) \sim \begin{pmatrix} \overline{\alpha}_q & 0 \\ 0 & \overline{\beta}_q \end{pmatrix}$ with $\overline{\alpha}_q \neq \overline{\beta}_q \in \mathbb{F}$. Over the inertia group I_q, $\boldsymbol{\rho}^Q$ has the following shape by a theorem of Faltings

$$\boldsymbol{\rho}^Q|_{I_q} = \begin{pmatrix} \boldsymbol{\delta}_q & 0 \\ 0 & \boldsymbol{\delta}'_q \end{pmatrix} \tag{2.1}$$

for characters $\boldsymbol{\delta}_q, \boldsymbol{\delta}'_q : \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \to (R^Q)^\times$ such that $\boldsymbol{\delta}'_q|_{I_q} = \boldsymbol{\delta}_q^{-1}$ and $\boldsymbol{\delta}_q([q, \mathbb{Q}_q]) \equiv \overline{\alpha}_q \mod \mathfrak{m}_{\mathbb{T}}$ (e.g., [MFG, Theorem 3.32 (1)] or [HMI, Theorem 3.75]). Since $\overline{\rho}$ is unramified at q, $\boldsymbol{\delta}_q$ factors through the maximal p-abelian quotient Δ_q of $\mathbb{Z}_q^\times$ by local class field theory, and in fact, it gives an injection $\boldsymbol{\delta}_q : \Delta_q \hookrightarrow R^Q$ as we will see later. Note that $\rho \mapsto \rho \otimes \chi$ is still an automorphism of $\mathcal{D}^Q$ and hence induces an involution $\sigma = \sigma_Q$ of R^Q.

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

$q \in Q^+$, we choose a unique prime factor $\mathfrak{q}|q$ so that $\overline{\varphi}(\mathrm{Frob}_{\mathfrak{q}^c}) = \overline{\alpha}_q$. 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):

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

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

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

$$\rho^Q := \rho_{\mathbb{T}^Q} \otimes \sqrt{\epsilon}^{-1}. \tag{2.2}$$

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

By local class field theory, we identify Δ_q with the p-Sylow subgroup of $\mathbb{Z}_q^\times$. Then the p-abelian group Δ_Q defined above Theorem 1.2 has a canonical factorization: $\Delta_Q := \prod_{q\in Q}\Delta_q$. By Lemma 1.1, the inertia action $W[I_q] \to R^Q \twoheadrightarrow \mathbb{T}^Q$ makes $\mathbb{T}^Q$ free (of finite rank) over $W[\Delta_Q]$, and hence $\Delta_Q \hookrightarrow R^Q$ and $\Delta_Q \hookrightarrow \mathbb{T}^Q$. The character $\boldsymbol{\delta}_q : I_q \to R^{Q,\times}$ (resp. $\boldsymbol{\delta}_q^{-1} : I_q \to R^{Q,\times}$) extends uniquely to $\boldsymbol{\delta}_q : \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \to R^Q$ (resp. $\boldsymbol{\delta}'_q : \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \to R^Q$) so that

$$\boldsymbol{\rho}^Q|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)} = \begin{pmatrix} \boldsymbol{\delta}_q & 0 \\ 0 & \boldsymbol{\delta}'_q \end{pmatrix} \tag{2.3}$$

with $\boldsymbol{\delta}_q(\phi_q) \mod \mathfrak{m}_{R^Q} = \overline{\alpha}_q$ (resp. $\boldsymbol{\delta}'_q(\phi_q) \mod \mathfrak{m}_{R^Q} = \overline{\beta}_q$) for any $\phi_q \in \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ with $\phi_q \mod I_q = \mathrm{Frob}_q$ (e.g., [MFG, Theorem 3.32] or [HMI, Theorem 3.75]).

We choose $\mathfrak{q}|q$ for $q \in Q^+$ so that $\overline{\varphi}(\mathrm{Frob}_{\mathfrak{q}}) = \overline{\alpha}_q$, and define $\mathfrak{Q}_+$ by the product over $q \in Q^+$ of $\mathfrak{q}$ thus chosen. Define the functor $\mathcal{D}^\infty_{F,Q} : CL_W \to SETS$ by

$$\mathcal{D}^\infty_{F,Q}(A) = \{\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to A^\times | \lambda \equiv \overline{\varphi} \mod \mathfrak{m}_A \text{ has conductor a factor of } \mathfrak{Q}_+\mathfrak{c}\mathfrak{p}^\infty\}.$$

Hereafter we simply write Z_Q for Z_{Q^+}. Then plainly $\mathcal{D}^\infty_{F,Q}$ is representable by $W[[Z_Q]] \cong W[[H_Q]]$ in (1.6). Here is a generalization of Corollary 2.5:

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* $R^Q/I^Q \otimes_\Lambda \Lambda/(T) \cong W[C_Q]$ *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 $\mathrm{Spec}(A)$ over a base ring B, the functor $\mathrm{Spec}(A)^G : C \mapsto \mathrm{Spec}(A)(C)^G = \mathrm{Hom}_{B\text{-alg}}(A, C)^G$ sending B-algebras C to the set of fixed points is a closed subscheme of $\mathrm{Spec}(A)$ represented by $A_G := A/\sum_{g\in G} A(g-1)A$; i.e., $\mathrm{Spec}(A)^G = \mathrm{Spec}(A_G)$. Thus we need to prove that the natural transformation $\lambda \mapsto \mathrm{Ind}_F^{\mathbb{Q}}\lambda$ induces an isomorphism $\mathcal{D}^\infty_{F,Q} \cong (\mathcal{D}^Q)^{\mathcal{G}}$, where $(\mathcal{D}^Q)^{\mathcal{G}}(A) = \{\rho \in \mathcal{D}^Q(A) | \rho \otimes \chi \cong \rho\}$. If $\rho \in \mathcal{D}^Q(A)$, we have a unique algebra homomorphism $\phi : R^Q \to A$ such that $\rho \cong \phi \circ \boldsymbol{\rho}^Q$ and $\rho|_{I_q} \cong \begin{pmatrix} \phi\circ\boldsymbol{\delta}|_{I_q} & 0 \\ 0 & (\phi\circ\boldsymbol{\delta}|_{I_q})^{-1} \end{pmatrix}$. This implies $\rho \otimes (\phi\circ\boldsymbol{\delta})|_{I_q} \sim \left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for the global character $\boldsymbol{\delta} : \mathrm{Gal}(\mathbb{Q}(\mu_q)_{q\in Q}/\mathbb{Q}) \to (R^Q)^\times$, and hence its prime-to-p conductor is a factor of N_Q. On the other hand, for $\rho = \mathrm{Ind}_F^{\mathbb{Q}}\lambda$ in $\mathcal{D}^Q(A)$, if ρ ramifies at $q \in Q^-$, the q-conductor of $\rho \otimes (\phi\circ\boldsymbol{\delta})$ is $N_{F/\mathbb{Q}}(q) = q^2$, a contradiction as $q^2 \nmid N_Q$. Thus λ is unramified at $q \in Q^-$, and we may assume $\lambda \in \mathcal{D}^\infty_{F,Q}(A)$. Indeed, among λ, λ_c for $\lambda_c(\sigma) = \lambda(c\sigma c^{-1})$, we can characterize λ uniquely (by (h0)) so that $\lambda \mod \mathfrak{m}_A = \overline{\varphi}$. Thus $\mathcal{D}^\infty_{F,Q}(A) \to (\mathcal{D}^Q)^{\mathcal{G}}(A)$ is an injection. Surjectivity follows from [DHI98, 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 $\mathcal{Q}$ of finite sets Q made of primes $q \equiv 1 \mod p$ outside N. We can choose infinitely many distinct Qs with $\overline{\rho}(\mathrm{Frob}_q)$ for $q \in Q$ having two distinct eigenvalues. Recall $\chi = \left(\frac{F/\mathbb{Q}}{}\right)$ and $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$ as in Theorem B. We split $Q = Q^+ \sqcup Q^-$ so that $Q^{\pm} = \{q \in Q | \chi(q) = \pm 1\}$. By fixing a weight $k \geq 0$ and choosing an eigenvalue $\overline{\alpha}_q$ of $\overline{\rho}(\mathrm{Frob}_q)$ for each $q \in Q$, we have a unique local factor $\mathbb{T}^Q$ (resp. $\mathbb{T}_Q$) of the Hecke algebra $\mathbf{h}^Q$ (resp. $\mathbf{h}_{Q,k,\psi_k}$) as in (1.7), whose residual representation is isomorphic to $\overline{\rho}$ and $U(q) \mod \mathfrak{m}_{\mathbb{T}_Q}$ is the chosen eigenvalue $\overline{\alpha}_q$. 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 $\mathbb{T}_Q$-module M_Q in the definition of the Taylor–Wiles system in [HMI, §3.2.3] and [MFG, §3.2.6]. Here we choose $M_Q := \mathbb{T}_Q$ 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 the $\mathbb{T}_Q$-factor $H_1(X(\Gamma_Q), W) \otimes_{\mathbf{h}^Q} \mathbb{T}_Q$ 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 $h_k(\Gamma_Q, \psi; W)$ has an involution coming from the action of the normalizer of Γ_Q. Taking $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma \equiv \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \mod D^2$ and $\gamma \equiv 1 \mod (N_Q/D)^2$, put $\eta := \gamma \left(\begin{smallmatrix} D & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then η normalizes Γ_Q, and the action of η 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 $l \nmid N_Q$ (see [MFM, (4.6.22), page 168]). Thus the conjugation of η induces on $\mathbb{T}_Q$ an involution compatible with σ_Q under the canonical surjection $R_Q \twoheadrightarrow \mathbb{T}_Q$. Note that $\sigma_Q(U(q)) = -U(q)$ for $q \in Q^-$; so, the role of $\overline{\alpha}_q$ will be played by $-\overline{\alpha}_q = \overline{\beta}_q$. This affects on the inertia action of Δ_q at q by $\delta_q \mapsto \delta_q^{-1}$ for $q \in Q^-$, because the action is normalized by the choice of $\overline{\alpha}_q$ with $\overline{\alpha}_q \equiv U(q) \mod \mathfrak{m}_{\mathbb{T}_Q}$ (see Lemma 3.1 and [HMI, Theorem 3.74]). Since $\mathbb{T}^Q$ is the local component of the big Hecke algebra of tame level Γ_Q whose reduction modulo $t - \gamma^k$ is $\mathbb{T}_Q$, again $\mathbb{T}^Q$ has involution σ_Q induced from η. We write $\mathbb{T}^Q_+$ (resp. $\mathbb{T}^+_Q$) for the fixed subring of $\mathbb{T}^Q$ (resp. $\mathbb{T}_Q$) 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 here 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 Δ_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 $q \in Q$, $\Delta_q/\Delta_q^{p^n}$ for $0 < n \leq m$ is a cyclic group of order p^n. We put $\Delta_n = \Delta_{n,Q} := \prod_{q \in Q} \Delta_q/\Delta_q^{p^n}$. By Lemma 1.1, the inertia action $I_q \twoheadrightarrow \mathbb{Z}_q^\times \to R_Q \twoheadrightarrow \mathbb{T}_Q$ makes $\mathbb{T}_Q$ free of finite rank over $W[\Delta_Q]$. Then they found an infinite sequence $\mathcal{Q} = \{Q_m | m = 1, 2, \dots\}$ of ordered finite sets $Q = Q_m$ of primes q (with $q \equiv 1 \mod p^m$) which produces a projective system:

$$\{((R_{n,m(n)}, \alpha = \alpha_n), \widetilde{R}_{n,m(n)}, (f_1 = f_1^{(n)}, \dots, f_r = f_r^{(n)}))\}_n \tag{3.1}$$

made of the following objects:

(1) $R_{n,m} := \mathbb{T}_{Q_m}/(p^n, \delta_q^{p^n} - 1)_{q \in Q_m} \mathbb{T}_{Q_m}$ for each $0 < n \leq m$. 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 $\mathrm{End}_{W[\Delta_n]}(M_{n,m})$ for $M_{n,m} := M_{Q_m}/(p^n, \delta_q^{p^n} - 1)_{q \in Q_m} M_{Q_m}$, but by our choice $M_Q = \mathbb{T}_Q$, the image is identical to $\mathbb{T}_{Q_m}/(p^n, \delta_q^{p^n} - 1)_{q \in Q_m} \mathbb{T}_{Q_m}$. An important point is that $R_{n,m}$ is a finite ring whose order is bounded independent of m (by (Q0) below).

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

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

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

Thus for each $n > 0$, the projection $\pi_n^{n+1} : R_{n+1,m(n+1)} \to R_{n,m(n)}$ is compatible with all the data in the system (3.1) (the meaning of this compatibility is specified below) and induces the projection $\widetilde{\pi}_n^{n+1} : \widetilde{R}_{n+1,m(n+1)} \to \widetilde{R}_{n,m(n)}$. In [HMI, page 191], there is one more datum of an algebra homomorphism $\beta : R_{n,m} \to \mathrm{End}_{\mathbb{T}_{Q_m}}(M_{n,m}) \subset \mathrm{End}_{W[\Delta_n]}(M_{n,m})$. Since we have chosen M_Q to be $\mathbb{T}_Q$, $M_{n,m}$ is by definition $R_{n,m}$; so, β 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] taking $M_{Q_m} := \mathbb{T}_{Q_m}$).

(Q1) $|Q_m| = r \geq \dim_{\mathbb{F}} \mathcal{D}_{Q_m,k,\psi_k}(\mathbb{F}[\epsilon])$ for r independent of m [HMI, Propositions 3.29 and 3.33], where ϵ is the dual number with $\epsilon^2 = 0$. (Note that $\dim_{\mathbb{F}} \mathcal{D}_{Q_m,k,\psi_k}(\mathbb{F}[\epsilon])$ is the minimal number of generators of R_{Q_m} over W.)

(Q2) $q \equiv 1 \mod p^m$ and $\overline{\rho}(\mathrm{Frob}_q) \sim \begin{pmatrix} \overline{\alpha}_q & 0 \\ 0 & \overline{\beta}_q \end{pmatrix}$ with $\overline{\alpha}_q \neq \overline{\beta}_q \in \mathbb{F}$ if $q \in Q_m$ (so, $|\Delta_q| =: p^{e_q} \geq p^m$). Actually as we will see later in Lemma 3.2, we can impose a slightly stronger condition: $q \equiv 1 \mod Cp^m$ for $C = N_{F/\mathbb{Q}}(\mathfrak{c})$.

(Q3) The set $Q_m = \{q_1, \ldots, q_r\}$ is ordered so that
- $\Delta_{q_j} \subset \Delta_{Q_m}$ is identified with $\mathbb{Z}/p^{e_{q_j}}\mathbb{Z}$ by $\delta_{q_j} \mapsto 1$; so, $\Delta_n = \Delta_{n,Q_{m(n)}} = (\mathbb{Z}/p^n\mathbb{Z})^{Q_{m(n)}}$,
- $\Delta_n = (\mathbb{Z}/p^n\mathbb{Z})^{Q_{m(n)}}$ is identified with $\Delta_{n+1}/\Delta_{n+1}^{p^n} = ((\mathbb{Z}/p^{n+1}\mathbb{Z})/p^n(\mathbb{Z}/p^{n+1}\mathbb{Z}))^{Q_{m(n)}}$,
- the diagram

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

is commutative for all $n > 0$ (and by (Q0), α_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 $\pi_n^{n+1}(f_j^{(n+1)}) = f_j^{(n)}$ for each $j = 1, 2, \ldots, r$.

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

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

(Q7) $R_\infty/(S_1, \ldots, S_r) \cong \varprojlim_n \widetilde{R}_{n,m(n)} \cong R_\emptyset \cong \mathbb{T}_\emptyset$, where $R_\emptyset$ is the universal deformation ring for the deformation functor $\mathcal{D}_{\emptyset,k,\psi_k}$ and $\mathbb{T}_\emptyset$ is the local factor of the Hecke algebra $\mathbf{h}_{\emptyset,k,\psi_k}$ whose residual representation is isomorphic to $\overline{\rho}$.

(Q8) We have $R_{Q_m} \cong \mathbb{T}_{Q_m}$ by the canonical morphism, and $R_{Q_m} \cong R_\infty/\mathfrak{A}_{Q_m}R_\infty$ for the ideal $\mathfrak{A}_{Q_m} := ((1 + S_j)^{|\Delta_{q_j}|} - 1)_{j=1,2,\ldots r}$ of $W[[S_1, \ldots, S_r]]$ is a local complete intersection.

All the above facts (Q0–8) follows, for example, from [HMI, Theorem 3.23] and its proof. Since $m(n)$ is determined by n, if confusion is unlikely, we simply drop "$m(n)$" from the notation (so, we often write R_n for $R_{n,m(n)}$). For $q \in Q = Q_m$, we write S_q for the one of the variables in $\{S_1, \ldots, S_r\}$ in (Q6) corresponding to q.

Lemma 3.1. *Let $\chi := \left(\frac{F/\mathbb{Q}}{}\right)$ as before. Then the involution σ_{Q_m} on $\mathbb{T}_{Q_m}$ 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 $\mathbb{T}_{Q_m}$ is stable under σ_{Q_m}, and the involution σ_{Q_m} induces an involution $\sigma = \sigma_n$ of $R_n = R_{n,m}$.*

Proof. For each $q \in Q$, by (2.1), the restriction of $\boldsymbol{\rho}^Q$ to the inertia group $I_q \subset \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ has the form $\begin{pmatrix} \boldsymbol{\delta}_q & 0 \\ 0 & \boldsymbol{\delta}_q^{-1} \end{pmatrix}$ and the choice of the eigenvalue $\overline{\alpha}_q$ determines the character $\boldsymbol{\delta}_q$ (i.e., $\overline{\alpha}_q$-eigenspace of $\overline{\rho}(\mathrm{Frob}_q)$ is the image of $\boldsymbol{\delta}_q^{-1}$-eigenspace in $\overline{\rho}$ by (2.3); see also [MFG, Theorem 3.32 and its proof] or [HMI, Theorem 3.75]). By tensoring χ, $\overline{\alpha}_q$ is transformed to $\chi(q)\overline{\alpha}_q = \overline{\beta}_q$, and hence $\boldsymbol{\delta}_q$ will be transformed to $\boldsymbol{\delta}_q^{\chi(q)}$ under σ_{Q_m}. Thus, we get the desired result as the canonical morphism $R_{Q_m} \to \mathbb{T}_{Q_m}$ is $W[\Delta_{Q_m}]$-linear.

Since $\delta_q^{-p^n} - 1 = -\delta_q^{-p^n}(\delta_q^{p^n} - 1)$, the ideal $(p^n, \delta_q^{p^n} - 1)_{q \in Q_m}$ of $\mathbb{T}_{Q_m}$ is stable under σ_{Q_m}. Therefore $\sigma_{Q_m} \in \mathrm{Aut}(\mathbb{T}_{Q_m})$ induces an involution σ_n on $R_n = R_{n,m} = \mathbb{T}_{Q_m}/(p^n, \delta_q^{p^n} - 1)_{q \in Q_m}$. □

We recall the way Wiles chose the sets $\mathcal{Q}$ 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 $\overline{\rho}$ acting on $\mathfrak{sl}_2(\mathbb{F})$ by conjugation, and put Ad^* for the $\mathbb{F}$-contragredient. Then $Ad^*(1)$ is one time Tate twist of Ad^*. Note that $Ad^* \cong Ad$ by the trace pairing as p is odd. Let Q be a finite set of primes, and consider

$$\beta_Q : H^1(\mathbb{Q}^{(QNp)}/\mathbb{Q}, Ad) \to \prod_{q\in Q} H^1(\mathbb{Q}_q, Ad),$$
$$\beta'_Q : H^1(\mathbb{Q}^{(QNp)}/\mathbb{Q}, Ad^*(1)) \to \prod_{q\in Q} H^1(\mathbb{Q}_q, Ad^*(1)).$$

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 $K_1 = \overline{\mathbb{Q}}^{\mathrm{Ker}\,Ad}$ (the splitting field of $Ad = Ad(\overline{\rho})$). Since $Ad \cong \overline{\chi} \oplus \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$, we have $K_1 = F(\varphi^-)$.

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

$$f_x : \mathrm{Gal}(\mathbb{Q}^{(QNp)}/K_1(\mu_p)) \to Ad^*(1) \in \mathrm{Hom}_{\mathrm{Gal}(K_1(\mu_p)/\mathbb{Q})}(\mathrm{Gal}(\mathbb{Q}^{(QNp)}/K_1(\mu_p), Ad^*(1))$$
$$f_y : \mathrm{Gal}(\mathbb{Q}^{(QNp)}/K_1) \to Ad \in \mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathrm{Gal}(\mathbb{Q}^{(QNp)}/K_1, Ad)$$

for the restriction of the cocycle representing x *and* y *to* $\mathrm{Gal}(\mathbb{Q}^{(QNp)}/K_1(\mu_p))$ *and* $\mathrm{Gal}(\mathbb{Q}^{(QNp)}/K_1)$, *respectively. Let* $\widetilde{\rho}$ *be the composite of* $\overline{\rho}$ *with the projection* $\mathrm{GL}_2(\mathbb{F}) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F})$, *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* $\mathrm{Gal}(\mathbb{Q}^{(Np)}/K_1(\mu_p))$ *(resp.* $\mathrm{Gal}(\mathbb{Q}^{(Np)}/K_1)$*), and there exists* $\sigma_? \in \mathrm{Gal}(\mathbb{Q}^{(Np)}/\mathbb{Q})$ *for* $? = x, y$ *such that*

1. $\widetilde{\rho}(\sigma_?) \neq 1$ *(so,* $Ad(\sigma_?) \neq 1$*),*
2. $\sigma_?$ *fixes* $\mathbb{Q}(\mu_{Cp^m})$ *for an integer* $m > 0$,
3. $f_?(\sigma_?^a) \neq 0$ *for* $a := \mathrm{ord}(\widetilde{\rho}(\sigma_?)) = \mathrm{ord}(Ad(\sigma_?))$.

We only use the result for x in this paper. 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 $\overline{\rho}$. Since the statement is about the cohomology group of Ad (and $Ad^*(1)$), we can replace K_0 in his argument by K_1. We note also $\mathrm{Ker}(Ad(\overline{\rho})) = \mathrm{Ker}(\widetilde{\rho})$ as the kernel of the adjoint representation: $\mathrm{GL}(2) \to \mathrm{GL}_3$ is the center of GL_2 (so it factors through PGL_2).

Proof. Since $x \in \mathrm{Ker}(\beta'_Q)$, f_x is unramified at $q \in Q$; so, f_x factors through $\mathrm{Gal}(\mathbb{Q}^{(Np)}/K_1(\mu_p))$.

We have two possibilities of $F' := K_1 \cap \mathbb{Q}(\mu_{Cp^m})$; 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 $\mathrm{ord}(\overline{\varphi}^-)$ is odd > 1) or a composite FF' of the quadratic extensions F and F' over $\mathbb{Q}$ (if $\mathrm{ord}(\overline{\varphi}^-)$ is even $2n > 2$). If $\overline{\varphi}^-$ has odd order, $F' = \mathbb{Q}(\mu_{Cp^m}) \cap K^1 = \mathbb{Q}$ 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 $\mathrm{ord}(\overline{\varphi}^-) = 2n > 3$. Let $\mathcal{D} := \mathrm{Gal}(K_1/\mathbb{Q})$ and $\mathcal{C} := \mathrm{Gal}(K_1/F)$. Then $\mathcal{C}$ is a cyclic group of order $2n$. Pick a generator $g \in \mathcal{C}$. Then $\mathcal{D} = \mathcal{C} \sqcup \mathcal{C}c$ for complex conjugation c, and we have a characterization $\mathcal{C}c = \{\tau \in \mathcal{D} | \tau g \tau^{-1} = g^{-1}, \tau^2 = 1\}$. For the derived group $\mathcal{D}'$ of $\mathcal{D}$, we have $\mathcal{D}^{ab} := \mathcal{D}/\mathcal{D}' \cong (\mathbb{Z}/2\mathbb{Z})^2$. We have $K_1^{\mathcal{D}'} = FF'$, and $\mathrm{Gal}(K_1/F')$ is equal to $\mathcal{C}^2 \rtimes \langle c \rangle$ (a dihedral group of order $2n$). If $n > 2$ (so, $2n > 4$), $\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$ restricted to $\mathrm{Gal}(K_1/F')$ is still irreducible isomorphic to $\mathrm{Ind}_{F'F}^{F'} \overline{\varphi}^-$. If $n = 2$, F' is a unique quadratic extension in $K_1^{\mathcal{D}'}$ 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 σ_x in $\mathcal{C}^2 \rtimes \langle c \rangle$ because $Ad = \overline{\chi} \oplus \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$.

Let $M_x := \overline{\mathbb{Q}}^{\mathrm{Ker}(f_x)}$. Then $Y := \mathrm{Gal}(M_x/K_1(\mu_p))$ is embedded into $Ad^*(1)$ by f_x and f_x is equivariant under the action of $\mathrm{Gal}(K_1(\mu_p)/\mathbb{Q})$ which acts on Y by conjugation. Since $Ad = \overline{\chi} \oplus \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$, we have two irreducible invariant subspaces $X \subset Ad^*(1)$: $X = \overline{\chi\omega}$ and $\mathrm{Ind}_F^{\mathbb{Q}}(\overline{\varphi}^- \overline{\omega})$. Thus $f_x(Y)$ contains one of X as above. By (1), we have $\overline{\rho}(\sigma) \sim \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ with $\alpha \neq \beta$. By (2), we have $\alpha\beta = \det(\overline{\rho})|_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{Cp^m}))}(\sigma) = \overline{\chi\omega}^{k_0}(\sigma) = \overline{\chi}(\sigma)$ for some k_0 (since $\det(\overline{\rho})|_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{Cp^m}))}$ is equal to $\overline{\chi}$ up to a power of $\overline{\omega}$). The eigenvalue of $Ad^*(1)(\sigma) = Ad(\sigma)$ is therefore $\overline{\chi}(\sigma)\alpha^2, 1, \overline{\chi}(\sigma)\alpha^{-2}$. By (1), we have $\alpha^2 \neq \overline{\chi}(\sigma)$.

If $f_x(Y) \supset X$, we claim to find σ satisfying (1) and (2) and having eigenvalue 1 in X. If $X = \overline{\chi\omega}$, the splitting field of X is $F(\mu_p)$. Note that $F(\mu_{Cp^m})$ is abelian over $\mathbb{Q}$. Thus choosing σ fixing

$F(\mu_{Cp^m})$ with $\sigma \in \mathcal{C}^2|_{K_1}$ and having $\mathrm{ord}(\overline{\varphi}^-(\sigma)) \geq \mathrm{ord}((\overline{\varphi}^-)^2) = |\mathcal{C}^2| \geq 2$, we have σ having eigenvalue 1 on $X = \overline{\chi\omega}$.

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

Since $f_x(Y) \supset X[1] = \{v \in X | Ad(\sigma)(v) = v\}$, we can find $1 \neq \tau \in Y$ such that $f_x(\tau) \in X[1]$; so, $f_x(\tau) \neq 0$. Thus τ commutes with $\sigma \in \mathrm{Gal}(M_x/\mathbb{Q})$. This shows $(\sigma\tau)^a = \sigma^a\tau^a$, and $f_x((\sigma\tau)^a) = f(\sigma^a\tau^a) = af_x(\tau) + f(\sigma^a)$. Since $af_x(\tau) \neq 0$, at least one of $f(\sigma^a\tau^a)$ and $f(\sigma^a)$ is non-zero. Then $\sigma_x = \sigma$ or $\sigma_x := \sigma\tau$ 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 $Y := \mathrm{Gal}(M_y/K_1)$. Since $Ad = \overline{\chi} \oplus \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$, for $X = \overline{\chi}$ or $\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$, we have $f_y(Y) \supset X$. Then we argue in exactly the same way as above and find σ_y with the required property. □

Let $Q = \emptyset$ and choose a basis $\{x\}_x$ over $\mathbb{F}$ of the "dual" Selmer group $\mathrm{Sel}_{\emptyset}^{\perp}(Ad^*(1))$ inside $H^1(\mathbb{Q}^{(Np)}/\mathbb{Q}, Ad^*(1))$ (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 $\mathrm{Frob}_q = \sigma_x$ 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 notation be as in* Lemma 3.2 *and its proof. If* $0 \neq f_x(Y) \subset \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^- \overline{\omega}$, *the field automorphism* σ *in* Lemma 3.2 *satisfies* $\left(\frac{F/\mathbb{Q}}{\sigma}\right) = -1$. *Otherwise, we can choose* σ *so that* $\left(\frac{F/\mathbb{Q}}{\sigma}\right) = 1$.

Proof. In this case, we can have $X[1] \subset \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^- \overline{\omega} \neq 0$; so, $Ad(\sigma)(1) = Ad(\sigma)$ (as $\omega(\sigma) = 1$) must have two distinct eigenvalues $\{1, -1\}$ on $\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$, which implies $\left(\frac{F/\mathbb{Q}}{\sigma}\right) = -1$ as $Ad(\sigma)$ has to have eigenvalues -1 with multiplicity 2. □

Definition 3.4. Let $\mathcal{Y}^-$ (resp. $\mathcal{Y}^-_{sp}$, $\mathcal{Y}^-_{tsp}$) be the Galois group over $K^-_{\emptyset}F(\phi)$ of the maximal p-abelian extension $L_{\emptyset}$ (resp. $L^{sp}_{\emptyset}$, $L^{tsp}_{\emptyset}$) of $K^-_{\emptyset}F(\phi)$ unramified outside $\mathfrak{p}$ (resp. totally split at $\mathfrak{p}^c$ and unramified outside $\mathfrak{p}$, totally splits at all prime factors of $\mathfrak{p}^cN$ and unramified outside $\mathfrak{p}$). Regarding $\mathrm{Gal}(F(\phi)/F)$ as a subgroup of $\mathrm{Gal}(K_{\emptyset}F(\phi)/F) \cong \mathrm{Gal}(F(\phi)/F) \times \mathrm{Gal}(K_{\emptyset}/F)$, define, for $? = sp, tsp$,

$$\mathcal{Y}^-(\phi) := \mathcal{Y}^- \otimes_{\mathbb{Z}_p[\mathrm{Gal}(F(\phi)/F)],\phi} \mathbb{Z}_p(\phi) \text{ and } \mathcal{Y}^-_?(\phi) := \mathcal{Y}^-_? \otimes_{\mathbb{Z}_p[\mathrm{Gal}(F(\phi)/F)],\phi} \mathbb{Z}_p(\phi).$$

More generally write $\mathcal{Y}^-_Q$ for the Galois group over $K^-_QF(\phi)$ of the maximal p-abelian extension L_Q of $K^-_QF(\phi)$ unramified outside $\mathfrak{p}$ and Q. Then define $\mathcal{Y}^-_Q(\phi) := \mathcal{Y}^-_Q \otimes_{\mathbb{Z}_p[\mathrm{Gal}(F(\phi)/F)],\phi} \mathbb{Z}_p(\phi)$.

Thus we have a natural restriction map $\mathcal{Y}^- \twoheadrightarrow Y^-$ which is an isomorphism if $p \nmid h_F$. In particular $\mathcal{Y}^-(\phi) = Y^-(\phi)$ if $p \nmid h_F$. As we will see later in Proposition 7.1, for example if $\phi = \varphi^-\omega$, we can replace the requirement "total splitting at $\mathfrak{p}^c$" (and unramifiedness at N) in the above definition by a stronger condition "total splitting at all prime factors in $\mathfrak{p}^cN$" and the resulting Iwasawa module is the same (i.e., $\mathcal{Y}^-(\varphi^-\omega) = \mathcal{Y}^-_{sp}(\varphi^-\omega) = \mathcal{Y}^-_{tsp}(\varphi^-\omega)$). This is important because the dual Selmer cocycle has to be not just unramified at $\mathfrak{p}^cN$ but trivial at $\mathfrak{p}^cN$. Proposition 7.1 also shows $\mathcal{Y}^-(\varphi^-) = \mathcal{Y}^-_{sp}(\varphi^-)$, and we can replace "total splitting at $\mathfrak{p}^c$" just by the "unramifiedness at $\mathfrak{p}^c$".

Let $\mathcal{D}_Q := \mathcal{D}_{Q,k,\psi_k}$ and $\mathcal{D}^l_Q$ for the corresponding local functor at a prime $l|N_Qp$ defined below (det) in Section 2. For a prime $l|Np$ or $l \in Q$, regard $\mathcal{D}^l_Q(\mathbb{F}[\epsilon])$ for the dual number ϵ as a subspace of $H^1(\mathbb{Q}_l, Ad)$ in the standard way: For $\rho \in \mathcal{D}^l_{\emptyset}(\mathbb{F}[\epsilon])$, we write $\rho\overline{\rho}^{-1} = 1 + \epsilon u_\rho$. Then u_ρ is the cocycle with values in $\mathfrak{sl}_2(\mathbb{F}) = Ad$. Thus we have the orthogonal complement $\mathcal{D}^l_Q(\mathbb{F}[\epsilon])^\perp \subset H^1(\mathbb{Q}_l, Ad^*(1))$ under Tate local duality. We recall the definition of the Selmer group giving the global tangent space $\mathcal{D}_Q(\mathbb{F}[\epsilon])$ and its dual from the work of Wiles and Taylor–Wiles (e.g., [HMI, §3.2.4]):

$$\mathrm{Sel}_Q(Ad) := \mathrm{Ker}(H^1(\mathbb{Q}^{(QNp)}/\mathbb{Q}, Ad) \to \prod_{l|Np} H^1(\mathbb{Q}_l, Ad)/\mathcal{D}^l_Q(\mathbb{F}[\epsilon])) \ (\cong \mathcal{D}_Q(\mathbb{F}[\epsilon])),$$

$$\mathrm{Sel}^\perp_Q(Ad^*(1)) := \mathrm{Ker}(H^1(\mathbb{Q}^{(QNp)}/\mathbb{Q}, Ad^*(1)) \to \prod_{l|Np} \frac{H^1(\mathbb{Q}_l, Ad^*(1))}{\mathcal{D}^l_Q(\mathbb{F}[\epsilon])^\perp} \times \prod_{q \in Q} H^1(\mathbb{Q}_q, Ad^*(1))). \tag{3.2}$$

Remark 3.5. As noticed in [CV03, Theorem 3.1], the decomposition $Ad = \overline{\chi} \oplus \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$ for $\overline{\chi} := (\chi \bmod p)$, $\mathrm{Sel}_Q(Ad)$ (resp. $\mathrm{Sel}_Q^{\perp}(Ad^*(1))$) induces the direct sum of the Selmer groups $\mathrm{Sel}_Q(\overline{\chi})$ (resp. $\mathrm{Sel}_Q^{\perp}(\overline{\chi\omega})$) and $\mathrm{Sel}_Q(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-)$ (resp. $\mathrm{Sel}_Q^{\perp}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^- \overline{\omega})$).

To prove the direct sum decomposition in Remark 3.5, we need to decompose $\mathcal{D}_Q^l(\mathbb{F}[\epsilon])^{\perp}$ as in (3.3) below (which is equivalent to the decomposition of the original $\mathcal{D}_Q^l(\mathbb{F}[\epsilon])$). We consider $\mathrm{Sel}_Q^{\perp}(Ad^*(1))$ (whose decomposition as above is equivalent to (3.3) below). Then $\mathcal{D}_Q^p(\mathbb{F}[\epsilon])$ is made of classes of cocycles such that $u_\rho|_{I_p}$ is upper nilpotent and $u_\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q})}$ is upper triangular. Thus we confirm for $l = p$ that

$$\mathcal{D}_Q^l(\mathbb{F}[\epsilon])^{\perp} = (\mathcal{D}_Q^l(\mathbb{F}[\epsilon])^{\perp} \cap H^1(\mathbb{Q}_l, \overline{\chi\omega})) \oplus (\mathcal{D}_Q^l(\mathbb{F}[\epsilon])^{\perp} \cap H^1(\mathbb{Q}_l, \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^- \overline{\omega})), \tag{3.3}$$

and $\mathcal{D}_Q^p(\mathbb{F}[\epsilon])^{\perp} \cap H^1(\mathbb{Q}_p, \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^- \overline{\omega})$ is made of upper nilpotent matrices in $Ad^*(1)$ (since $\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-(1)$ is the direct sum of the upper nilpotent Lie algebra and the lower nilpotent Lie algebra). Therefore $\mathcal{D}_Q^p(\mathbb{F}[\epsilon])^{\perp} \cap H^1(\mathbb{Q}_p, \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^- \overline{\omega})$ is the direct factor $H^1(F_{\mathfrak{p}}, \overline{\varphi}^- \overline{\omega})$ of

$$H^1(F_{\mathfrak{p}}, \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^- \overline{\omega}) = H^1(F_{\mathfrak{p}}, \overline{\varphi}^- \overline{\omega}) \oplus H^1(F_{\mathfrak{p}}, \overline{\varphi}^{-\,-1} \overline{\omega}),$$

where $\overline{\varphi}_c^-(\tau) = \overline{\varphi}^-(c\tau c^{-1}) = (\overline{\varphi}^-)^{-1}(\tau)$ for complex conjugation c. This implies

(3.4) a cocycle u giving a class in $\mathrm{Sel}_Q^{\perp}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^- \overline{\omega})$ is possibly ramified at $\mathfrak{p}$ but trivial at $\mathfrak{p}^c N$.

We now compute $\mathcal{D}_Q^p(\mathbb{F}[\epsilon])^{\perp} \cap H^1(\mathbb{Q}_p, \overline{\chi\omega})$. Since $\overline{\chi}$ is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, we have $H^1(\mathbb{Q}_p, \overline{\chi\omega}) = H^1(\mathbb{Q}_p, \mu_p) \cong \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p$ by Kummer theory. Since $\overline{\omega}$ ramifies at p, we have $H^0(I_p, \overline{\chi\omega}) = 0$, and by inflation and restriction sequence, we have an exact sequence:

$$0 = H^1(\mathrm{Frob}_p^{\widehat{\mathbb{Z}}}, H^0(I_p, \overline{\chi\omega})) \to H^1(\mathbb{Q}_p, \overline{\chi\omega}) \to H^1(I_p, \mu_p)^{\mathrm{Frob}_p = 1} \to H^2(\mathrm{Frob}_p^{\widehat{\mathbb{Z}}}, H^0(I_p, \overline{\chi\omega})) = 0.$$

This implies all non-zero classes in $H^1(\mathbb{Q}_p, \overline{\chi\omega})$ is ramified.

We study the cohomology group $H^1(\mathbb{Q}_p, \overline{\chi})$ to determine $\mathcal{D}_Q^p(\mathbb{F}[\epsilon]) \cap H^1(\mathbb{Q}_p, \overline{\chi})$. Since $\overline{\chi}$ is unramified and $\widehat{\mathbb{Z}}$ has cohomological dimension 1, we have a commutative diagram with exact rows:

$$\begin{tikzcd}
H^1(\mathrm{Frob}_p^{\widehat{\mathbb{Z}}}, \overline{\chi}) \arrow[r, "\hookrightarrow"] \arrow[d, "\wr"'] & H^1(\mathbb{Q}_p, \overline{\chi}) \arrow[r, "\twoheadrightarrow"] \arrow[d, "\wr"'] & H^1(I_p, \overline{\chi})^{\mathrm{Frob}_p = 1} \arrow[d, "\wr"'] \\
\mathrm{Hom}(\mathrm{Frob}_p^{\widehat{\mathbb{Z}}}, \mathbb{F}) \arrow[r, "\hookrightarrow"'] & \mathrm{Hom}(\mathbb{Q}_p^\times, \mathbb{F}) \arrow[r, "\twoheadrightarrow"'] & \mathrm{Hom}(\mathbb{Z}_p^\times, \mathbb{F})^{\mathrm{Frob}_p = 1}.
\end{tikzcd}$$

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

$$\mathcal{D}_Q^p(\mathbb{F}[\epsilon])^{\perp} \cap H^1(\mathbb{Q}_p, \overline{\chi\omega}) = H^1(I_p, \overline{\omega})^{\mathrm{Frob}_p = 1} = (\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^p) \otimes_{\mathbb{Z}} \mathbb{F}.$$

So, it is ramified, and hence

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

For a prime $l | N_{F/\mathbb{Q}}(\mathfrak{c})$, $Ad \cong \overline{\chi} \oplus \overline{\varphi}^- \oplus (\overline{\varphi}^-)^{-1}$ and $Ad^*(1) \cong \overline{\chi\omega} \oplus \overline{\varphi}^- \overline{\omega} \oplus (\overline{\varphi}^-)^{-1} \overline{\omega}$ over $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ (as $F_l = \mathbb{Q}_l \oplus \mathbb{Q}_l$). Write $\overline{\varphi}'$ (resp. $\overline{\chi}'$) for $\overline{\varphi}^-$ and $\overline{\varphi}^- \overline{\omega}$ (resp. for $\overline{\chi}$ and $\overline{\chi\omega}$) in order to treat the two cases at the same time. We normalize Ad so that the character $\overline{\chi}$ is realized on $\mathbb{F}\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\overline{\varphi}^-$ appears on the upper nilpotent matrices and $(\overline{\varphi}^-)^{-1}$ acts on lower nilpotent matrices, and we also normalize $Ad^*(1)$ accordingly. By (h3), $\overline{\varphi}^-$ has ordr ≥ 3, and via this action, the upper nilpotent subspace is distinguished from lower nilpotent subspace. Since $H^0(I_l, \overline{\varphi}') = 0$, we have an isomorphism $H^1(\mathbb{Q}_l, \overline{\varphi}') \cong H^1(I_l, \overline{\varphi}')^{\mathrm{Frob}_l = 1}$ by the restriction map. Since $\overline{\omega}$ is unramified at l, we have $\overline{\varphi}^- \overline{\omega}|_{I_l} = \overline{\varphi}^-|_{I_l}$. We have the following inflation-restriction exact sequence for $K := \mathrm{Ker}(\overline{\varphi}'|_{I_l})$:

$$0 \to H^1(\overline{\varphi}'(I_l), \overline{\varphi}') \to H^1(I_l, \overline{\varphi}') \to \mathrm{Hom}_{\overline{\varphi}'(I_l)}(K, \overline{\varphi}') \to H^2(\overline{\varphi}'(I_l), \overline{\varphi}').$$

Here $\overline{g} \in \overline{\varphi}'(I_l)$ acts on K by $k \mapsto \overline{g}(k) := gkg^{-1}$ taking a lift $g \in I_l$ of $\overline{g}$, and for $\phi : K \to \mathbb{F}$, $\phi \in \mathrm{Hom}_{\overline{\varphi}'(I_l)}(K, \overline{\varphi}')$ implies $\phi(\overline{g}(k)) = \overline{\varphi}'(g)\phi(k)$. Since ϕ has order a factor of p, ϕ factors through the tame quotient of K^t of K, which is abelian; so, the tame quotient K^t embeds into the tame quotient I_l^t of I_l. Thus $\overline{g}(k) = k$ on K^t. Since $\overline{\varphi}'(I_l)$ has order prime to p, we have $H^j(\overline{\varphi}'(I_l), \overline{\varphi}') = 0$ for all $j > 0$. Since φ' is non-trivial, we have $\phi(k) = \phi(\overline{g}(k)) = \overline{\varphi}'(g)\phi(k)$ for some $g \in I_l$ with $\overline{\varphi}'(g) \neq 1$; so, we conclude $H^1(I_l, \overline{\varphi}') \cong \mathrm{Hom}_{\overline{\varphi}'(I_l)}(K, \overline{\varphi}')$ vanishes. Thus we get $H^1(\mathbb{Q}_l, Ad) = \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l), \mathbb{F}\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)) \cong \mathbb{F}$ and $H^1(\mathbb{Q}_l, Ad^*(1)) = H^1(\mathbb{Q}_l, \mathbb{F}\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right) \otimes \overline{\omega}) = H^1(\mathrm{Frob}_l^{\widehat{\mathbb{Z}}}, \mathbb{F}\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right) \otimes \overline{\omega}) \cong \mathbb{F}$, which is the Tate dual of $H^1(\mathbb{Q}_l, Ad)$. This tell us that the Selmer cocycle u_ρ giving a class in $\mathcal{D}^l_Q(\mathbb{F}[\epsilon])$ for Ad has values in $\mathbb{F}\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ over $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ and is unramified. In other words, we have $\mathcal{D}^l_Q(\mathbb{F}[\epsilon]) = H^1(\mathbb{Q}_l, Ad)$; so, again the direct sum decomposition (3.3) holds, and we find $\mathcal{D}^l_Q(\mathbb{F}[\epsilon])^\perp = H^1(\mathbb{Q}_l, Ad)^\perp = 0$.

At $l|D$, $\overline{\varphi}^-|_{\mathrm{Gal}(\overline{\mathbb{Q}}_l/F_l)}$ is trivial. Thus we have $Ad \cong \overline{\chi} \oplus \mathrm{Ind}_F^{\mathbb{Q}} \overline{\mathbf{1}} \cong \overline{\chi} \oplus \mathbf{1} \oplus \overline{\chi}$ over $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$. The first factor $\overline{\chi}$ is realized in $\mathbb{F}\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$, the last factor $\overline{\chi}$ is realized on $\mathbb{F}\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$ and the middle factor $\mathbf{1}$ is realized on $Ad^{I_l} = \mathbb{F}\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$. Arguing in the same way as we showed $H^1(\mathbb{Q}_l, \overline{\varphi}^-) = 0$, replacing $\overline{\varphi}^-$ by $\overline{\chi}$, we find that $H^1(\mathbb{Q}_l, \overline{\chi}) = 0$. We have $H^1(\mathbb{Q}_l, \mathrm{Ind}_F^{\mathbb{Q}} \mathbf{1}) = H^1(F_l, \mathbb{F}) = \mathrm{Hom}(F_l^\times, \mathbb{F}) \cong \mathbb{F}$ by (h0). Thus the cohomology classes in $H^1(\mathbb{Q}_l, Ad)$ is represented by cocycles with values in $\mathbb{F}\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$. Therefore we get $H^1(\mathbb{Q}_l, Ad) = \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}_l/F_l), \mathbb{F}\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right))$, and $\rho \in \mathcal{D}^l_Q(\mathbb{F}[\epsilon])$ if and only if u_ρ has image in $Ad(\mathbb{F})^{I_l} = \mathbb{F}\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$ and is unramified. In particular, $\mathcal{D}^l_Q(\mathbb{F}[\epsilon]) = H^1(\mathbb{Q}_l, Ad) \cong \mathbb{F}$.

By the same argument applied to $Ad^*(1)|_{\mathrm{Gal}(\mathbb{Q}_l/\mathbb{Q}_l)} = \overline{\chi\omega} \oplus \overline{\omega} \oplus \overline{\chi\omega}$ with $H^1(\mathbb{Q}_l, \overline{\chi\omega}) = 0$, Kummer's theory tells us that $H^1(\mathbb{Q}_l, Ad^*(1)) = \mathbb{Q}_l^\times/(\mathbb{Q}_l^\times)^p \otimes_{\mathbb{F}_p} \mathbb{F} \cong \mathbb{F}$, which is represented by cocycle with values in $\mathbb{F}\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$ on which $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ acts by $\overline{\omega}$ as a factor of $Ad^*(1)$. Therefore the direct sum decomposition (3.3) holds, and $\mathcal{D}^l_Q(\mathbb{F}[\epsilon])^\perp = H^1(\mathbb{Q}_l, Ad)^\perp = 0$. We record this fact as

(D$_N$) *Cohomology classes in* $\mathrm{Sel}^\perp_{\mathbb{Q}}(Ad \otimes \overline{\omega})$ *is trivial at all primes* $l|N$.

Thus, for the dual Selmer groups of $\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^- \overline{\omega}$ and $\overline{\chi\omega}$, triviality at $l|N$ is imposed (under (h0)). In particular, for the splitting field K of $\chi\omega$, writing $Cl_{\chi\omega}(p^\infty) := \varprojlim_n Cl_{\chi\omega}(p^n)$ for the ray class group modulo p^n $(n = 0, \dots, \infty)$ of K, we have

$$\mathrm{Sel}^\perp_\emptyset(\overline{\chi\omega}) \hookrightarrow \mathrm{Hom}(Cl_{\chi\omega}(p^\infty), \mathbb{F})[\overline{\chi\omega}],$$

where $\mathrm{Hom}(Cl_{\chi\omega}(p^\infty), \mathbb{F})[\overline{\chi\omega}]$ is the $\overline{\chi\omega}$-eigen subspace of $\mathrm{Hom}(Cl_{\chi\omega}(p^\infty), \mathbb{F})$ under the action of $\mathrm{Gal}(K/\mathbb{Q})$ and by (Km) the cocycles in the image of $\mathrm{Sel}^\perp_\emptyset(\overline{\chi\omega})$ in $\mathrm{Hom}(Cl_{\mathbb{Q}(\chi\omega)}(p^\infty), \mathbb{F})[\overline{\chi\omega}]$ give rise to locally at p a Kummer cocycle coming from $\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times p}$. Note that $\overline{\varphi}^-$ ramifies both at two primes $\mathfrak{l}$ and $\overline{\mathfrak{l}}$ over $l|N_{F/\mathbb{Q}}(\mathfrak{c})$. Since φ^- is anti-cyclotomic, any prime $\mathfrak{l}|D$ is fully split in $F(\varphi^-)/F$.

Recall the splitting field K_0 of $\overline{\rho}$. Let F^Q be the maximal extension of K_0 unramified outside Q and p. By (h0), all deformations of $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$ satisfying (D1–4) factors through $\mathrm{Gal}(F^Q/\mathbb{Q})$. Write M_Q for the maximal p-abelian extension of $F(\varphi^-\omega)$ inside F^Q unramified outside N, Q and $\mathfrak{p}$ in which all prime factors of $\mathfrak{p}^c N$ totally split (by (3.4)). By Proposition 7.1, as mentioned already, we can replace "total splitting at $\mathfrak{p}^c N$" by "unramifiedness at $\mathfrak{p}^c N$" without changing the Iwasawa module (in other words, for the Galois extension $L/F_\infty^- F(\varphi^-\omega)$ with $\mathrm{Gal}(L/F_\infty^- F(\varphi^-\omega)) = \mathcal{Y}(\varphi^-\omega)$, prime factors of $\mathfrak{p}^c N$ automatically split). Thus we conclude

$$\mathrm{Sel}^\perp_\emptyset(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^- \overline{\omega}) \cong \mathrm{Sel}^\perp_\emptyset(\overline{\varphi}^- \overline{\omega}) = \mathrm{Hom}_{\mathrm{Gal}(F(\varphi^-\omega)/F)}(\mathrm{Gal}(M_\emptyset/F(\varphi^-\omega)), \overline{\varphi}^- \overline{\omega}).$$

Since $p \nmid h_F$, $K_\emptyset^-/F$ is fully wild $\mathfrak{p}^c$-ramified, while $F(\varphi^-\omega)$ is at most tamely $\mathfrak{p}^c$-ramified. Therefore the inertia subgroup of $\mathfrak{p}^c$ for the extension $K_\emptyset^- F(\varphi^-\omega)/F(\varphi^-\omega)$ is the entire Galois group $\mathrm{Gal}(K_\emptyset^- F(\varphi^-\omega)/F(\varphi^-\omega))$. This tells us that $M_\emptyset \cap K_\emptyset^- F(\varphi^-\omega) = F(\varphi^-\omega)$. Thus, we have the vanishing of the $\varphi^-\omega$-eigenspace

$$\begin{aligned}\mathrm{Coker}(\mathcal{Y}^- &\xrightarrow{\mathrm{Res}} \mathrm{Gal}(M_\emptyset/F(\varphi^-\omega)))[\varphi^-\omega] \\ &= \mathrm{Coker}(\mathcal{Y}^- \xrightarrow{\mathrm{Res}} \mathrm{Gal}(M_\emptyset/F(\varphi^-\omega))) \otimes_{\mathbb{Z}_p[\mathrm{Gal}(F(\varphi^-\omega)/F)], \varphi^-\omega} W = 0,\end{aligned}$$

and we find $\mathrm{Gal}(M_\emptyset/F(\varphi^-\omega))[\varphi^-\omega] = \mathcal{Y}^-(\varphi^-\omega)_H = H_0(H, \mathcal{Y}^-(\varphi^-\omega))$ and

$$\mathrm{Hom}_{\mathrm{Gal}(F(\varphi^-\omega)/F)}(\mathrm{Gal}(M_\emptyset/F(\varphi^-\omega)), \overline{\varphi}^- \overline{\omega}) = \mathrm{Hom}(\mathcal{Y}^-(\varphi^-\omega)_H, \mathbb{F}) = \mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-\omega), \mathbb{F}).$$

Proposition 3.6. *Let* $Cl^-_{Q^+} = \{x \in Cl_{Q^+} | c(x) = x^{-1}\}$, *and write* $Cl_{\chi\omega}(p^\infty)$ *for the class group of the splitting field of* $\chi\omega$. *Then, under* (h0–4), *we have* $\mathcal{Y}^-_Q(\varphi^-) \otimes_{W[[H_Q]]} \mathbb{F} = \mathcal{Y}^-(\varphi^-) \otimes_{W[[H]]} \mathbb{F}$ *for*

$Q \in \mathcal{Q}$,

$$\begin{aligned}\mathrm{Sel}_Q(Ad) &\cong \mathrm{Hom}(Cl^-_{Q^+}, \mathbb{F}) \oplus \mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-), \mathbb{F}) \text{ \textit{including} } Q = \emptyset, \\ \mathrm{Sel}^\perp_\emptyset(Ad^*(1)) &\cong \mathrm{Sel}^\perp_\emptyset(\overline{\chi\omega}) \oplus \mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-\omega), \mathbb{F}),\end{aligned} \tag{3.5}$$

and

$$\begin{aligned}\mathrm{Sel}_Q(\overline{\chi}) &\cong \mathrm{Hom}(Cl^-_{Q^+}, \mathbb{F}) \text{ \textit{including} } Q = \emptyset, \\ \mathrm{Sel}_Q(\mathrm{Ind}^{\mathbb{Q}}_F \overline{\varphi}^-) &\cong \mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-), \mathbb{F}) \text{ \textit{including} } Q = \emptyset, \\ \mathrm{Sel}^\perp_\emptyset(\overline{\chi\omega}) &\hookrightarrow \mathrm{Hom}(Cl_{\mathbb{Q}(\chi\omega)}(p^\infty), \mathbb{F})[\overline{\chi\omega}] \\ \mathrm{Sel}^\perp_\emptyset(\mathrm{Ind}^{\mathbb{Q}}_F \overline{\varphi}^- \overline{\omega}) &\cong \mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-\omega), \mathbb{F}),\end{aligned} \tag{3.6}$$

where the cocycles in the image of $\mathrm{Sel}^\perp_\emptyset(\overline{\chi\omega})$ in $\mathrm{Hom}(Cl_{\mathbb{Q}(\chi\omega)}(p^\infty), \mathbb{F})[\overline{\chi\omega}]$ give rise to locally at p a Kummer cocycle coming from $\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times p}$.

Proof. We have already proven the last two identities of (3.6) and the second identity of (3.5). Thus we deal the rest. The subspace $\mathcal{D}^p_Q(\mathbb{F}[\epsilon])$ is made of classes of cocycles with values in $Ad = \mathfrak{sl}_2(\mathbb{F})$ such that $u_\rho|_{I_p}$ is upper nilpotent and $u_\rho|_{D_p}$ ($D_p := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$) is upper triangular. Similarly $\mathcal{D}^l(\mathbb{F}[\epsilon])$ for $l|N$ is made of classes of unramified cocycles u_ρ 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

$$\mathrm{Sel}_Q(Ad) = \mathrm{Sel}_Q(\overline{\chi}) \oplus \mathrm{Sel}_Q(\mathrm{Ind}^{\mathbb{Q}}_F \overline{\varphi}^-),$$

where $\mathrm{Sel}_Q(\overline{\chi}) = \mathrm{Ker}(H^1(\mathbb{Q}^{(QNp)}/\mathbb{Q}, \overline{\chi}) \xrightarrow{\mathrm{Res}} \prod_{l|Np} H^1(I_l, \overline{\chi}))$ and

$$\begin{aligned}\mathrm{Sel}_Q(\mathrm{Ind}^{\mathbb{Q}}_F \overline{\varphi}^-) &= \mathrm{Ker}(H^1(\mathbb{Q}^{(QNp)}/\mathbb{Q}, \mathrm{Ind}^{\mathbb{Q}}_F \overline{\varphi}^-) \xrightarrow{\mathrm{Res}} \prod_{l|Np} \frac{H^1(\mathbb{Q}_l, \mathrm{Ind}^{\mathbb{Q}}_F \overline{\varphi}^-)}{\mathcal{D}^l(\mathbb{F}[\epsilon])}) \\ &= \mathrm{Ker}(H^1(\mathbb{Q}^{(QNp)}/\mathbb{Q}, \mathrm{Ind}^{\mathbb{Q}}_F \overline{\varphi}^-) \xrightarrow{\mathrm{Res}} H^1(F_{\overline{\mathfrak{p}}}, \overline{\varphi}^-) \times \prod_{l|N} H^1(I_l, \mathrm{Ind}^{\mathbb{Q}}_F \overline{\varphi}^-).\end{aligned} \tag{3.7}$$

By the inflation restriction sequence,

$$\mathrm{Sel}_Q(\chi) \cong \mathrm{Ker}(\mathrm{Hom}_{\mathrm{Gal}(F/\mathbb{Q})}(\mathrm{Gal}(F^Q/F), \chi) \to \prod_{l|N} H^1(I_l, \chi)) \cong \mathrm{Hom}(Cl^-_Q, \mathbb{F}).$$

However the order of $\mathrm{Ker}(Cl^-_Q, Cl^-_{Q^+})$ is $\prod_{q \in Q^-}(q+1)$, which is prime to p; so, we conclude

$$\mathrm{Sel}_Q(\chi) \cong \mathrm{Hom}(Cl^-_Q, \mathbb{F}) \cong \mathrm{Hom}(Cl^-_{Q^+}, \mathbb{F}).$$

Again by the inflation restriction sequence, identifying $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ with the decomposition group at $\overline{\mathfrak{p}}$, we have an exact sequence

$$0 \to H^1(\mathrm{Frob}_p^{\widehat{\mathbb{Z}}}, H^0(I_{\mathfrak{p}}, \overline{\varphi}^-)) \to H^1(F_{\overline{\mathfrak{p}}}, \overline{\varphi}^-) \to H^1(I_{\overline{\mathfrak{p}}}, \mathbb{F}(\overline{\varphi}^-))^{\mathrm{Frob}_{\mathfrak{p}}} \to 0.$$

If φ is ramified at $\mathfrak{p}$ (so, φ^- ramifies at $\mathfrak{p}$ and $\overline{\mathfrak{p}}$), we conclude $H^0(I_{\mathfrak{p}}, \overline{\varphi}^-) = 0$. If φ is unramified at p, we have $H^1(\mathrm{Frob}_p^{\widehat{\mathbb{Z}}}, H^0(I_{\mathfrak{p}}, \overline{\varphi}^-)) = \overline{\varphi}^-/(\mathrm{Frob}_p - 1)\overline{\varphi}^- = 0$, since $\varphi^-(\mathrm{Frob}_p) \neq 1$ by (h4). Thus we conclude

$$\mathrm{Ker}(H^1(F_{\overline{\mathfrak{p}}}, \overline{\varphi}^-) \xrightarrow{\mathrm{Res}} H^1(I_{\overline{\mathfrak{p}}}, \overline{\varphi}^-)) = 0,$$

and $\mathrm{Sel}_Q(\mathrm{Ind}^{\mathbb{Q}}_F \overline{\varphi}^-)$ is actually given (by replacing $H^1(F_{\overline{\mathfrak{p}}}, \overline{\varphi}^-)$ by $H^1(I_{\overline{\mathfrak{p}}}, \overline{\varphi}^-)$ in (3.7))

$$\mathrm{Ker}(H^1(\mathbb{Q}^{(QNp)}/\mathbb{Q}, \mathrm{Ind}^{\mathbb{Q}}_F \overline{\varphi}^-) \xrightarrow{\mathrm{Res}} H^1(I_{\overline{\mathfrak{p}}}, \overline{\varphi}^-) \times \prod_{l|N} H^1(I_l, \mathrm{Ind}^{\mathbb{Q}}_F \overline{\varphi}^-). \tag{3.8}$$

By the inflation-restriction sequence, we have an exact sequence $H^1(\mathrm{Frob}_l^{\widehat{\mathbb{Z}}}, (\overline{\varphi}^-)^{I_l}) \hookrightarrow H^1(D_l, \overline{\varphi}^-) \to H^1(I_l, \overline{\varphi}^-)$ with $(\overline{\varphi}^-)^{I_l} = 0$ for $l|N$, and hence by Shapiro's lemma (and (h0), we can rewrite

$$\mathrm{Sel}_Q(\mathrm{Ind}^{\mathbb{Q}}_F \overline{\varphi}^-) \cong \mathrm{Ker}(H^1(\mathbb{Q}^{(QNp)}/\mathbb{Q}, \varphi^-) \xrightarrow{\mathrm{Res}} H^1(I_{\overline{\mathfrak{p}}}, \overline{\varphi}^-) \times \prod_{\mathfrak{l}|N} H^1(I_{\mathfrak{l}}, \overline{\varphi}^-)),$$

where $\mathfrak{l}$ running over all prime factors of N in F. Thus, restricting to the Galois group over $F(\overline{\varphi}^-)$, by the restriction-inflation sequence, we have

$$\mathrm{Sel}_Q(\mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}^-)\cong \mathrm{Hom}_{W[[H_Q]]}(\mathcal{Y}_Q^-(\overline{\varphi}^-),\mathbb{F}).$$

Similarly, $\mathrm{Sel}_Q(\overline{\chi})\cong \mathrm{Hom}_{\mathrm{Gal}(F/\mathbb{Q})}(\mathrm{Gal}(\mathbb{Q}^{(QNp)}/F),\overline{\chi})=\mathrm{Hom}(Cl_Q^-,\mathbb{F})$. Therefore the first identity of (3.5) follows if we prove $\mathcal{Y}_Q^-(\varphi^-)\otimes_{W[[H_Q]]}\mathbb{F}=\mathcal{Y}^-(\varphi^-)\otimes_{W[[H]]}\mathbb{F}$.

To prove $\mathcal{Y}_Q^-(\varphi^-)\otimes_{W[[H_Q]]}\mathbb{F}=\mathcal{Y}^-(\varphi^-)\otimes_{W[[H]]}\mathbb{F}$, writing $I_{\mathfrak{Q}}^{p\text{-ab}}$ for the maximal p-abelian quotient of the inertia group $I_{\mathfrak{Q}}\subset \mathrm{Gal}(\overline{\mathbb{Q}}/K_Q^-F(\varphi^-))$ of a prime $\mathfrak{Q}|q$ in $K_Q^-F(\varphi^-)$, we have an exact sequence

$$\prod_{\mathfrak{Q}|q,q\in Q} I_{\mathfrak{Q}}^{p\text{-ab}}\to\mathcal{Y}_Q^-\to\mathcal{Y}^-\to 0$$

as $\mathrm{Ker}(\mathcal{Y}_Q^-\to\mathcal{Y}^-)$ is generated by the image $I_{\mathfrak{Q}}^{p\text{-ab}}\cong\mathbb{Z}_p$. The surjectivity of the restriction map: $\mathcal{Y}_Q^-\to\mathcal{Y}^-$ follows from linear-disjointness of $L_\emptyset$ and $K_Q^-F(\varphi^-)$ over $K^-F(\varphi^-)$ as at least one of $q\in Q$ ramifies in any intermediate field of $K_Q^-F(\varphi^-)/K^-F(\varphi^-)$. Note that $q\in Q^-$ totally splits in $K_Q^-F(\varphi^-)/F$. Thus $I_q^-:=\prod_{\mathfrak{Q}|q}I_{\mathfrak{Q}}^{p\text{-ab}}$ for $q\in Q^-$ is isomorphic to

$$\mathbb{Z}_p^{\mathrm{Gal}(K_Q^-F(\varphi^-)/F)}=\mathbb{Z}_p[[\mathrm{Gal}(K_Q^-F(\varphi^-)/F)]]=\mathbb{Z}_p[[H_Q]][\mathrm{Im}(\varphi^-)]$$

as $\mathbb{Z}_p[[\mathrm{Gal}(K_Q^-F(\varphi^-)/F)]]$-modules. Since $I_{\mathfrak{Q}}^{p\text{-ab}}\cong\mathbb{Z}_p$ is the quotient of the maximal q-tame quotient of $I_{\mathfrak{Q}}$, $\mathrm{Frob}_{\mathfrak{q}}$ (for the prime $\mathfrak{q}|q\in Q^-$ in F) acts on it via multiplication by q^2. Since $\varphi^-(\mathrm{Frob}_{\mathfrak{q}})=1$, the map $I_q^-\otimes_{\mathbb{Z}_p[\mathrm{Im}(\varphi^-)],\varphi^-}W\to\mathcal{Y}_Q^-(\varphi^-)$ factors through

$$\mathcal{I}_q^-(\varphi^-)=I_q^-\otimes_{\mathbb{Z}_p[\mathrm{Im}(\varphi^-)],\varphi^-}W\cong W[[H_Q]]/(q^2-1).$$

Thus we have $\mathcal{I}_q^-(\varphi^-)\otimes_{W[[H_Q]]}\mathbb{F}=\mathbb{F}(\varphi^-)$ (one dimensional space over $\mathbb{F}$ on which $\mathrm{Gal}(F(\varphi^-)/F)$ acts by φ^-). Note that Frob_q acts on $\mathcal{I}_q^-(\varphi^-)\otimes_{W[[H_Q]]}\mathbb{F}$ via multiplication by q, which is trivial as $q\equiv 1\mod p$. Thus the image of $\mathcal{I}_q^-(\varphi^-)\otimes_{W[[H_Q]]}\mathbb{F}$ in $\mathcal{Y}_Q^-(\varphi^-)\otimes_{W[[H_Q]]}\mathbb{F}$ is stable under $\mathrm{Frob}_q=c$, and hence stable under $\mathrm{Gal}(F(\overline{\varphi}^-)/\mathbb{Q})$. The $\mathrm{Gal}(F(\varphi^-)/\mathbb{Q})$-module $\mathrm{Ind}_F^{\mathbb{Q}}\varphi^-$ is absolutely irreducible by (h3). Since $\mathcal{I}_q^-(\varphi^-)\otimes_{W[[H_Q]]}\mathbb{F}=\mathbb{F}(\varphi^-)$, if the image is non-trivial, it must contain the irreducible $\mathrm{Gal}(F(\varphi^-)/\mathbb{Q})$-module $\mathrm{Ind}_F^{\mathbb{Q}}\varphi^-$, which is impossible as the image has dimension ≤ 1. Thus the image of $\mathcal{I}_q^-(\varphi^-)\otimes_{W[[H_Q]]}\mathbb{F}$ in $\mathcal{Y}_Q^-(\varphi^-)\otimes_{W[[H_Q]]}\mathbb{F}$ is trivial.

The set $\mathfrak{Q}_{\mathfrak{q}}^+$ of primes $\mathfrak{Q}$ in $K_Q^-F(\varphi^-)$ above $\mathfrak{q}|q\in Q^+$ is a finite set on which the Galois group $\mathrm{Gal}(K_Q^-F(\varphi^-)/F)$ acts by permutation. Then, writing $D(\mathfrak{Q}/\mathfrak{q})\subset\mathrm{Gal}(K_Q^-F(\varphi^-)/F)$ for the decomposition grup of $\mathfrak{Q}$, we have

$$I_q^+:=\prod_{\mathfrak{Q}\in\mathfrak{Q}_q^+}I_{\mathfrak{Q}}^{p\text{-ab}}\cong\mathbb{Z}_p^{\mathfrak{Q}_{\mathfrak{q}}^+}\cong\mathbb{Z}_p[\mathrm{Gal}(K_Q^-F(\varphi^-)/F)/D(\mathfrak{Q}/\mathfrak{q})]$$

on which $\mathrm{Frob}_{\mathfrak{q}}$ acts by $\sigma D(\mathfrak{Q}/\mathfrak{q})\mapsto q\sigma\mathrm{Frob}_{\mathfrak{q}}D(\mathfrak{Q}/\mathfrak{q})=q\sigma D(\mathfrak{Q}/\mathfrak{q})$ for $\sigma\in\mathrm{Gal}(K_Q^-F(\varphi^-)/F)$ and $\Delta_q\subset H_Q$ act trivially. Thus putting $I_q^+(\varphi^-):=I_q^+\otimes_{\mathbb{Z}_p[\varphi^-],\varphi^-}W$, we conclude from $q\equiv 1\mod p$

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

since $q\equiv 1\mod p$ (i.e., after tensoring $\mathbb{F}$, $\mathrm{Frob}_{\mathfrak{q}}$ acts on $\mathbb{F}[\mathrm{Gal}(K_Q^-F(\varphi^-)/F)/D(\mathfrak{Q}/\mathfrak{q})]$ by multiplication by $q\equiv 1\mod p$). By our choice of $Q\in\mathcal{Q}$, $\overline{\rho}(\mathrm{Frob}_q)$ has two distinct eigenvalues, and hence $\varphi^-(\mathrm{Frob}_{\mathfrak{q}})\neq 1$. Thus we get the following isomorphism:

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

as desired. □

The primes $q_x\in Q_m$ is indexed by a basis $\{x\}_x$ of the Selmer group $\mathrm{Sel}_\emptyset^\perp(Ad^*(1))$ so that f_x as in Lemma 3.2 has non-trivial value at Frob_{q_x}. Thus writing $Q_m^\pm:=\{q\in Q_m|\chi(q)=\pm 1\}$, we get from our choice in Corollary 3.3

$$|Q_m^-|=\dim_{\mathbb{F}}\mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-\omega),\mathbb{F})\ \text{ and }\ |Q_m^+|=\dim_{\mathbb{F}}\mathrm{Sel}_\emptyset^\perp(\overline{\chi\omega}).\tag{3.9}$$

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) $\pi_n^{n+1} \circ \sigma_{n+1} = \sigma_n \circ \pi_n^{n+1}$, and the set $\{f_1^{(n)}, \dots, f_r^{(n)}\}$ is made of eigenvectors of σ_n for all n (i.e., $\sigma_n(f_j^{(n)}) = \pm f_j^{(n)}$).

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

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

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

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

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

$$((R_{n,m(n)}, \alpha), \widetilde{R}_{n,m(n)}, (f_1, \dots, f_r))$$

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

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

satisfying (Q0–8) with m varying in the choosing process of $\mathcal{Q}$ (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 σ induced by σ_{Q_m}. Therefore, we look into isomorphism classes in the infinite set of (σ-added) quadruples (varying m)

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

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

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

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

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

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 $R_{Q,j} = \mathbb{T}_Q/(p^j, \delta_q^{p^j} - 1)_{q \in Q}$, the projections

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

are compatible with the involutions induced by σ_Q, and hence for the same set of generators $\{f_j\}_j$, the two quadruples

$$\{((R_{Q,j},\alpha),\widetilde{R}_{Q,j},(f_1,\dots,f_r),\sigma_j)\}_j$$

of level $j = n+1, n$ are automatically σ_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 $\pi_n^{n+1}\circ\sigma_{n+1} = \sigma_n\circ\pi_n^{n+1}$ for $\mathcal{I}_{n+1}$; i.e., $\mathcal{I}_{n+1} \xrightarrow{\text{reduction}} \mathcal{I}_n \to \mathcal{I}_{n-1} \to \cdots \to \mathcal{I}_1$ with $|\mathcal{I}_j| = \infty$ for all $j = 1,2,\dots,n+1$. We hereafter write $m(n)$ for the minimal of m with $((R_{n,m},\alpha),\widetilde{R}_{n,m},(f_1,\dots,f_r),\sigma_{n,m})$ appearing in $\mathcal{I}_n$. □

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

Proof. Since $|Q_m^-| = \dim_{\mathbb{F}} \operatorname{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-\omega),\mathbb{F})$ by Proposition 3.6, it is independent of m. □

By (Q9), we have the limit involution σ_∞ acting on $R_\infty = \varprojlim_n R_{n,m(n)}$, and we may assume that the generators $(f_1^{(n)},\dots,f_r^{(n)})$ to satisfy $\sigma_n(f_j^{(n)}) = \pm f_j^{(n)}$. Therefore we may assume that $(f_1^{(n)},\dots,f_r^{(n)}) = (f_{1,+}^{(n)},\dots,f_{r',+}^{(n)},f_{1,-}^{(n)},\dots,f_{r'',-}^{(n)})$ with $\sigma_\infty(f_{j,\pm}^{(n)}) = \pm f_{j,\pm}^{(n)}$ for $r = r'+r''$, and hence, we may assume that

$$R_\infty \cong W[[T_{1,+},\dots,T_{r',+},T_{1,-},\dots,T_{r'',-}]]$$

with variables $T_{j,\pm}$ satisfying $\sigma_\infty(T_{j,\pm}) = \pm T_{j,\pm}$ for $r = r'+r''$, and we have the following presentation for $\mathfrak{A}_Q := (s_j^{|\Delta_{q_j}|}-1)_j$:

$$R_\infty/\mathfrak{A}_Q = W[[T_{1,+},\dots,T_{r',+},T_{1,-},\dots,T_{r'',-}]]/\mathfrak{A}_Q \cong \mathbb{T}_Q. \tag{4.1}$$

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 $\mathbb{T}^Q/(t-\gamma^k)\mathbb{T}^Q \cong \mathbb{T}_Q$, we can lift, as is well known, the above presentation over W and the involution σ_∞ to that of $\mathbb{T}^Q$ over Λ to obtain:

$$\Lambda[[T_{1,+},\dots,T_{r',+},T_{1,-},\dots,T_{r'',-}]]/\mathfrak{A}_Q\Lambda[[T_{1,+},\dots,T_{r',+},T_{1,-},\dots,T_{r'',-}]] \cong \mathbb{T}^Q, \tag{4.2}$$

where $\sigma_\infty(T_{j,\pm}) = \pm T_{j,\pm}$ intact. We write simply $\mathcal{R} = \mathcal{R}_\infty := \Lambda[[T_{1,+},\dots,T_{r',+},T_{1,-},\dots,T_{r'',-}]]$.

Here is a brief outline how to lift the presentation (cf. [MFG, §5.3.5]): Let $f_j^{(\infty)} := \varprojlim_n f_j^{(n)}$. Since $f_j^{(n)}$ is an eigenvector of σ_n, $f_j^{(\infty)}$ is an eigenvector of σ_∞. Let $\mathcal{R} := \Lambda[[T_1,\dots,T_r]]$ and define an involution σ on $\mathcal{R}$ by $\sigma(T_i) = \pm T_i \Leftrightarrow \sigma_\infty(f_i^{(\infty)}) = \pm f_i^{(\infty)}$. Choose $\mathbf{f}_j \in \mathcal{R}$ such that $\mathbf{f}_j \bmod (t-\gamma^k) = f_j^{(\infty)}$ and $g_j \in \mathbb{T} = \mathbb{T}^\emptyset$ such that $g_j \bmod (t-\gamma^k)$ giving the image of $f_j^{(\infty)}$ in $\mathbb{T}_\emptyset$. We can impose that these $\mathbf{f}_j$ and g_j are made of eigenvectors of the involution. By sending $T_i = \mathbf{f}_i$ to g_i, we have $\mathcal{R}/\mathfrak{A}_\emptyset\mathcal{R} \cong \mathbb{T}$, $\mathcal{R}^+/\mathfrak{A}_\emptyset = \mathbb{T}^+$, $\mathcal{R}/(t-\gamma^k) = R_\infty$ and $\mathcal{R}^+/(t-\gamma^k) = R_\infty^+$.

We reformulate the ring $W[[S_1,\dots,S_r]]$ in terms of group algebras. Let $\Delta_{Q_m^\pm} = \prod_{q\in Q_m^\pm}\Delta_q$ and $\Delta_n^\pm := \prod_{q\in Q_m^\pm}\Delta_q/\Delta_q^{p^n}$; so, $\Delta_n = \Delta_n^+\times\Delta_n^-$. Define p-profinite groups $\mathbf{\Delta}$ and $\mathbf{\Delta}_\pm$ by $\mathbf{\Delta} = \varprojlim_n \Delta_n \cong \mathbb{Z}_p^r$ and $\mathbf{\Delta}_\pm = \varprojlim_n \Delta_n^\pm \cong \mathbb{Z}_p^{r_\pm}$ for $r_\pm := |Q_m^\pm|$. Here the limits are taken with respect to π_n^{n+1} restricted to Δ_{n+1}.

Set

$$\mathcal{S} := W[[\mathbf{\Delta}]] = \varprojlim_n W[\mathbf{\Delta}/\mathbf{\Delta}^{p^n}] = \varprojlim_n W[\Delta_n] \tag{4.3}$$

for the p-profinite group $\mathbf{\Delta} = \varprojlim_n \Delta_n \cong \mathbb{Z}_p^r$ with $\mathbf{\Delta} = \mathbf{\Delta}_+\times\mathbf{\Delta}_-$ and A be a local $\mathcal{S}$-algebra. Thus by identifying $\mathbf{\Delta}/\mathbf{\Delta}^{p^n}$ with Δ_n, we have the identification $\mathcal{S} = W[[S_1,\dots,S_r]]$. The image $\mathcal{S}_n := W_n[\Delta_n]$ ($W_n = W/p^nW$) of $\mathcal{S}$ 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 $Q_m^- := \{q_1,\dots,q_{r_-}\}$ and $Q_m^+ := \{q_{r_-+1} =: q_1^+,\dots,q_r = q_{r_+}^+\}$. We now write $s_j^\pm$ for the generator of $\mathbf{\Delta}$ corresponding to $\delta_{q_j^\pm}$.

Definition 4.3. *Write $s_j^{\pm}$ for the generator of $\boldsymbol{\Delta}_{\pm}$ corresponding to $\delta_{q_j^{\pm}}$. Then define $S_j^+ = s_j^+ - 1$ and $S_j^- := s_j^- - (s_j^-)^{-1}$. Thus $\sigma_\infty(S_j^{\pm}) = \pm S_j^{\pm}$. Write G for the subgroup of involutions in $\mathrm{Aut}(W[[\boldsymbol{\Delta}]]_{/W})$ generated by the involutions $\flat_i$ ($i = 1, \dots, r_-$) such that $\flat_i(S_j^-) = (-1)^{\delta_{ij}} S_j^-$ for Kronecker's delta δ_{ij} and $\flat_i(S_j^+) = S_j^+$ for all $j = 1, 2, \dots, r_+$. Put $S := \mathcal{S}^G = W[[\boldsymbol{\Delta}]]^G$.*

Since σ_∞ acts as $\sigma_\infty(S_j^-) = -S_j^-$ for all $j = 1, 2, \dots, r_-$, the group $\mathcal{G} = \langle\sigma\rangle$ embeds into G so that $\sigma_\infty = \prod_j \flat_j$ on $W[[\boldsymbol{\Delta}]]$.

For the ideal $\mathfrak{a}_n := \mathrm{Ker}(W[[\boldsymbol{\Delta}_+] \to W_n[\Delta_n^+])$ for $W_n := W/p^nW$, we put

$$\mathfrak{A}_n = \mathfrak{a}_n + ((s_1^-)^{p^n} - 1, \dots, (s_{r_-}^-)^{p^n} - 1) \subset \mathcal{S}$$

as an $\mathcal{S}$-ideal. Then $\mathfrak{A}_n$ is stable under σ, and $\mathfrak{A}_n := \mathrm{Ker}(\mathcal{S} \to W_n[\boldsymbol{\Delta}/\boldsymbol{\Delta}^{p^n}])$. Put

$$\begin{aligned}(4.4)\quad \mathfrak{S}_n &:= \mathfrak{A}_n \cap W[\boldsymbol{\Delta}]^G = \mathrm{Ker}(W[\boldsymbol{\Delta}]^G \to W_n[\boldsymbol{\Delta}/\boldsymbol{\Delta}^{p^n}]^G)\\ &= \mathfrak{a}_n + (((s_1^-)^{p^n} - 1) + \sigma((s_1^-)^{p^n} - 1), \dots, ((s_{r_-}^-)^{p^n} - 1) + \sigma((s_{r_-}^-)^{p^n} - 1)).\end{aligned}$$

By this expression, we confirm the following fact:

Lemma 4.4. *The ring $S_n := S/\mathfrak{S}_n = W_n[\boldsymbol{\Delta}/\boldsymbol{\Delta}^{p^n}]^G$ 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 $\boldsymbol{\Delta} \twoheadrightarrow \Delta_{Q_m}$ sending $s_j^{\pm}$ to $\delta_{q_j^{\pm}}$, we get $\mathfrak{A}_{Q_m} = \mathrm{Ker}(\mathcal{S} \to W[\Delta_{Q_m}])$. We define $\mathfrak{S}_{Q_m} := \mathrm{Ker}(S \to W[\Delta_{Q_m}]^G)$. Let A be a local $\mathcal{S}_n$-algebra for $\mathcal{S}_n = \mathcal{S}/\mathfrak{A}_n = W_n[\boldsymbol{\Delta}/\boldsymbol{\Delta}^{p^n}]$ (and hence A is an S_n-algebra for $S_n = S/\mathfrak{S}_n \subset \mathcal{S}_n$). We suppose that σ acts on A as an involution extending its action on $\mathcal{S}_n$. Then σ acts on $A^\dagger = \mathrm{Hom}_S(A, S_n)$ (resp. $A^\# = \mathrm{Hom}_{\mathcal{S}}(A, \mathcal{S}_n)$) by $f^\sigma(x) = \sigma(f(\sigma(x))$. Indeed, $f^\sigma(sx) = \sigma(f(\sigma(sx)) = \sigma(f(\sigma(s)\sigma(x)) = \sigma(\sigma(s))\sigma(f(\sigma(x)) = sf^\sigma(x)$, and hence f^σ is $\mathcal{S}$-linear. We put $\mathcal{S}_\infty = \mathcal{S}$ and $S_\infty = S$ and allow $n = \infty$.

Remark 4.5. Let $C \subset A$ 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 $\mathrm{Hom}_B(C, B) \cong C$ as B-modules (cf., Lemma 10.1). Thus by [BAL, Proposition II.4.1.1],

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

This isomorphism is sending $g \in \mathrm{Hom}_C(A, \mathrm{Hom}_B(C, B))$ to $\widetilde{g} \in \mathrm{Hom}_B(A \otimes_C C, B)$ given by $\widetilde{g}(a \otimes c) = g(a)(c)$. Applying this to $(A, B, C) := (R_n, S_n, \mathcal{S}_n)$ and then to $(A, B, C) := (R_n, W_n, S_n)$, we get $A^\# \cong A^\dagger \cong A^*$ as A-modules for $A^* = \mathrm{Hom}_{W_n}(A, W_n)$. The identity $A^\# \cong A^\dagger$ is valid for $n = \infty$ also. Since the isomorphism $\mathcal{S}_n \cong \mathcal{S}_n^\dagger$ can be chosen to be compatible with the action of G (including σ), the isomorphisms

$$(4.5)\qquad A^\# \cong A^\dagger \cong A^*$$

can be chosen to be σ-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_∞ is free of finite rank over $\mathcal{S}$, we get the following σ-compatible identity:

$$\begin{aligned}(4.6)\quad \varprojlim_n R_n^\dagger &\overset{(1)}{\cong} \varprojlim_n R_n^\# = \varprojlim_n \mathrm{Hom}_{\mathcal{S}_n}(R_n, \mathcal{S}_n)\\ &\overset{(2)}{=} \varprojlim_n \mathrm{Hom}_{\mathcal{S}}(R_\infty/\mathfrak{A}_n R_\infty, \mathcal{S}/\mathfrak{A}_n) \cong \mathrm{Hom}_{\mathcal{S}}(R_\infty, \mathcal{S}) \cong R_\infty^\# \overset{(1)}{\cong} R_\infty^\dagger.\end{aligned}$$

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 $\mathcal{S}_n := \mathcal{S}/\mathfrak{A}_n$.

Define

$$\mathrm{Hom}_B(A, B)^{\pm} := \{\phi \in \mathrm{Hom}_B(A, B) | \phi \circ \sigma = \pm\sigma \circ \phi\}$$

for $A = \mathbb{T}^\dagger_{Q_m} := \mathrm{Hom}_{W[\Delta_{Q_m}]^G}(\mathbb{T}_{Q_m}, W[\Delta_{Q_m}]^G)$ or $R^\dagger_n$ and $B = \mathbb{T}_{Q_m}$ or R_n accordingly. Write $\mathrm{Isom}_B(A,B)^\pm \subset \mathrm{Hom}_B(A,B)^\pm$ for the subset made of isomorphisms. Using the Gorenstein-ness of $\mathbb{T}_Q$ for $Q = Q_m$ or $Q = \emptyset$ (which follows from the presentation (4.1) and for $Q = \emptyset$ from Theorem 2.1), by Lemma 10.2 (1) applied to the involution σ_{Q_m} of $\mathbb{T}_{Q_m}$, we have

$$\mathrm{Isom}_{\mathbb{T}_{Q_m}}(\mathbb{T}^\dagger_{Q_m}, \mathbb{T}_{Q_m})^\varepsilon \neq \emptyset$$

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

Lemma 4.6. *We have*

$$\mathrm{Isom}_{\mathbb{T}_{Q_m}}(\mathbb{T}^\dagger_{Q_m}, \mathbb{T}_{Q_m})^\varepsilon \neq \emptyset \Leftrightarrow \mathrm{Isom}_{R_{n,m}}(R^\dagger_{n,m}, R_{n,m})^\varepsilon \neq \emptyset$$

for each $0 < n \leq m$.

Proof. The direction ($\Rightarrow$) is just reduction modulo $(p^n, \delta_q^{p^n} - 1)_{q \in Q_m}$. We prove the converse. If we have $\phi \in \mathrm{Isom}_{R_{n,m}}(R^\dagger_{n,m}, R_{n,m})^\varepsilon$, then $\sigma(\phi^{-1}(1)) = \varepsilon\phi^{-1}(1)$. We can lift $\phi^{-1}(1)$ to $v \in \mathbb{T}^\dagger_{Q_m}$ with $\sigma(v) = \varepsilon v$ so that $v \mod (p^n, \delta_q^{p^n} - 1)_{q \in Q_m} = \phi^{-1}(1)$. Define $\Phi : \mathbb{T}_{Q_m} \to \mathbb{T}^\dagger_{Q_m}$ by $\Phi(t) = tv$. Then Φ is a $\mathbb{T}_{Q_m}$-linear map. By definition, $\Phi \mod (p^n, \delta_q^{p^n} - 1)_{q \in Q_m} = \phi^{-1}$; so, by Nakayama's lemma, Φ is onto. Since $\mathbb{T}_{Q_m}$ and $\mathbb{T}^\dagger_{Q_m}$ are W-free of equal rank, Φ must be an isomorphism. Thus $\Phi^{-1} \in \mathrm{Isom}_{\mathbb{T}_{Q_m}}(\mathbb{T}^\dagger_{Q_m}, \mathbb{T}_{Q_m})^\varepsilon$. □

We want to add one more datum $\phi_n \in \mathrm{Isom}_{R_n}(R^\dagger_n, R_n)^\varepsilon$ to the data $((R_n, \alpha), \widetilde{R}_n, (f_1, \dots, f_r), \sigma_n)$ which is required to satisfy the following compatibility condition:

(Q10) We have $\phi_n \in \mathrm{Isom}_{R_n}(R^\dagger_n, R_n)^\varepsilon$ with $\varepsilon \in \{\pm\}$ 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 $\pi : A \twoheadrightarrow B$. 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

$$\begin{tikzcd}
A \arrow[r, "\pi", "\twoheadrightarrow"'] & B \\
A^* \arrow[u, "\phi_A"', "\wr"] \arrow[r, "\varpi"] & B^*. \arrow[u, "\phi_B"', "\wr"]
\end{tikzcd}$$

By defining $\varpi := \phi_B^{-1} \circ \pi \circ \phi_A$, the above diagram is commutative. Thus we can always adjust $A^* \twoheadrightarrow B^*$ making the above diagram commutative. Suppose that A and B have involutions $\sigma_X \curvearrowright X$ for $X = A, B$. By duality, the involution σ_X acts on the dual X^*, which we denote by σ_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

$$\varpi \circ \sigma_A^* = \phi_B^{-1} \circ \pi \circ \phi_A \circ \sigma_A^* = \phi_B^{-1} \circ \pi \circ \varepsilon\sigma_A \circ \phi_A = \phi_B^{-1} \circ \varepsilon\sigma_B \circ \pi \circ \phi_A = \varepsilon^2 \sigma_B^* \circ \phi_B^{-1} \circ \pi \circ \phi_A = \sigma_B^* \circ \varpi.$$

Thus the adjusted ϖ commutes with the involution.

This remark shows that if we have a projective system $\{((R_n, \alpha), \widetilde{R}_n, (f_1, \dots, f_r), \sigma_n)\}_n$ satisfying (Q0–9), we can add the datum of an R_n-linear isomorphism $\phi_n : R^\dagger_n \overset{(4.5)}{=} R^*_n \cong R_n$ compatible with σ; i.e., (Q10) is automatically satisfied for ϕ_n induced by $\phi_{Q_{m(n)}}$, as long as we can take $\phi_{Q_{m(n)}} \in \mathrm{Isom}_{\mathbb{T}_{Q_{m(n)}}}(\mathbb{T}^\dagger_{Q_{m(n)}}, \mathbb{T}_{Q_{m(n)}})^\varepsilon$ with ε independent of $m(n)$. Explicitly, the compatibility of ϕ_n means the following:

(1) the datum ϕ_n satisfies $\phi_n \circ \sigma^*_n = \varepsilon\sigma_n \circ \phi_n$ for all n and for ε as in (Q10) independent of $m = m(n)$, and

(2) the projections $\pi_{n',n} : R_{n'} \twoheadrightarrow R_n$ and $\varpi_{n',n} : R^\dagger_{n'} = R^*_{n'} \twoheadrightarrow R^*_n = R^\dagger_n$ for all $n' > n$ commute with the involution in addition to the commutativity of the diagram:

$$\begin{tikzcd}
R_{n'} \arrow[r, "\pi_{n',n}", "\twoheadrightarrow"'] & R_n \\
R^\dagger_{n'} \arrow[u, "\phi_{n'}"', "\wr"] \arrow[r, "\varpi_{n',n}"] & R^\dagger_n. \arrow[u, "\phi_n"', "\wr"]
\end{tikzcd}$$

Now we again go through the Taylor-Wiles system argument made of the augmented tuples

$$((R_n,\alpha),\widetilde{R}_n,(f_1,\dots,f_r),\sigma_n,\phi_n)$$

with $\phi_n = (\phi_{Q_m} \mod (p^n, \delta_q^{p^n}-1)_{q\in Q_m}) \in \mathrm{Isom}_{R_n}(R_n^\dagger, R_n)^\varepsilon$ for $m = m(n)$; then, we obtain R_∞ with the limit involution σ_∞ and the limit isomorphism $\phi_\infty \in \mathrm{Isom}_{R_\infty}(R_\infty^\dagger, R_\infty)^\varepsilon$. Here $R_n^\dagger = \mathrm{Hom}_S(R_n, S_n)$. Thus we get

Corollary 4.8. *Suppose* (h0–4). *Then we can choose the Taylor–Wiles projective system*

$$((R_n,\alpha),\widetilde{R}_n,(f_1,\dots,f_r),\sigma_n,\phi_n)_n = ((R_{n,m(n)},\alpha_{n,m(n)}),\widetilde{R}_{n,m(n)},(f_1,\dots,f_r),\sigma_{n,m(n)},\phi_{n,m(n)})_n$$

satisfying (Q0–10). *If $\varepsilon = +$ in* (Q10), *then we conclude that R_∞^+ is a Gorenstein ring over $S = \mathcal{S}^G$, $R_\infty/\mathfrak{A}_{Q_m}R_\infty \cong R_{Q_m} \cong \mathbb{T}_{Q_m}$.*

Proof. For simplicity, write $A := R_{n',m(n')}$ and $B := R_{n,m(n)}$ for $n' \geq n$ and $m(n') \geq m(n)$. As we will see in Lemma 10.2 later, $\mathrm{Hom}(A^*, A)^\varepsilon \neq \emptyset$ and $\mathrm{Hom}(B^*, B)^\epsilon \neq \emptyset$ for a suitable choice of sign ε, ϵ. When F is imaginary, always $\varepsilon = \epsilon = +$ as we prove in Lemma 5.3. If F is real, choosing such sign and making the diagram in Remark 4.7 commutative, it is easy to see that $\varepsilon = \epsilon$ under these choices (although we do not need the case of F real in this paper). □

Here is a prototypical example of the rings of type R_∞, R_∞^+ corresponding to the choice $r_+ = r' = 0$ and $r_- = r'' = 1$:

Example 4.9. Consider $0 \neq \delta \in \mathfrak{m}_W$ and put

$$W[\sqrt{\delta}] = \begin{cases} W + W\sqrt{\delta} & \text{if } \delta \notin W^2, \\ \{(x,y) \in W \oplus W | (x \bmod \sqrt{\delta}) = y \bmod \sqrt{\delta})\} & \text{if } \sqrt{\delta} \in W. \end{cases}$$

Define

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

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 σ of $W[[T_-]]$ over $W[[T_-^2]]$ with $\sigma(T_-) = -T_-$ and $\sigma(S_-) = -S_-$.

For $Q \in \mathcal{Q}$, 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). *Let $\mathcal{Q}$ be the family satisfies* (Q0–10). *Let $Q \in \mathcal{Q}$ or $Q = \emptyset$. Suppose that σ is non-trivial on $\mathbb{T}_\emptyset$ (so, nontrivial on $\mathbb{T}^\emptyset$). Then we have $\varepsilon = +$ in* (Q10), *and the following three assertions holds.*

1. *We have $0 < r_- = \dim_{\mathbb{F}} \mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-\omega), \mathbb{F}) = r''$.*
2. *If $r_- = 1$, the $\mathbb{T}_+^Q$-module $\mathbb{T}_-^Q$ is generated by a single element over $\mathbb{T}_+^Q$.*
3. *If $r_- = 1$, the ring $\mathbb{T}_+ = \mathbb{T}_+^\emptyset$ is a local complete intersection over Λ. More generally, for $Q \in \mathcal{Q}$, the rings $\mathbb{T}_+^Q$ and $\mathbb{T}^Q$ are local complete intersection.*

Proof. By (Q9), σ is compatible with the projective system of tuples

$$((R_n,\alpha),\widetilde{R}_n,(f_1,\dots,f_r),\sigma_n) \in \mathcal{I}_n,$$

and by constancy of ε, we can find an isomorphism class $\mathcal{I}'_n$ with $|\mathcal{I}'_n| = \infty$ of the tuples

$$((R_n,\alpha),\widetilde{R}_n,(f_1,\dots,f_r),\sigma_n,\phi_n)$$

with an extra datum ϕ_n compatible with projections. Indeed, we will see in Lemma 5.3 that if σ is non-trivial on $\mathbb{T}^\emptyset$, we have $\mathrm{Isom}_{\mathbb{T}_{Q_m}}(\mathbb{T}_{Q_m}^\dagger, \mathbb{T}_{Q_m})^- = \emptyset$ for all m, where we recall $\mathbb{T}_{Q_m}^\dagger = \mathrm{Hom}_{W[\Delta_{Q_m}]^G}(\mathbb{T}_{Q_m}, W[\Delta_{Q_m}]^G)$, and hence $\mathrm{Isom}_{\mathbb{T}_{Q_m}}(\mathbb{T}_{Q_m}^\dagger, \mathbb{T}_{Q_m})^+ \neq \emptyset$ by Lemma 10.2 (1), proving $\varepsilon = +$ for ε in (Q10). As explained after Remark 4.7, by Lemma 4.6, we can add the datum ϕ_n to our tuples without changing the isomorphism class $\mathcal{I}_n$ as long as ε is constant for all Q_m. In other words,

$$((R_n,\alpha),\widetilde{R}_n,(f_1,\dots,f_r),\sigma_n,\phi_n) \mapsto ((R_n,\alpha),\widetilde{R}_n,(f_1,\dots,f_r),\sigma_n)$$

induces a bijection between $\mathcal{I}'_n$ and $\mathcal{I}_n$. Then by the finiteness of isomorphism classes of the tuples

$$((R_n,\alpha),\widetilde{R}_n,(f_1,\dots,f_r),\sigma_n,\phi_n)$$

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 $\phi_j\in\mathrm{Isom}_{R_j}(R_j^\dagger,R_j)^+$ $(j=n+1,n)$ for $R_j^\dagger=\mathrm{Hom}_{S_j}(R_j,S_j)$ with S_j as in Remark 4.5). Since $\mathcal{I}'_n$ and $\mathcal{I}_n$ are in bijection, hereafter we use the symbol $\mathcal{I}_n$ also for $\mathcal{I}'_n$ (identifying the two index sets).

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

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

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

We now claim that $r_->0$ if σ acts non-trivially on $\mathbb{T}^\emptyset=R^\emptyset$. Here is a proof of this claim. First assume that the class number of F is prime to p (so, $C=C_\emptyset$ in the introduction is trivial). Note that $\mathbb{T}^Q/I^Q\cong W[[H_Q]]$ for $I^Q:=\mathbb{T}^Q(\sigma-1)\mathbb{T}^Q$ 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 $I_\infty=\mathcal{R}(\sigma_\infty-1)\mathcal{R}$, we have $\mathcal{R}/I_\infty=\varprojlim_n W[[H_{Q_m}]]/\mathfrak{A}_n\cong W[[S_1^+,\dots,S_{r_+}^+]]$; so, $\dim\mathcal{R}=\dim\mathcal{R}/I_\infty$.

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

$$R^{Q_m}/I^{Q_m}\otimes_\Lambda\Lambda/(T)\cong W[C_{Q_m}]$$

for C_{Q_m} defined above Theorem B in the introduction. By [H16, Corollary 6.6], the ring $W[C_{Q_m}]$ determines functorially the group C_{Q_m}; so, the projection $R^{Q_{m(n+1)}}/\mathfrak{A}_{n+1}\twoheadrightarrow R^{Q_{m(n)}}/\mathfrak{A}_n$ induces a surjective group homomorphism

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

Here C_{Q_m} is as in the introduction. This tells us that we have a surjective group homomorphism $Z_{Q_m}/\Delta_{Q_{m(n+1)}}^{p^{n+1}}\twoheadrightarrow Z_{Q_{m(n)}}/\Delta_{Q_{m(n)}}^{p^n}$. Thus the sequence $\{Q_{m(n)}\}_n$ satisfies the requirement of the sequence in Proposition 1.5, and by Proposition 1.5, we have $\mathcal{R}/I_\infty=\varprojlim_n W[[H_{Q_m}]]/\mathfrak{A}_n$ which is free of finite rank over $\Lambda[[\boldsymbol{\Delta}]]=\Lambda[[\boldsymbol{\Delta}_+]]$; so, $\dim\mathcal{R}=\dim\mathcal{R}/I_\infty$ without assuming that the class number is prime to p. Thus, if $|Q^-|=0$, then $\mathrm{Spec}(\mathcal{R}/I_\infty)$ contains an irreducible component of the integral scheme $\mathrm{Spec}(\mathcal{R})$. This implies $\mathrm{Spec}(\mathcal{R})=\mathrm{Spec}(\mathcal{R}/I_\infty)$, and hence the involution σ acts trivially on $\mathcal{R}$, a contradiction (against the non-triviality of σ on $\mathbb{T}^\emptyset=\mathcal{R}/\mathfrak{A}_\emptyset\mathcal{R}$). Therefore we conclude that $r_-=|Q^-|>0$. This implies that $\mathcal{R}/I_\infty$ is a torsion S_Λ-module of finite type for $S_\Lambda=\Lambda[[\boldsymbol{\Delta}_+]][[(S_1^-)^2,\dots,(S_{r_-}^-)^2]]=\Lambda\widehat{\otimes}_W S$ with S as in Definition 4.3. Since $R_\infty/I_\infty\cong R_\infty^+/I_\infty^+$ has finite flat over $W[[\boldsymbol{\Delta}_+]]$ which is the ramification locus (fixed by σ_∞), we find that $r'=\dim_W\mathrm{Spec}(R_\infty/I_\infty)=\dim_W\mathrm{Spec}(W[[\boldsymbol{\Delta}_+]])=r_+$, which implies $0<r_-=r''$ as $r'+r''=r_++r_-$. The identity $r_-=\dim_{\mathbb{F}}\mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-\omega),\mathbb{F})$ follows from (3.9).

Since $\mathcal{R}$ is free of finite rank over S_Λ by the Auslander-Buchsbaum formula (e.g. [CMA, Theorem 19.9]), regularity of $\mathcal{R}$ implies that $\mathcal{R}$ is a Gorenstein ring over S_Λ; in particular, $\mathcal{R}^\dagger:=\mathrm{Hom}_{S_\Lambda}(\mathcal{R},S_\Lambda)\cong\mathcal{R}$ as $\mathcal{R}$-modules. By Corollary 4.8 (and (4.6)), ϕ_∞ commutes with σ_∞, and we conclude that $\phi_\infty:\mathrm{Hom}_S(R_\infty,S)\cong R_\infty$ induces $\phi_\infty^+:\mathrm{Hom}_S(R_\infty^+,S)\cong R_\infty^+$ as R_∞^+-modules. Since $\mathcal{R}_+/(t-\gamma^k)\mathcal{R}_+\cong R_\infty^+$, $\mathcal{R}_+$ is Gorenstein by [CRT, Exercise 18.1], and by Lemma 10.1, $\mathcal{R}_+^\dagger:=\mathrm{Hom}_{S_\Lambda}(\mathcal{R}_+,S_\Lambda)\cong\mathcal{R}_+$ as $\mathcal{R}_+$-modules.

Suppose $r_-=r''=1$. Let $\mathcal{S}_\Lambda=\mathcal{S}\widehat{\otimes}_W\Lambda=\Lambda[[\boldsymbol{\Delta}]]$. Then plainly $\mathcal{S}_\Lambda$ is flat over $\mathcal{S}_\Lambda^+:=\mathcal{S}_\Lambda^{\mathcal{G}}$. By Lemma 10.4, $\mathcal{R}_-$ is generated over $\mathcal{R}_+$ by a single element δ with $\sigma(\delta)=-\delta$. If a power series $\Phi(T_{1,+},\dots,T_{r-1,+},T_{1,-})$ is fixed by σ_∞, by equating the coefficients of the identity:

$$\Phi(T_{1,+},\dots,T_{r-1,+},T_{1,-})=\sigma(\Phi(T_{1,+},\dots,T_{r-1,+},T_{1,-}))=\Phi(T_{1,+},\dots,T_{r-1,+},-T_{1,-}),$$

we find that Φ is actually a power series of $(T_{1,+},\dots,T_{r-1,+},T_{1,-}^2)$. Thus the fixed part $\mathcal{R}_+:=\mathcal{R}^G$ for $G=\mathcal{G}=\{\mathrm{id},\sigma_\infty\}$ is still a power series ring, and we have $\mathcal{R}_+=\Lambda[[T_{1,+},\dots,T_{r-1,+},T_{1,-}^2]]$. Since $\mathbb{T}_\emptyset=\varprojlim_m\widetilde{R}_m$ by the original Taylor–Wiles argument (e.g., [HMI, page 194]), lifting it to Λ, we get $\mathbb{T}=\mathbb{T}^\emptyset=\mathcal{R}/\mathfrak{A}_\emptyset\mathcal{R}$ and $\mathbb{T}_-$ is the surjective image of $\mathcal{R}_-$. Since $\mathcal{R}_-$ is generated by one element δ over $\mathcal{R}_+$ (which can be given by $T_{1,-}$), its image $\mathbb{T}_-$ in $\mathbb{T}$ is generated by one element θ over $\mathbb{T}_+$. This proves the assertion (2) for $Q=\emptyset$.

For a given $Q = Q_{m_0} \neq \emptyset$, we take n_0 such that $p^{n_0} = \max_{q \in Q}(|\Delta_q|)$. Then we restart the Taylor-Wiles argument from $\mathbb{T}_Q$ in place of $\mathbb{T}_\emptyset$. In other words, we consider the projective system for $n \geq n_0$:

$$((R_n, \alpha), \widetilde{R}_{Q,n}, (f_1, \dots, f_r), \sigma_n, \phi_n) \in \mathcal{I}_n \tag{4.7}$$

for $\widetilde{R}_{Q,n} = R_n/((p^n) + \mathfrak{A}_Q)R_n$. Then by the same argument, we get

$$\mathbb{T}_Q \cong \varprojlim_{n \geq n_0} \widetilde{R}_{Q,n} = R_\infty/\mathfrak{A}_Q.$$

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

We now prove (3). Since $r'' = r_- = 1$, we can write $Q^+ = Q^+_m = \{q_1, \dots, q_{r-1}\}$ and $Q^- = Q^-_m = \{q_r\}$. Recall $\mathcal{S}_\Lambda = \mathcal{S}\widehat{\otimes}_W\Lambda = \Lambda[[\boldsymbol{\Delta}]]$, and write $\{s_j = 1 + S_j\}_{j=1,\dots,r}$ for the basis of $\boldsymbol{\Delta}$ corresponding to $\varprojlim_m \delta_{q_j}$. Since $r'' = r_- = 1$, $\mathcal{R}_+ = \Lambda[[T_{1,+}, \dots, T_{r-1,+}, T^2_{1,-}]]$ and $\mathfrak{s}_Q = \mathfrak{A}_Q \cap S_\Lambda$ is generated by an S-sequence

$$\{s_1^{|\Delta_{q_1}|} - 1, \dots, s_{r-1}^{|\Delta_{q_{r-1}}|} - 1, s_r^{|\Delta_{q_r}|} + s_r^{-|\Delta_{q_r}|} - 2\}$$

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

$$\begin{aligned}\mathfrak{b}_Q := \mathrm{Ker}(\mathcal{R}_+/\mathfrak{s}_Q\mathcal{R}_+ \to \mathbb{T}^Q_+ \subset \mathbb{T}^Q) &= \mathrm{Ker}(\mathcal{R} \to \mathbb{T}^Q) \cap \mathcal{R}_+ \\ &= \mathfrak{A}_Q\mathcal{R} \cap \mathcal{R}_+ = H^0(G, \mathfrak{A}_Q\mathcal{R}) = \mathfrak{s}_Q + (T_{1,-}(s_r^{|\Delta_{q_r}|} - s_r^{-|\Delta_{q_r}|})),\end{aligned}$$

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

$$\{s_1^{|\Delta_{q_1}|} - 1, \dots, s_{r-1}^{|\Delta_{q_{r-1}}|} - 1, T_{1,-}(s_r^{|\Delta_{q_r}|} - s_r^{-|\Delta_{q_r}|})\}.$$

Since S_j $(j \leq r-1)$ is fixed by σ, we find that $\mathbb{T}^Q_+ = \Lambda[[T_{1,+}, \dots, T_{r-1,+}, T^2_{1,-}]]/\mathfrak{b}_Q$ is a local complete intersection. □

5. Proof of Theorem B

In Sections 5–9, unless otherwise mentioned, we assume that $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}$ for the imaginary quadratic field F. Let Q be either $Q \in \mathcal{Q}$ as in Theorem 4.10 or $Q = \emptyset$. Thus $\mathbb{T}^\emptyset = \mathbb{T}$ by our convention. So, when $Q = \emptyset$, we omit the superscript or subscript "Q" from the notation. Recall the fixed integer $k \geq 1$ and the local direct summand $\mathbb{T}_Q = \mathbb{T}^Q/(t - \gamma^k)\mathbb{T}^Q$ of $\mathbf{h}_{Q,k,\psi_k}$. Since we use the anticyclotomic Katz p-adic L-function L_p^- defined as an element of $W[[H]]$, the base ring W is a finite extension of $W(\overline{\mathbb{F}}_p)$ (see [Ka78]), though, replacing L_p^- by a generator of the ideal (L_p^-) 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 $\mathbb{T}^Q/I^Q \cong W[[H_Q]]$. Write $\mathbb{K} := \mathrm{Frac}(\Lambda)$ for the weight Iwasawa algebra Λ. Since $\mathbb{T}^Q$ is a reduced algebra finite flat over Λ (cf. [H13, Corollary 1.3]), we have $\mathrm{Frac}(\mathbb{T}^Q) = \mathbb{T}^Q \otimes_\Lambda \mathbb{K} = X \oplus \mathrm{Frac}(W[[H_Q]])$ for a ring direct summand X. Put $\mathbb{T}^{Q,\mathrm{ncm}}$ for the image of $\mathbb{T}^Q$ in X. Then we have $I^Q = (\mathbb{T}^{Q,\mathrm{ncm}} \oplus 0) \cap \mathbb{T}^Q$ in $\mathrm{Frac}(\mathbb{T}^Q)$. In particular, the involution σ_Q preserves the quotient ring $\mathbb{T}^{Q,\mathrm{ncm}}$ as an automorphism of $\mathrm{Frac}(\mathbb{T}^Q)$.

Since $W[[H_Q]]$ is Λ-free of finite rank, the exact sequence of Proposition 2.6

$$0 \to I^Q \to \mathbb{T}^Q \to W[[H_Q]] \to 0$$

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

$$\begin{tikzcd} W[[H_Q]]^\vee \arrow[r, hook] \arrow[d, "\wr"'] & (\mathbb{T}^Q)^\vee \arrow[r, two heads] \arrow[d, "\wr"'] & (I^Q)^\vee \arrow[d, "\wr"'] \\ W[[H_Q]] \arrow[r, hook] & \mathbb{T}^Q \arrow[r, two heads] & \mathbb{T}^{Q,\mathrm{ncm}}. \end{tikzcd}$$

Thus we get

Lemma 5.1. *Suppose* (h0–4)*. Let* $\mathfrak{a}_Q := \mathbb{T}^Q \cap (0 \oplus \mathrm{Frac}(W[[H_Q]]) = \mathrm{Ker}(\mathbb{T}^Q \twoheadrightarrow \mathbb{T}^{Q,\mathrm{ncm}})$*. Then* $\mathfrak{a}_Q$ *is a principal ideal generated by* $a_Q \in \mathbb{T}^Q_+$ *in* $\mathbb{T}^Q_+$ *isomorphic to* $W[[H_Q]]$ *as* $\mathbb{T}^Q_+$*-modules.*

We find $a_Q \in \mathbb{T}^Q_+$ since $W[[H_Q]]$ is fixed by σ_Q.

If $Q = \emptyset$, we have the anticyclotomic Katz measure $L_p^- \in W[[Z_p^-]]$ with branch character given by the anticyclotomic projection φ^- of the Teichmüller lift φ of $\overline{\varphi}$ (see [H15, §6]). 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* $\mathfrak{a} = \mathfrak{a}_\emptyset$ *is generated by* $L_p^- \in W[[H]]$*.*

Let $\mathbb{T}^Q_\pm = \{x \in \mathbb{T}^Q | x^\sigma = \pm x\}$, $\mathbb{T}^{Q,\mathrm{ncm}}_\pm = \{x \in \mathbb{T}^{Q,\mathrm{ncm}} | x^\sigma = \pm x\}$, $\mathbb{T}^\pm_Q = \{x \in \mathbb{T}_Q | x^\sigma = \pm x\}$ and $I^Q_\pm = \{x \in I^Q | x^\sigma = \pm x\}$. Since no irreducible components of $\mathrm{Spec}(\mathbb{T}^{Q,\mathrm{ncm}})$ is fixed by σ_Q and $I^Q = \mathbb{T}^Q(\sigma_Q - 1)\mathbb{T}^Q = \mathbb{T}^Q \cdot \mathbb{T}^Q_-$, we have $\mathbb{T}^Q_- = \mathbb{T}^{Q,\mathrm{ncm}}_- = I^Q_-$. Also $I^Q \subset \mathbb{T}^{Q,\mathrm{ncm}}$, as I^Q is generated by $\mathbb{T}^Q_- \subset \mathbb{T}^{Q,\mathrm{ncm}}$. Taking σ_Q-invariant, from $\mathbb{T}^Q/I^Q = W[[H_Q]]$, we conclude $\mathbb{T}^Q_+/I^Q_+ = W[[H_Q]]$.

We now prove the following key lemma.

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

$$\mathrm{Isom}_{\mathbb{T}^Q}((\mathbb{T}^Q)^\vee, \mathbb{T}^Q)^- = \mathrm{Isom}_{\mathbb{T}_Q}(\mathbb{T}^*_Q, \mathbb{T}_Q)^- = \emptyset,$$

where $M^* = \mathrm{Hom}_W(M, W)$ *and* $M^\vee = \mathrm{Hom}_\Lambda(M, \Lambda)$*.*

In the lemma, we can replace $\mathbb{T}^*_Q$ (resp. $(\mathbb{T}^Q)^\vee$) by $\mathrm{Hom}_{S_Q}(\mathbb{T}_Q, S_Q)$ (resp. $\mathrm{Hom}_{S_{\Lambda,Q}}(\mathbb{T}^Q, S_{\Lambda,Q})$) for the image S_Q (resp. $S_{\Lambda,Q}$) of S (resp. S_Λ) 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 $\mathbb{T}^Q$, we prove the lemma for $\mathbb{T}_+ = \mathbb{T}^\emptyset_+$.

Let $C := \mathrm{Gal}(F_{\mathfrak{cp}}/F)$ for the maximal p-abelian extension $F_{\mathfrak{cp}}/F$ of conductor dividing $\mathfrak{cp}$. Then C is isomorphic to $C_\emptyset$ in the introduction as in (1.6). Since $\mathbb{T}/I = W[[H]]$ by Corollary 2.5 and $W[[H]]$ is Λ-free of rank $|C|$, I is a Λ-direct summand of $\mathbb{T}$, and hence I is Λ-free. Taking the Λ-dual sequence of $0 \to I \to \mathbb{T} \to W[[H]] \to 0$ (with all Λ-free terms), we have another exact sequence: $0 \leftarrow I^\vee \leftarrow \mathbb{T}^\vee \leftarrow W[[H]]^\vee \to 0$ of $\mathbb{T}$-modules. By Theorem 2.1, $\mathbb{T}$ 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 $\mathbb{T}^\vee \cong \mathbb{T}$ and $W[[H]]^\vee \cong W[[H]]$ as $\mathbb{T}$-modules. From this, we conclude $\mathbb{T}^{\mathrm{ncm}} \cong I^\vee$. Thus $\mathbb{T}^{\mathrm{ncm}}$ is Λ-free and is non-trivial as σ acts on $\mathbb{T}$ non-trivially. Since $\mathbb{T}^{\mathrm{ncm}}$ is reduced (by cube-freeness of N; see [H13, Corollary 1.3]) and there is no irreducible component of $\mathrm{Spec}(\mathbb{T}^{\mathrm{ncm}})$ on which σ-acts trivially, $\mathrm{Frac}(\mathbb{T}^{\mathrm{ncm}}) = \mathbb{T}^{\mathrm{ncm}} \otimes_\Lambda \mathbb{K}$ is equal to $\mathrm{Frac}(\mathbb{T}^{\mathrm{ncm}}_+) \oplus \mathrm{Frac}(\mathbb{T}^{\mathrm{ncm}}_+)\delta$ for a non-zero divisor δ with $\delta^2 \in \mathrm{Frac}(\mathbb{T}^{\mathrm{ncm}}_+)$. In other words, $\mathrm{Frac}(\mathbb{T}^{\mathrm{ncm}})$ is a $\mathrm{Frac}(\mathbb{T}^{\mathrm{ncm}}_+)$-free module of rank 2, and $\mathbb{T}^{\mathrm{ncm}}_- \otimes_\Lambda \mathbb{K} = \mathbb{T}_- \otimes_\Lambda \mathbb{K}$ is a $\mathrm{Frac}(\mathbb{T}^{\mathrm{ncm}}_+)$-free module of rank 1. In particular, we have

$$\mathrm{rank}_\Lambda \mathbb{T}^{\mathrm{ncm}}_+ = \mathrm{rank}_\Lambda \mathbb{T}^{\mathrm{ncm}}_- = \mathrm{rank}_\Lambda \mathbb{T}_- > 0. \tag{5.1}$$

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

$$\mathbb{T}^{\mathrm{ncm}}/I \cong \mathbb{T}^{\mathrm{ncm}} \otimes_{\mathbb{T}} W[[H]] \cong W[[H]]/(L_p^-), \tag{5.2}$$

which is a torsion Λ-module. Thus we get

$$\mathrm{rank}_\Lambda I_\pm = \dim_{\mathbb{K}} I_\pm \otimes_\Lambda \mathbb{K} = \dim_{\mathbb{K}} \mathrm{Frac}(\mathbb{T}^{\mathrm{ncm}}_\pm) = \mathrm{rank}_\Lambda \mathbb{T}^{\mathrm{ncm}}_\pm \overset{(5.1)}{=} \mathrm{rank}_\Lambda \mathbb{T}_-. \tag{5.3}$$

Taking the σ-invariant of the two sides of the identity $\mathbb{T}/I = W[[H]]$, we have $\mathbb{T}_+/I_+ \cong W[[H]]$. Thus we get

$$\mathrm{rank}_\Lambda \mathbb{T}_+ = \mathrm{rank}_\Lambda I_+ + \mathrm{rank}_\Lambda W[[H]] = \mathrm{rank}_\Lambda \mathbb{T}_- + \mathrm{rank}_\Lambda W[[H]] > \mathrm{rank}_\Lambda \mathbb{T}_- > 0. \tag{5.4}$$

By Lemma 10.2 (2) applied to $A = \mathbb{T}$ and $S = \Lambda$, $\phi \in \mathrm{Isom}_{\mathbb{T}}(\mathbb{T}^\vee, \mathbb{T})$ must commutes with the involution; so, we get $\mathrm{Isom}_{\mathbb{T}^Q}(\mathbb{T}^\vee, \mathbb{T})^+ \neq \emptyset$ and $\mathbb{T}_+ \cong \mathbb{T}_+^\vee$. Thus $\mathbb{T}_+$ is a Gorenstein ring (by Lemma 10.1) as well as $\mathrm{Isom}_{\mathbb{T}}(\mathbb{T}^\vee, \mathbb{T})^- = \emptyset$. □

We want to prove the following slightly stronger version of Theorem B in the introduction allowing the case when $p|h_F$:

Theorem 5.4. *Assume* (h0–4). *Suppose that σ acts non-trivially on $\mathbb{T}$. Then the following four statements are equivalent:*

1. *The rings $\mathbb{T}^{\mathrm{ncm}}$ and $\mathbb{T}_+^{\mathrm{ncm}}$ are both local complete intersections.*
2. *The $\mathbb{T}^{\mathrm{ncm}}$-ideal $I = \mathbb{T}(\sigma - 1)\mathbb{T} \subset \mathbb{T}^{\mathrm{ncm}}$ is principal and is generated by a non-zero-divisor $\theta \in \mathbb{T}_- = \mathbb{T}_-^{\mathrm{ncm}}$ with $\theta^2 \in \mathbb{T}_+^{\mathrm{ncm}}$. The element θ generates a free $\mathbb{T}^{\mathrm{ncm}}$-module $\mathbb{T}_-$, and $\mathbb{T}^{\mathrm{ncm}} = \mathbb{T}_+^{\mathrm{ncm}}[\theta]$ is free of rank 2 over $\mathbb{T}_+^{\mathrm{ncm}}$.*
3. *The Iwasawa module $\mathcal{Y}^-(\varphi^-)$ is cyclic over $W[[H]]$.*
4. *The Iwasawa module $\mathcal{Y}^-(\varphi^-\omega)$ is cyclic over $W[[H]]$.*

Under these equivalent conditions, the ring $\mathbb{T}_+$ is a local complete intersection (not just a Gorenstein ring).

Note here that $H = \Gamma_- \cong \Gamma$ if $p \nmid h_F$ and that $\mathrm{rank}_W W[[H]]/(L_p^-)$ is the sum of the Iwasawa λ-invariant of the branches of the p-adic L-function L_p^- since the μ-invariant of L_p^- vanishes by [H10, Theorem I]. Thus if $p \nmid h_F$, we have $\mathcal{Y}^-(\xi) = Y^-(\xi)$.

Proof. For simplicity, we write $A := \mathbb{T}^{\mathrm{ncm}}$ and $A_+ := \mathbb{T}_+^{\mathrm{ncm}}$ and $S = W$. Suppose (1). Then A, A_+ are local complete intersections; so, Gorenstein. Thus the different inverse $\mathfrak{d}_{A/A_+}^{-1}$ and $\mathfrak{d}_{A/W}^{-1}$ are A-free modules of rank 1 and $\mathfrak{d}_{A_+/W}^{-1}$ is an A_+-module of rank 1. (See Section 10 for the definition of the different inverse). Since

$$\mathrm{Spec}(A)^{\sigma=1} = \mathrm{Spec}(A/I) \cong \mathrm{Spec}(W[[H]]/(L_p^-)) = \mathrm{Spec}(A_+/I_+),$$

the ramified locus of $\mathrm{Spec}(\mathbb{T}^{\mathrm{ncm}})$ is a non-trivial divisor given by the zero set of L_p^- which is a non-zero divisor of $W[[H]]$. Thus $\mathfrak{d}_{A/A_+}$ is the characteristic ideal (L_p^-) (by a theorem of Tate [MR70, A.3]; see also [MFG, Lemma 5.21]), which is contained in $\mathfrak{m}_A$. Thus by Lemma 10.4, 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 $\mathbb{T}^{\mathrm{ncm}}/I \cong W[[H]]/(L_p^-)$ and by the technique of [MT90] (see also [H16, §6.3.6]), we have an isomorphism $\mathcal{Y}^-(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W \cong \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} W[[H]]$ as Λ–modules, where φ is the unique character satisfying the assumption of the anticyclotomic cyclicity conjecture such that $\chi\varphi|_{\mathbb{A}^\times}$ is the Teichmüller lift of $\det(\overline{\rho})$ (i.e., the Neben character of $\mathbf{h}$). Thus we conclude $L_p = L_p(\varphi^-)$ 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:

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

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

$$\Lambda/(L_p(\varphi^-)) \cong \mathbb{T}^{\mathrm{ncm}}/(\theta) \xrightarrow[\sim]{x \mapsto \theta x} (\theta)/(\theta)^2 \cong \mathcal{Y}^-(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W.$$

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 $t_Q^* \cong \mathrm{Sel}_Q(Ad)$ and its minus-eigenspace for σ_Q is is isomorphic to $\mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-), \mathbb{F})$ by (3.5). Thus I_Q/I_Q^2 is generated by one element over $W[\Delta_Q]$. Consider the Taylor Wiles system $(R_n, \ldots)_n$ as in (3.1). Writing $I_n = R_n(\sigma_n - 1)R_n$ for the involution σ_n of R_n. Since I_n/I_n^2 is the image of $I_{Q_{m(n)}}/I_{Q_{m(n)}}^2$, it is generated by one element over R_n. Since $I_\infty/I_\infty^2 = \varprojlim_n I_n/I_n^2$, $I_\infty/I_\infty^2 \otimes_{R_\infty} \mathbb{F}$ factor through $I_n/I_n^2 \otimes_{R_n} \mathbb{F}$ for some n; so, I_∞/I_∞^2 is generated by one element over R_∞^+. Since $R_\infty = W[[T_1^+, \ldots, T_{r'}^+, T_1^-, \ldots, T_{r''}^-]]$, I_∞/I_∞^2 is generated by r'' elements over R_∞, we conclude $r'' = 1$. Since $r'' = r_-$ by Theorem 4.10 (1) and $r_- = \dim \mathrm{Hom}_{W[[H_Q]]}(\mathcal{Y}_Q^-(\varphi^-\omega), \mathbb{F})$ for all Q

including $Q = \emptyset$ by Proposition 3.6, we conclude $r^- = 1$ and $\mathcal{Y}^-(\varphi^-\omega)$ 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 $r_- = 1 = r''$ by Theorem 4.10 (1). Then $\mathbb{T}_-$ is generated by a non-zero divisor θ by Theorem 4.10 (2), and I_+ is generated by θ^2. This implies $\mathbb{T}^{\mathrm{ncm}}/(\theta) \cong W[[H]]/(L_p^-) \cong \mathbb{T}_+^{\mathrm{ncm}}/(\theta^2)$. Since $W[[H]]/(\theta)$ is a local complete intersection over W, by Lemma 5.5 below, the assertion (1) holds. Moreover, by Theorem 4.10 (3), $\mathbb{T}_+$ 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 Λ. Then A is a local complete intersection if and only if for a non-zero divisor $\delta \in \mathfrak{m}_A$, $A/(\delta)$ is a local complete intersection.*

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

We now prove the "only if"-part. Let $(a_1, \dots, a_m)$ be a sequence generating $\mathfrak{a}$. Pick a non-zero divisor $\delta \in \mathfrak{m}_A$ and lift it to $\widetilde{\delta} \in \Lambda[[x_1, \dots, x_m]]$. Then plainly $(a_1, \dots, a_m, \widetilde{\delta})$ is a regular $\Lambda[[x_1, \dots, x_m]]$-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_p^- to each irreducible component of* $\mathrm{Spec}(W[[H]])$ *is square-free.*

Note that each irreducible component of $\mathrm{Spec}(W[[H]])$ is the spectrum of a regular local ring $\boldsymbol{\Lambda} := W[[\Gamma_-]]$, which is a unique factorization domain; so, square-freeness of elements of $\boldsymbol{\Lambda}$ is well defined. If $\mathfrak{c}$ is divisible by non-split primes, there are some cases where L_p^- is divisible by p^2 (e.g., [H10, §5.5]). 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)$_\chi$ in No.62 and see also U3]). Thus the above conjecture is an anti-cyclotomic version of Iwasawa's semi-simplicity conjecture.

6. Proof of $r_- = \dim_{\mathbb{F}} \mathrm{Sel}^{\perp}_{\mathbb{Q}}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^- \overline{\omega}) \le 1$ and Theorem A

In this section, we first study mod p Selmer groups of an induced representation for $F/\mathbb{Q}$ via classical Kummer's theory and prove $r_- \le 1$ which proves Theorem A via Theorem B. Take an anti-cyclotomic finite order character ϕ of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, and recall $F(\phi)$ which is the splitting field $\overline{\mathbb{Q}}^{\mathrm{Ker}(\phi)}$. Write $\mathfrak{R}$ for the integer ring of $F(\phi)$. We study Galois module structure of $\mathfrak{R}^\times \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}$:

Proposition 6.1. *Write a for the order of ϕ. Then we have*

$$\mathfrak{R}^\times \otimes_{\mathbb{Z}} \overline{\mathbb{Q}} \cong \begin{cases} \xi \oplus \bigoplus_{j=1}^{b-1} \mathrm{Ind}_F^{\mathbb{Q}} \phi^j & \text{if } a \text{ is even with } a = 2b, \\ \bigoplus_{j=1}^{b} \mathrm{Ind}_F^{\mathbb{Q}} \phi^j & \text{if } a \text{ is odd with } a = 2b+1, \end{cases}$$

as $\mathrm{Gal}(F(\phi)/\mathbb{Q})$*-modules, where $\xi : \mathrm{Gal}(F(\phi)/\mathbb{Q}) \to \{\pm 1\}$ is a quadratic character such that $\xi|_{\mathrm{Gal}(F(\phi)/F)} = \phi^b$ and ξ is even at the infinite place of $\mathbb{Q}$.*

Proof. If $a = 2$, we have $\mathrm{Gal}(F(\phi)/\mathbb{Q}) \cong \{\pm 1\}^2$ as $\mathrm{Im}(\mathrm{Ind}_F^{\mathbb{Q}} \phi)$ is dihedral of order 4. Since complex conjugation $c \in \mathrm{Gal}(F(\phi)/\mathbb{Q})$ fixes a unique totally real quadratic extension $k'/\mathbb{Q}$ with $\xi = \left(\frac{k'/\mathbb{Q}}{}\right)$. Then $F(\phi)$ is a CM quadratic extension of k', and the assertion is clear.

Now suppose that $a > 2$ is even. The fixed field $F(\phi^b)$ of $\mathrm{Im}(\phi^2) \subset \mathrm{Im}(\phi) = \mathrm{Gal}(F(\phi)/F)$ is the composite of F and another quadratic extension k' of $\mathbb{Q}$. By the argument in the case of $a = 2$, we may assume that k' is real, and Fk' contains another imaginary quadratic extension $F'_{/\mathbb{Q}}$. Thus $\xi := \left(\frac{k'/\mathbb{Q}}{}\right)$ has multiplicity 1 in $\mathfrak{R}^\times \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}$ as the unit group of k' has rank 1. The maximal abelian quotient of $\mathrm{Gal}(F(\phi)/\mathbb{Q})$ is equal to $\mathrm{Gal}(Fk'/\mathbb{Q})$. Writing $a = 2b$ with $1 < b \in \mathbb{Z}$, the action of $\mathrm{Gal}(F(\phi)/\mathbb{Q})$ on $\mathfrak{R}^\times \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}$ is therefore isomorphic to

$$\mathfrak{R}^\times \otimes_{\mathbb{Z}} \overline{\mathbb{Q}} \cong \xi \oplus \bigoplus_{j=1}^{b-1} m(j)\,\mathrm{Ind}_F^{\mathbb{Q}} \phi^j,$$

since $\{\phi^j, \phi^{-j}\}$ $(j = 1, \dots, b-1)$ and $\{\phi^b = \xi|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}\}$ give conjugacy classes of characters under conjugation of c. Therefore we have $1 + \sum_j 2m(j) = a - 1$; so,

$$\sum_j m(j) = (b-1).$$

Write $\Sigma(\phi)$ for the set of infinite places of $F(\phi)$. The $\mathrm{Gal}(F(\phi)/\mathbb{Q})$-module $\mathfrak{R}^\times \otimes_{\mathbb{Z}} \mathbb{C}$ is embedded into the Galois module $\mathrm{Im}(\mathrm{Tr}_{\mathbb{C}/\mathbb{R}} : F(\phi) \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{R}^{\Sigma(\phi)}) \otimes_{\mathbb{R}} \mathbb{C}$ by the $(x_v)_v \otimes z \mapsto (z \log |x_v|^2)_v$ for infinite places v of $F(\phi)$ (e.g., the proof of Dirichlet's unit theorem). The cokernel of this embedding is identified with the trivial $\mathrm{Gal}(F(\phi)/\mathbb{Q})$-module $\mathbb{C}$ by the degree map $\deg(x_v) = \sum_v x_v$. Let $\mathrm{Gal}(F(\phi)/\mathbb{Q})$ act on $\Sigma(\phi)$ by permutation; so, the space of $\mathbb{C}$-valued functions $\mathbb{C}[\Sigma(\phi)]$ on $\Sigma(\phi)$ is a $\mathrm{Gal}(F(\phi)/\mathbb{Q})$-module. The $\mathrm{Gal}(F(\phi)/\mathbb{Q})$-module $\mathrm{Im}(\mathrm{Tr}_{\mathbb{C}/\mathbb{R}} : F(\phi) \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{R}^{\Sigma(\phi)}) \otimes_{\mathbb{R}} \mathbb{C}$ is isomorphic to $\mathbb{C}[\Sigma(\phi)]$. We claim

$$\mathbb{C}[\Sigma(\phi)] \cong \mathbf{1} \oplus \xi \oplus \bigoplus_{j=1}^{b-1} \mathrm{Ind}_F^{\mathbb{Q}} \phi^j \tag{6.1}$$

We prove this claim. The complex conjugation ϱ_v at v coincide with c on F, and hence $\mathrm{Ind}_F^{\mathbb{Q}} \phi^j$ for all $j = 1, \dots, b-1$ appears in addition to real characters ξ and $\mathbf{1}$. Since complex conjugation acts non-trivially on $F_\infty = \mathbb{C}$, this shows the desired formula from the exact sequence $\mathfrak{R}^\times \otimes_{\mathbb{Z}} \mathbb{C} \hookrightarrow \mathbb{C}[\Sigma(\phi)] \twoheadrightarrow \mathbb{C}$.

We now assume that $a = 2b + 1$ is odd. Then we have

$$\mathbb{C}[\Sigma(\phi)] \cong \mathbf{1} \oplus \bigoplus_{j=1}^{2b} \phi^j \tag{6.2}$$

as $\mathrm{Gal}(F(\phi)/F)$-modules, and $c \in \mathrm{Gal}(F/\mathbb{Q})$ interchanges ϕ^j and ϕ^{-j}, which implies

$$\mathbb{C}[\Sigma(\phi)] \cong \mathbf{1} \oplus \bigoplus_{j=1}^{b} \mathrm{Ind}_F^{\mathbb{Q}} \phi^j \tag{6.3}$$

as $\mathrm{Gal}(F(\phi)/\mathbb{Q})$-modules. Thus we conclude the desired formula. □

Recall the fixed embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ and $\mathfrak{p} := \{x \in O : |i_p(x)| < 1\}$. Then $(p) = \mathfrak{p}\mathfrak{p}^c$ with $\mathfrak{p} \neq \mathfrak{p}^c$. Let $\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \overline{\mathbb{Q}}^\times$ be a character of order prime to p with prime-to-p conductor $\mathfrak{c}$ as in the introduction. Let $\phi = \varphi^-$; so, $\mathfrak{R}$ is the integer ring of the splitting field $F(\varphi^-)$ of φ^-. Write $Cl_{F(\varphi^-)}$ for the class group of $F(\varphi^-)$ which is a $\mathrm{Gal}(F(\varphi^-)/\mathbb{Q})$-module. Recall $X[\overline{\varphi}^-] = X[\varphi^-] = \{x \in X | \tau x = \overline{\varphi}^-(\tau)x \text{ for all } \tau \in \mathrm{Gal}(F(\varphi^-)/F)\}$ for a $\mathbb{F}[\mathrm{Gal}(F(\varphi^-)/F)]$-module X; in particular,

$$(Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F})[\overline{\varphi}^-] = \{x \in Cl_{F(\varphi^-)} | x^\tau = \overline{\varphi}^-(\tau)x \text{ for all } \tau \in \mathrm{Gal}(F(\varphi^-)/F)\}.$$

Consider $\mathfrak{E} := \mathrm{Ker}(N_{F(\varphi^-)/F} : \mathfrak{R}^\times \to O^\times)$ to study $\mathrm{Sel}_\emptyset^\perp(\overline{\varphi}^-\overline{\omega}) := \mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-\omega), \mathbb{F})$. We write a for the exponent of $\mathfrak{E}$ modulo the radical $\sqrt{\mathfrak{p}^c}$ of $\mathfrak{p}^c$ in $\mathfrak{R}$ (i.e., a is the minimal positive integer so that $\varepsilon^a \equiv 1 \mod \sqrt{\mathfrak{p}^c}$ for all $\varepsilon \in \mathfrak{E}$). Since $-1 \in \mathfrak{E}$ (and $p > 2$), a is even, and plainly a is prime to p. Let $\mathfrak{E}_- := \{\varepsilon^a | \varepsilon \in \mathfrak{E}\}$. Put $\mathfrak{E}_+ = \mathfrak{E}_- \cap (1 + \sqrt{\mathfrak{p}^c}\mathfrak{R}_{\mathfrak{p}^c})^p$ for the $\sqrt{\mathfrak{p}^c}$-adic completion $\mathfrak{R}_{\mathfrak{p}^c}$ of $\mathfrak{R}$. Thus $\mathfrak{E}_+ \supset \mathfrak{E}_-^p$.

Proposition 6.2. *Let the notation be as above, and assume that $p \geq 5$. Then we have*

$$\mathrm{Sel}_\emptyset^\perp(\overline{\varphi}^-\overline{\omega}) = \mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-\omega), \mathbb{F}) \cong (\mathfrak{E}_+/\mathfrak{E}_-^p \otimes_{\mathbb{F}_p} \mathbb{F})[(\overline{\varphi}^-)^{-1}]$$

if $(Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F})[\overline{\varphi}^-] = 0$. So, we have $\dim_{\mathbb{F}} \mathrm{Sel}_\emptyset^\perp(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-\overline{\omega}) \leq 1$ if $(Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F})[\overline{\varphi}^-] = 0$.

Note here the action of $\gamma \in \mathrm{Gal}(F(\varphi^-\omega)/F)$ on $f \in \mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-\omega), \mathbb{F})$ is given by $\gamma f(x) = f(\gamma^{-1}x) = (\overline{\varphi}^-\overline{\omega})^{-1}(\gamma)f(x)$. We also note that $\varphi^-(c\gamma c^{-1}) = (\varphi^-)^{-1}(\gamma)$; so, by applying c, we have an equivalence $(Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F})[\overline{\varphi}^-] = 0 \Leftrightarrow (Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F})[(\overline{\varphi}^-)^{-1}] = 0$.

Proof. We first give a constructive proof when $\overline{\varphi}^-$ has values $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and after that, we give a shorter cohomological proof in the general case. Take $\varepsilon \in \mathfrak{E}_+$. Suppose that ε represents a non-trivial element in $(\mathfrak{E}_+/\mathfrak{E}_-^p)$. Consider a Kummer extension $F(\varphi^-)(\mu_p)[\sqrt[p]{\varepsilon}]/F(\varphi^-)(\mu_p)$. We let the Galois group acts on field elements from the left (to have left Galois modules which is more common than right modules). Pick a p-th root $\epsilon := \sqrt[p]{\varepsilon}$. Since $({}^\sigma\epsilon)^p = {}^\sigma\varepsilon = \varepsilon$, we have ${}^{\sigma-1}\epsilon \in \mu_p$. For $\sigma, \tau \in \mathrm{Gal}(F(\varphi^-)(\mu_p)[\sqrt[p]{\varepsilon}]/F(\varphi^-))$, we have $u(\sigma\tau) = {}^{\sigma\tau-1}\epsilon = {}^{\sigma\tau-\sigma+\sigma-1}\epsilon = {}^\sigma u(\tau)u(\sigma)$. Then $u = u_\epsilon : \sigma \mapsto {}^{\sigma-1}\epsilon = {}^\sigma\epsilon/\epsilon \in \mu_p$ is a cocycle with values in $\mu_p(\overline{\mathbb{Q}})$ of $\mathrm{Gal}(F(\varphi^-)(\mu_p)[\sqrt[p]{\varepsilon}]/F(\varphi^-))$ representing the cohomology class of $\varepsilon \in F(\varphi^-)^\times/(F(\varphi^-)^\times)^p \cong H^1(F(\varphi^-), \mu_p)$.

Fix a p-th primitive root ζ_p of unity, and identify μ_p with $\mathbb{F}_p$ by $\zeta_p^m \mapsto m \in \mathbb{F}_p$. In this way, we regard u_ϵ as a cocycle $U = U_\epsilon$ with values in $\mathbb{F}_p(1)$ so that $u_\epsilon(\sigma) = \zeta_p^{U_\epsilon(\sigma)}$. Then U_ϵ satisfies $U(\sigma\tau) = \omega(\sigma)U(\tau) + U(\sigma)$. Thus the Galois action on the subgroup $V \cong \mathbb{F}_p^2$ generated by ϵ and ζ_p inside $F(\varphi^-)(\mu_p)[\sqrt[p]{\varepsilon}]^\times/(F(\varphi^-)(\mu_p)[\sqrt[p]{\varepsilon}]^\times)^p$ is given by $\eta = \eta_\epsilon : \sigma \mapsto \left(\begin{smallmatrix} \omega & U_\epsilon \\ 0 & 1 \end{smallmatrix}\right)$, which is a Galois representation $\mathrm{Gal}(F(\varphi^-)(\mu_p)[\sqrt[p]{\varepsilon}]/F(\varphi^-)) \to \mathrm{GL}_2(\mathbb{F}_p)$. Note that $u_{\epsilon^{-1}}(\sigma) = {}^{1-\sigma}\epsilon = u_\epsilon(\sigma)^{-1}$ and that for any p-th root ζ of unity, $u_{\zeta\epsilon} = {}^{\sigma-1}(\zeta\epsilon) = {}^{\sigma-1}\zeta^{\sigma-1}\epsilon = {}^{\sigma-1}\zeta u_\epsilon(\sigma)$; so, $U_{\zeta\epsilon}(\sigma) = (1-\omega(\sigma))b + U_\epsilon(\sigma)$ with $\zeta = \zeta_p^{-b}$. Thus we conclude

$$\eta_{\zeta\epsilon} = \alpha(b)\eta_\epsilon\alpha(b)^{-1}$$

for $\alpha(b) = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$. Since $u_{\epsilon^a} = u_\epsilon^a$, we have $U_{\epsilon^a} = aU_\epsilon$ for $a \in \mathbb{Z}$ prime to p. Since U_{ϵ^a} only depends on $a \mod p$, we write $U_{\epsilon^a} := aU_\epsilon$ for $a \in \mathbb{F}$

The set of conjugates of ϵ over F is given by $\{\zeta\epsilon^\tau\}_{\tau \in \mathrm{Gal}(F(\varphi^-)/F), \zeta \in \mu_p(\overline{\mathbb{Q}})}$. If $\tau(\varepsilon) \equiv \varepsilon^{\varphi^-(\tau)^{-1}} \mod \mathfrak{E}^p$ (i.e., $\varepsilon \in \mathfrak{E}/\mathfrak{E}^p[(\overline{\varphi}^-)^{-1}]$), $L := F(\varphi^-)(\mu_p)[\epsilon]$ is a Galois extension over $\mathbb{Q}$ and $\mathrm{Gal}(L/F(\varphi^-)) \triangleleft \mathrm{Gal}(L/F)$. Suppose $\varepsilon \in \mathfrak{E}/\mathfrak{E}^p[(\overline{\varphi}^-)^{-1}]$. Then for any lift $\gamma \in \mathrm{Gal}(L/F)$ of the generator γ_0 of $\mathrm{Gal}(F(\varphi^-)/F)$, we can think of $\eta'(\sigma) := \eta(\gamma\sigma\gamma^{-1})$ which is a representation of $\mathrm{Gal}(L/F)$ into $\mathrm{GL}_2(\mathbb{F}_p)$ with values in the mirabolic subgroup

$$P := \left\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_p) | a, b \in \mathbb{F}_p\right\}.$$

Indeed, η induces an isomorphism $\mathrm{Gal}(L/F(\varphi^-)) \cong P$. Therefore the composite of the following isomorphisms

$$P \xrightarrow[\sim]{\eta^{-1}} \mathrm{Gal}(L/F(\varphi^-)) \xrightarrow[\sim]{\eta'} P$$

induces an automorphism in $\mathrm{Aut}_{\mathrm{gp}}(P)$. Since any automorphism of P inducing the identity modulo unipotent matrices is inner, we have $\eta' \circ \eta^{-1}(x) = gxg^{-1}$ for $g \in P$. Taking x to be $\eta(\sigma)$, we find $\eta'(\sigma) = g\eta(\sigma)g^{-1}$; so, η' and η is equivalent as representations. Write $g := \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$, we find $\eta' = \left(\begin{smallmatrix} \omega & aU+b(1-\omega) \\ 0 & 1 \end{smallmatrix}\right)$. Replace ϵ by $\zeta_p^{-b}\epsilon^a$ (this modification does not change L). Then we may assume that $\eta' = \eta$, and under this choice of ϵ, we find that γ commutes with the elements in $\mathrm{Gal}(L/F(\varphi^-)) \subset \mathrm{Gal}(L/F)$. Since $\mathrm{Gal}(L/F) = \bigsqcup_{j=1}^a \mathrm{Gal}(L/F(\varphi^-))\gamma^j$, γ must be in the center Z of $\mathrm{Gal}(L/F)$. Since $P \cong \mathrm{Gal}(L/F(\varphi^-))$ has trivial center, the intersection $Z \cap \mathrm{Gal}(L/F(\varphi^-)) = \{1\}$ is trivial. Thus $Z \cong \mathrm{Gal}(F(\varphi^-)/F)$ and $\mathrm{Gal}(L/F) = \mathrm{Gal}(L/F(\varphi^-)) \times Z$.

Thus we may lift the generator γ_0 of $\mathrm{Gal}(F(\varphi^-)/F)$ uniquely to a central element $\gamma \in \mathrm{Gal}(L/F)$. Write $[\varphi^-(\tau)] \in \mathbb{Z}$ representing the mod p class of $\overline{\varphi}^-(\tau) \in (\mathbb{Z}/p\mathbb{Z})^\times$; so, $[\varphi^-(\tau)]^{-1}$ is the inverse of the mod p class $[\varphi^-(\tau)]$ in $\mathbb{Z}/p\mathbb{Z}$. Then we define, for $x \in L^\times$, $x^{\varphi^-(\tau)} := x^{[\varphi^-(\tau)]} \mod x^{p\mathbb{Z}}$ and $x^{\varphi^-(\tau)^{-1}} := x^{[\varphi^-(\tau)]^{-1}} \mod x^{p\mathbb{Z}}$. This makes sense only modulo p-power of x. Then we have

$${}^\gamma\epsilon \equiv \zeta\epsilon^{\varphi^-(\gamma_0)^{-1}} \mod \varepsilon^{\mathbb{Z}}$$

(as $\epsilon^{p\mathbb{Z}} = \varepsilon^{\mathbb{Z}}$) for some $\zeta \in \mu_p(L)$ since ${}^{\gamma_0}\varepsilon \equiv \varepsilon^{\varphi^-(\gamma_0)^{-1}} \mod \mathfrak{E}^p$. So we conclude ${}^{\gamma-\varphi^-(\gamma_0)^{-1}}\epsilon \equiv \zeta \mod \varepsilon^{\mathbb{Z}}$. The element $\gamma - \varphi^-(\gamma_0)^{-1}$ is in the center of the group algebra $\mathbb{Z}_p[\mathrm{Gal}(L/F)]$, we have

$$\zeta^{\sigma-1} \equiv {}^{(\sigma-1)(\gamma-\varphi^-(\gamma_0)^{-1})}\epsilon \equiv {}^{(\gamma-\varphi^-(\gamma_0)^{-1})(\sigma-1)}\epsilon \equiv {}^{(\gamma-\varphi^-(\gamma_0)^{-1})}u_\epsilon(\sigma) \mod \varepsilon^{\mathbb{Z}}.$$

Taking σ such that $u_\epsilon(\sigma) = \zeta_p$ and $\omega(\sigma) = 1$ (i.e., $\eta(\sigma) = \alpha(1)$), we have

$${}^\gamma\zeta_p = \zeta_p^{\varphi^-(\gamma_0)^{-1}}.$$

Thus $\omega(\gamma) \equiv \varphi^-(\gamma_0)^{-1} \mod p\mathbb{Z}_p$. Therefore

$$F(\varphi^-)(\mu_p)^Z := H^0(Z, F(\varphi^-)(\mu_p)) = F(\varphi^-\omega). \tag{6.4}$$

Hence we have a cyclic p-extension $F_\varepsilon/F(\varphi^-\omega)$ which is the fixed subfield of L by γ. Since ε is a unit, only possible ramification of L over $F(\varphi^-)(\mu_p)$ at finite places is at a prime over p. The extension $L/F(\varphi^-\omega)$ is unramified outside $\mathfrak{p}$ and totally split at $\mathfrak{p}^c$ if and only if ε is locally a p-power at all place $\mathfrak{P}|\mathfrak{p}^c$ of $F(\varphi^-)$ ($\Leftrightarrow \varepsilon \in \mathfrak{E}_-$). Since p is prime to $|Z| = [F(\varphi^-) : F]$ and only p ramifies in $F(\varphi^-)[\mu_p]/F(\varphi^-)$, $F_\varepsilon/F(\varphi^-\omega)$ is a p-cyclic extension unramified outside $\mathfrak{p}$ in which $\mathfrak{p}^c$ splits totally. Since units in $\mathfrak{E}_+$ are p-power locally at $\mathfrak{p}^c$, we get injective homomorphism

$$(\mathfrak{E}_+/\mathfrak{E}_-^p)[(\overline{\varphi}^-)^{-1}] \hookrightarrow \mathrm{Hom}(Cl_{F(\varphi^-\omega)}(p^\infty), \mathbb{F}_p)[\overline{\varphi}^-\overline{\omega}] \tag{6.5}$$

sending ε to $U_\epsilon|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F(\varphi^-\omega))} : Cl_{F(\varphi^-)[\mu_p]}(p^\infty) \to \mathbb{F}_p$ which factors through $Cl_{F(\varphi^-\omega)}(p^\infty)$. Here note that $C(\varphi^-\omega)(p^\infty)$ is the Galois group of the maximal abelian extension of $F(\varphi^-\omega)$ unramified outside p. Since units in $\mathfrak{E}_+$ are locally p-power at $\mathfrak{p}^c$, U_ϵ is trivial at each places over $\mathfrak{p}^c$. Then by (3.4), the image of $(\mathfrak{E}/\mathfrak{E}^p)[(\overline{\varphi}^-)^{-1}]$ lands in the image of $\mathrm{Sel}_\emptyset^\perp(\overline{\varphi}^-\overline{\omega})$ in $\mathrm{Hom}(Cl_{F(\varphi^-\omega)}(p^\infty), \mathbb{F}_p)[\overline{\varphi}^-\overline{\omega}]$.

We now prove the equality: $(\mathfrak{E}/\mathfrak{E}^p)[(\overline{\varphi}^-)^{-1}] \cong \mathrm{Sel}_\emptyset^\perp(\overline{\varphi}^-\overline{\omega})$. Let $L/F(\varphi^-)(\mu_p)$ be a p-abelian extension unramified outside p. Then we can choose $\xi \in F(\varphi^-)(\mu_p)^\times$ so that $L = F(\varphi^-)(\mu_p)[\sqrt[p]{\xi}]$ by Kummer's theory; i.e.,

$$F(\varphi^-)[\mu_p]^\times/(F(\varphi^-)[\mu_p]^\times)^p \cong H^1(F(\varphi^-)[\mu_p], \mu_p).$$

Suppose that L/F is a Galois extension such that the conjugation action of $\mathrm{Gal}(F(\varphi^-)[\mu_p]/\mathbb{Q})$ on $\mathrm{Gal}(L/F(\varphi^-)[\mu_p]) \cong \mathbb{F}_p$ is given by $\overline{\varphi}^-\overline{\omega}$. By Kummer's theory, we have

$$F(\varphi^-)[\mu_p]^\times/(F(\varphi^-)[\mu_p]^\times)^p[\overline{\omega}] \cong H^1(F(\varphi^-)[\mu_p], \mu_p)[\overline{\omega}].$$

The action of $\tau \in \mathrm{Gal}(F(\varphi^-)[\mu_p]/F(\varphi^-))$ on a cocycle $u : \mathrm{Gal}(\overline{\mathbb{Q}}/F(\varphi^-)) \to \mu_p$ is ${}^\tau u : \sigma \mapsto \tau(u(\widetilde{\tau}^{-1}\sigma\widetilde{\tau}))$ for a lift $\widetilde{\tau} \in \mathrm{Gal}(L/F(\varphi^-))$ of $\tau \in \mathrm{Gal}(F(\varphi^-)[\mu_p]/F(\varphi^-))$. For the Kummer cocycle $u_\xi(\tau) = {}^{\tau-1}\sqrt[p]{\xi}$ giving rise to an $\overline{\omega}$-eigen class in $H^1(F(\varphi^-)[\mu_p], \mu_p)[\overline{\omega}]$, we have

$$\tau({}^{\widetilde{\tau}^{-1}\sigma\widetilde{\tau}-1}(\sqrt[p]{\xi})) \equiv \tau u_\xi(\widetilde{\tau}^{-1}\sigma\widetilde{\tau}) \equiv \overline{\omega}(\tau)u_\xi(\sigma) \equiv {}^{\overline{\omega}(\tau)(\sigma-1)}(\sqrt[p]{\xi}) \mod (F(\varphi^-)[\mu_p]^\times)^p.$$

On the other hand, we may choose $\widetilde{\tau}$ so that ${}^{\widetilde{\tau}}(\sqrt[p]{\xi}) = \sqrt[p]{{}^\tau\xi}$. Under this choice, we have

$$\tau({}^{\widetilde{\tau}^{-1}\sigma\widetilde{\tau}}(\sqrt[p]{\xi})) = {}^\sigma(\sqrt[p]{{}^\tau\xi}).$$

Thus we get $\tau({}^{(\sigma-1)}(\sqrt[p]{{}^\tau\xi})) = {}^{\overline{\omega}(\tau)(\sigma-1)}(\sqrt[p]{{}^\tau\xi})$. This shows $\xi^\tau \equiv \xi \mod (F(\varphi^-)[\mu_p]^\times)^p$, and $\tau \mapsto {}^{\tau-1}\xi$ is a cocycle with values in $(F(\varphi^-)[\mu_p]^\times)^p$. The exact sequence

$$\begin{aligned}1 \to H^0(F(\varphi^-)[\mu_p]/F(\varphi^-), F(\varphi^-)[\mu_p]^\times/\mu_p) &\xrightarrow{x\mapsto x^p} H^0(F(\varphi^-)[\mu_p]/F(\varphi^-), F(\varphi^-)[\mu_p]^\times) \\ \to H^0(F(\varphi^-)[\mu_p]/F(\varphi^-), &\frac{F(\varphi^-)[\mu_p]^\times}{(F(\varphi^-)[\mu_p]^\times)^p}) \to H^1(F(\varphi^-)[\mu_p]/F(\varphi^-), F(\varphi^-)[\mu_p]^\times/\mu_p)\end{aligned}$$

combined with the fact that $H^1(F(\varphi^-)[\mu_p]/F(\varphi^-), F(\varphi^-)[\mu_p]^\times/\mu_p)$ is killed by $[F(\varphi^-)[\mu_p] : F(\varphi^-)]$ prime to p, we find that

$$H^0(F(\varphi^-)[\mu_p]/F(\varphi^-), F(\varphi^-)[\mu_p]^\times/(F(\varphi^-)[\mu_p]^\times)^p) \cong F(\varphi^-)^\times/(F(\varphi^-)^\times)^p.$$

Thus we can choose $\xi \in F(\varphi^-)^\times$.

By the inflation-restriction sequence combined with Kummer's theory produces an isomorphism

$$\begin{aligned}H^1(F, \overline{\varphi}^-\overline{\omega}) &\cong H^0(F(\varphi^-)/F, H^1(F(\varphi^-), \overline{\omega})) \\ &\cong H^0(F(\varphi^-)/F, F(\varphi^-)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p) \cong (F(\varphi^-)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)[(\overline{\varphi}^-)^{-1}],\end{aligned} \tag{6.6}$$

as $H^j(F(\varphi^-)/F, H^0(F(\varphi^-), M)) = 0$ with $j > 0$ for any $\mathbb{F}[\mathrm{Gal}(\overline{\mathbb{Q}}/F(\varphi^-))]$-module M because of $p \nmid [F(\varphi^-) : F]$. Thus we may assume that the class $[\xi]$ of ξ is in the $(\overline{\varphi}^-)^{-1}$-eigenspace $(F(\varphi^-)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)[(\overline{\varphi}^-)^{-1}]$. Here the action of $\mathrm{Gal}(F(\varphi^-)/F)$ on cohomology is the contravariant action; so, we get $(\overline{\varphi}^-)^{-1}$-eigen vector.

Since $L/F(\varphi^-)[\mu_p]$ is unramified outside p, $(\xi) := \xi\mathfrak{R}[\frac{1}{p}]$ is a p-power as a fractional $\mathfrak{R}[\frac{1}{p}]$-ideal in $F(\varphi^-)[\mu_p]$. Since $F(\varphi^-)[\mu_p]$ only ramifies at p with ramification index prime to p, (ξ) is a p-power as a fractional $\mathfrak{R}[\frac{1}{p}]$-ideal of $F(\varphi^-)$. Write $(\xi) = \prod_{\mathfrak{l}} \mathfrak{l}^{pe(\mathfrak{l})}$ for prime ideals $\mathfrak{l}$ of $\mathfrak{R}[\frac{1}{p}]$. If $h = h_{F(\varphi^-)}$ is prime to p, we may replace ξ by ξ^h without changing $F(\varphi^-)[\mu_p][\sqrt[p]{\xi}]$, and then the hth power of

$\prod_{\mathfrak{l}} \mathfrak{l}^{pe(\mathfrak{l})}$ becomes a p-power of a principal ideal (ξ'); i.e., $\xi^h = \varepsilon\xi'^p$ for $\varepsilon \in \mathfrak{R}[\frac{1}{p}]^\times$. Thus we may replace ξ by ξ^h and then by $\varepsilon \in \mathfrak{R}[\frac{1}{p}]^\times$.

We now show that we can replace ξ by $\varepsilon \in \mathfrak{R}[\frac{1}{p}]^\times$ under the assumption: $(Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F}_p)[\overline{\varphi}^-] = 0$ milder than $p \nmid h_{F(\varphi^-)}$. Since $\mathrm{Gal}(F(\varphi^-)[\mu_p]/F)$ acts on $\mathrm{Gal}(L/F(\varphi^-)[\mu_p])$ by $\overline{\varphi}^-\overline{\omega}$, we have $\prod_{\mathfrak{l}} \mathfrak{l}^{\tau e(\mathfrak{l})} \equiv (\sqrt[p]{\tau\xi}) \equiv (\sqrt[p]{\xi})^{[\varphi^-(\tau)^{-1}]} \equiv \prod_{\mathfrak{l}} \mathfrak{l}^{[\varphi^-(\tau)^{-1}]e(\mathfrak{l})}$ modulo p-power of fractional $\mathfrak{R}[\frac{1}{p}]$-ideals. Thus we conclude $e(\mathfrak{l}) \equiv [\varphi^-(\gamma)^{-1}]e(\mathfrak{l}^\gamma) \mod p$ for the generator $\gamma \neq 1$ of $\mathrm{Gal}(F(\varphi^-)/F)$. In particular, $\mathfrak{l}$ is completely split in $F(\varphi^-)/F$ if $e(\mathfrak{l}) \neq 0$, since $\overline{\varphi}^-(\gamma) \neq 1$. Write Cl'_X for the ideal class group of $O_X[\frac{1}{p}]$ for a number field X with integer ring O_X. Note that $Cl'_{F(\varphi^-)}$ is the surjective image of $Cl_{F(\varphi^-)}$. If the class group

$$Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F}_p[\overline{\varphi}^-] = 0 \; (\Rightarrow Cl'_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F}_p[\overline{\varphi}^-] = Cl'_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F}_p[(\overline{\varphi}^-)^{-1}] = 0),$$

for $\mathfrak{a} = \prod_{\mathfrak{l}} \mathfrak{l}^{e(\mathfrak{l})}$, we get $(Cl'_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{Z}_p)[\overline{\varphi}^-]) = 0$ by Nakayama's lemma, and $\prod_{j=1}^a {}^{\gamma^j}\mathfrak{a}^{[\varphi^-(\gamma^j)]}$ is principal generated by ξ'. Replacing ξ by the $(\varphi^-)^{-1}$-projection $\prod_{j=1}^a {}^{\gamma^j}\xi^{[\varphi^-(\gamma^j)]}$ which does not affect the corresponding Kummer extension, we may assume that $\xi = \varepsilon\xi'^p$. Then $\varepsilon \in \mathfrak{R}[\frac{1}{p}]^\times$.

By construction, $\sqrt[p]{\varepsilon}$ generates L over $F(\varphi^-)[\mu_p]$. In $F(\varphi^-)^\times/(F(\varphi^-)^\times)^p$, $\varepsilon^\tau = \varepsilon^{\varphi^-(\tau)}$. Regard ε as an element in $\mathfrak{R}[\frac{1}{p}]^\times/(\mathfrak{R}[\frac{1}{p}]^\times)^p$. For a $\mathbb{Z}[\mathrm{Gal}(F(\varphi^-)/F)]$-module M, we write $M \otimes \varphi^-$ a new twisted module with underlying $\mathbb{Z}_p[\varphi^-]$-module $M \otimes_{\mathbb{Z}} \mathbb{Z}_p$ having Galois action given by $M \otimes \varphi^- \ni x \mapsto \varphi^-(\tau)\tau(x) \in M \otimes \varphi^-$ for the original action $x \mapsto \tau(x)$ for $x \in M \otimes_{\mathbb{Z}} \mathbb{Z}_p$. The exact sequence

$$\begin{aligned} 1 \to H^0(F(\varphi^-)/F, \mathfrak{R}[\frac{1}{p}]^\times \otimes \varphi^-) &\xrightarrow{x \mapsto x^p} H^0(F(\varphi^-)/F, \mathfrak{R}[\frac{1}{p}]^\times \otimes \varphi^-) \\ &\to H^0(F(\varphi^-)/F, (\mathfrak{R}[\frac{1}{p}]^\times/(\mathfrak{R}[\frac{1}{p}]^\times)^p) \otimes \varphi^-) \to H^1(F(\varphi^-)/F, \mathfrak{R}[\frac{1}{p}]^\times \otimes \varphi^-), \end{aligned}$$

combined with the fact that $H^1(F(\varphi^-)/F, \mathfrak{R}[\frac{1}{p}]^\times \otimes \varphi^-)$ is killed by $[F(\varphi^-) : F]$ prime to p, we find that $H^0(F(\varphi^-)/F, (\mathfrak{R}[\frac{1}{p}]^\times/(\mathfrak{R}[\frac{1}{p}]^\times)^p) \otimes \varphi^-) = (\mathfrak{R}[\frac{1}{p}]^\times/(\mathfrak{R}[\frac{1}{p}]^\times)^p)[(\overline{\varphi}^-)^{-1}]$. Therefore the class of ε in $\mathfrak{R}[\frac{1}{p}]^\times \otimes_{\mathbb{Z}} \mathbb{F}$ is in the $(\overline{\varphi}^-)^{-1}$-eigenspace.

Since p splits in $F/\mathbb{Q}$, the divisor group of $\mathrm{Spec}(\mathfrak{R})$ generated by primes over p is isomorphic to $\mathrm{Ind}_F^{\mathbb{Q}} \mathbb{Z}[\mathrm{Gal}(F(\varphi^-)/F)/D]$ for the decomposition group D of a prime $\mathfrak{P}|\mathfrak{p}$ in $F(\varphi^-)$. We have an exact sequence of $\mathrm{Gal}(F(\varphi^-)/F)$-modules:

$$1 \to \mathfrak{R}^\times \to \mathfrak{R}[\frac{1}{p}]^\times \xrightarrow{\pi} \mathrm{Ind}_F^{\mathbb{Q}} \mathbb{Z}[\mathrm{Gal}(F(\varphi^-)/F)/D] \to C \to 0$$

with finite C. Since $\mathrm{Im}(\pi) \subset \mathrm{Ind}_F^{\mathbb{Q}} \mathbb{Z}[\mathrm{Gal}(F(\varphi^-)/F)/D]$ is $\mathbb{Z}$-free, after tensoring with $\mathbb{F}$, we still have an exact sequence:

$$0 \to \mathfrak{R}^\times \otimes_{\mathbb{Z}} \mathbb{F} \to \mathfrak{R}[\frac{1}{p}]^\times \otimes_{\mathbb{Z}} \mathbb{F} \to \mathrm{Im}(\pi) \otimes_{\mathbb{Z}} \mathbb{F} \to 0.$$

Taking $(\overline{\varphi}^-)^{-1}$-eigenspace, we have one more exact sequence

$$0 \to (\mathfrak{R}^\times \otimes_{\mathbb{Z}} \mathbb{F})[(\overline{\varphi}^-)^{-1}] \to (\mathfrak{R}[\frac{1}{p}]^\times \otimes_{\mathbb{Z}} \mathbb{F})[(\overline{\varphi}^-)^{-1}] \to (\mathrm{Im}(\pi) \otimes_{\mathbb{Z}} \mathbb{F})[(\overline{\varphi}^-)^{-1}].$$

Note that $\overline{\mathbb{Q}}[\mathrm{Gal}(F(\varphi^-)/F)/D] = \mathrm{Im}(\pi) \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}$ contain only characters trivial over D as a subquotient. Since $D \cong \varphi^-(\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p))$ is non-trivial by (h4), $(\mathrm{Im}(\pi) \otimes_{\mathbb{Z}} \mathbb{F})[(\overline{\varphi}^-)^{-1}] = 0$ as φ^- induces an isomorphism of $\mathrm{Gal}(F(\varphi^-)/F) \cong \mathrm{Im}(\varphi^-)$. Thus we may assume that $\varepsilon \in \mathfrak{R}^\times$. By the local triviality of the Kummer cocycle at $\mathfrak{p}^c$ (i.e., (3.4)), we have $\varepsilon \in \mathfrak{E}_+$. Thus $\mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-\overline{\omega}) \cong \mathfrak{E}_+/\mathfrak{E}_-^p[(\overline{\varphi}^-)^{-1}]$. By Proposition 6.1 (1), we have $\dim_{\mathbb{F}} \mathfrak{R}^\times \otimes_{\mathbb{Z}} \mathbb{F}[(\overline{\varphi}^-)^{-1}] = \dim_{\overline{\mathbb{Q}}} \mathfrak{R}^\times \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}[(\varphi^-)^{-1}] = 1$, and hence $\dim_{\mathbb{F}} \mathfrak{E}_+/\mathfrak{E}_-^p[(\overline{\varphi}^-)^{-1}] \leq \dim_{\mathbb{F}} \mathfrak{R}^\times \otimes_{\mathbb{Z}} \mathbb{F}[(\overline{\varphi}^-)^{-1}] = 1$, which conclude the proof when $\mathbb{F} = \mathbb{F}_p$.

Now we deal with the general case cohomologically. We may assume that $\mathbb{F}$ is generated by the values of φ^- over $\mathbb{F}_p$. By the inflation-restriction sequence combined with Kummer's theory produces an isomorphism

$$\begin{aligned}(6.7)\quad H^1(F,\overline{\varphi}^-\overline{\omega}) &\cong H^0(F(\varphi^-)/F, H^1(F(\varphi^-),\overline{\omega}\otimes_{\mathbb{F}_p}\mathbb{F}))\\ &\cong H^0(F(\varphi^-)/F, F(\varphi^-)^\times\otimes_{\mathbb{Z}}\mathbb{F}) \cong (F(\varphi^-)^\times\otimes_{\mathbb{Z}}\mathbb{F})[(\overline{\varphi}^-)^{-1}],\end{aligned}$$

as $H^j(F(\varphi^-)/F, H^0(F(\varphi^-),M)) = 0$ with $j > 0$ for any $\mathbb{F}[\mathrm{Gal}(\overline{\mathbb{Q}}/F(\varphi^-))]$-module M because of $p \nmid [F(\varphi^-):F]$. The last identity follows from the fact that ${}^\tau u(g) = \tau u(\tau^{-1}g\tau) = \overline{\varphi}^-(\tau)u(\tau^{-1}g\tau)$ for cocycle u giving rise to a class $H^1(F,\overline{\varphi}^-\overline{\omega})$ for $\tau \in \mathrm{Gal}(F(\varphi^-)/F)$. By Kummer's theory, non-zero elements in the right-hand-side of (6.7) correspond, up to scalar multiples, bijectively to p-abelian extensions L' of $F(\varphi^-\omega)[\mu_p]$ with $\mathrm{Gal}(L'/F(\varphi^-)[\mu_p]) \cong \mathbb{F}$ such that $\mathrm{Gal}(F(\varphi^-\omega)[\mu_p]/F)$ acts on $\mathrm{Gal}(L'/F(\varphi^-\omega)[\mu_p])$ by $\overline{\varphi}^-\overline{\omega}$ by conjugation.

Let $EXT_{/F(\varphi^-\omega)}$ (resp. $EXT_{/F(\varphi^-)[\mu_p]}$) be the set of p-abelian extensions L (inside $\overline{\mathbb{Q}}$) of $F(\varphi^-\omega)$ (resp. $F(\varphi^-)[\mu_p]$) with $\mathrm{Gal}(L/F(\varphi^-\omega)) \cong \mathbb{F}$ (resp. $\mathrm{Gal}(L'/F(\varphi^-)[\mu_p]) \cong \mathbb{F}$) such that $\mathrm{Gal}(F(\varphi^-\omega)/F)$ (resp. $\mathrm{Gal}(F(\varphi^-)[\mu_p]/F)$) acts on the normal subgroup $\mathrm{Gal}(L/F(\varphi^-\omega))$ by $\overline{\varphi}^-\overline{\omega}$ via conjugation. Non-zero elements in the extension group $H^1(F,\overline{\varphi}^-\overline{\omega}) \cong \mathrm{Ext}_{\mathbb{F}_p[\mathrm{Gal}(\overline{\mathbb{Q}}/F)]}(\mathbb{F},\overline{\varphi}^-\overline{\omega})$ correspond, up to scalar multiples, bijectively to extensions $\overline{\varphi}^-\overline{\omega} \hookrightarrow X \twoheadrightarrow \mathbb{F}$. As an $\mathbb{F}$-vector space, X is two dimensional, and choosing a basis x_1, x_2 of X over $\mathbb{F}$ so that on $\mathbb{F}x_1$, $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ acts by $\overline{\varphi}^-\overline{\omega}$. For $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/F)$, $(\tau(x_1),\tau(x_2)) = (x_1,x_2)\rho(\tau)$ with $\rho = \left(\begin{smallmatrix}\overline{\varphi}^-\overline{\omega} & u\\ 0 & 1\end{smallmatrix}\right)$ for a 1-cocycle u representing X. Since X is a non-trivial extension, the class $[u]$ of u is non-trivial in $H^1(F,\overline{\varphi}^-\overline{\omega})$. Then the splitting field L of X gives rise to an element in $EXT_{/F(\varphi^-\omega)}$. Since cohomologous relation on cocycles u corresponds equivalence relations on ρ by conjugation of unipotent elements inside the mirabolic subgroup P, we again conclude that non-zero elements in the left-hand-side of (6.7) correspond, up to scalar multiples, one to one onto to elements in $EXT_{/F(\varphi^-\omega)}$. Therefore $EXT_{/F(\varphi^-\omega)} \ni L \mapsto L[\mu_p] \in EXT_{/F(\varphi^-\omega)[\mu_p]}$ is a bijection.

Since $F(\varphi^-)[\mu_p]/F(\varphi^-)$ only ramifies at p, $L \in EXT_{/F(\varphi^-)}$ is unramified outside p if and only if $L[\mu_p]/F(\varphi^-)[\mu_p]$ is unramified outside p. If every prime factor of $\mathfrak{p}^c$ in $F(\varphi^-)[\mu_p]$ totally splits in $L[\mu_p]/F(\varphi^-)[\mu_p]$, it has to totally split in $L/F(\varphi^-\omega)$, since in $F(\varphi^-)[\mu_p]/F(\varphi^-\omega)$, there is no residual extension possible for prime factors in p.

Thus writing $EXT^{\mathfrak{p}^c\text{-sp}}_{/F(\varphi^-)}$ for the subset of $EXT_{/F(\varphi^-)}$ made up of extensions unramified outside $\mathfrak{p}$ in which every prime factors of $\mathfrak{p}^c$ splits totally, we need to show that $EXT^{\mathfrak{p}^c\text{-sp}}_{/F(\varphi^-)}$ corresponds to bijectively non-zero elements of $(\mathfrak{E}_+/\mathfrak{E}_-^p\otimes_{\mathbb{F}_p}\mathbb{F})[\overline{\varphi}^-]$ up to scalar multiples. By definition, $EXT^{\mathfrak{p}^c\text{-sp}}_{/F(\varphi^-)}$ embeds (up to scalars) into the subgroup of $H^1(F(\varphi^-),\overline{\omega}\otimes_{\mathbb{F}_p}\mathbb{F})$ spanned over $\mathbb{F}$ by the class of Kummer cocycles unramified outside p. Consider the sum of Galois conjugates $\Phi = \bigoplus_{\tau\in\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)}(\overline{\varphi}^-)^{-\tau}$. Then Φ is defined over $\mathbb{F}_p$ and is an $\mathbb{F}_p$-irreducible representation. Since $\mathfrak{E}_+/\mathfrak{E}_-^p$ is an $\mathbb{F}_p$ vector space on which $\mathrm{Gal}(F(\varphi^-)/F)$ acts, we can consider Φ-isotypical subspace $(\mathfrak{E}_+/\mathfrak{E}_-^p)[\Phi]$ which is isomorphic to $(\mathfrak{E}_+/\mathfrak{E}_-^p\otimes_{\mathbb{F}_p}\mathbb{F})[(\overline{\varphi}^-)^{-1}]$ as $\mathbb{F}_p$-vector spaces by projecting down to $(\overline{\varphi}^-)^{-1}$-eigenspace in $(\mathfrak{E}_+/\mathfrak{E}_-^p)[\Phi]\otimes_{\mathbb{F}_p}\mathbb{F}$ as

$$(\mathfrak{E}_+/\mathfrak{E}_-^p)[\Phi]\otimes_{\mathbb{F}_p}\mathbb{F} \cong \bigoplus_\tau (\mathfrak{E}_+/\mathfrak{E}_-^p\otimes_{\mathbb{F}_p}\mathbb{F})[(\overline{\varphi}^-)^{-\tau}].$$

Similarly, for $X = F(\varphi^-)^\times/(F(\varphi^-)^\times)^p = F(\varphi^-)^\times\otimes_{\mathbb{Z}}\mathbb{F}_p$, $Cl_{F(\varphi^-)}\otimes_{\mathbb{Z}}\mathbb{F}_p$ and $Cl'_{F(\varphi^-)}\otimes_{\mathbb{Z}}\mathbb{F}_p$, we have

$$X[\Phi] \cong (X\otimes_{\mathbb{F}_p}\mathbb{F})[(\overline{\varphi}^-)^{-1}].$$

A Kummer cocycle $[\xi] = \xi\otimes 1 \in F(\varphi^-)^\times\otimes_{\mathbb{Z}}\mathbb{F}_p$ with $\xi \in F(\varphi^-)^\times$ is unramified outside p if its image in $F(\varphi^-)_v^\times\otimes_{\mathbb{Z}}\mathbb{F}_p$ vanishes at all finite places $v \nmid p$ of $F(\varphi^-)$. Thus the principal ideal $\xi\mathfrak{R}[\frac{1}{p}]$ is a p-power $\mathfrak{a}^p$. Suppose that $[\xi] \in (F(\varphi^-)^\times\otimes_{\mathbb{Z}}\mathbb{F}_p)[\Phi]$. Since $(Cl'_{F(\varphi^-)}\otimes_{\mathbb{Z}}\mathbb{Z}_p)[\Phi] = 0$ by our assumption $(Cl_{F(\varphi^-)}\otimes_{\mathbb{Z}}\mathbb{F})[\overline{\varphi}^-] = 0$, the projected image $[\mathfrak{a}]_\Phi$ in $(Cl'_{F(\varphi^-)}\otimes_{\mathbb{Z}}\mathbb{Z}_p)[\Phi] = 0$ of the class $[\mathfrak{a}] \in Cl'_{F(\varphi^-)}$ is trivial. Thus replacing $\mathfrak{a}$ and ξ by its Φ-projection (in the fractional ideal group of $\mathfrak{R}[\frac{1}{p}]$) which is principal, we find that $\xi = \varepsilon\xi'^p$ for $\varepsilon \in \mathfrak{R}[\frac{1}{p}]^\times$. Then repeating the same argument in the case of $\mathbb{F} = \mathbb{F}_p$, we conclude $\varepsilon \in \mathfrak{E}_-$ and $\mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}^-) \cong (\mathfrak{E}_+/\mathfrak{E}_-^p)[\Phi]$ as $\mathbb{F}_p$-vector space. Then we have $\mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}^-) \cong (\mathfrak{E}_+/\mathfrak{E}_-^p\otimes_{\mathbb{F}_p}\mathbb{F})[(\overline{\varphi}^-)^{-1}]$, and thus $\dim_{\mathbb{F}}\mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}^-) \le 1$ as before. □

Proof of Theorem A: We want to prove the following slightly stronger version of Theorem A allowing the case when $p|h_F$:

Theorem 6.3. *Suppose* (h0–4) *and* $(Cl_{F(\varphi^-)}\otimes_{\mathbb{Z}}\mathbb{F})[\overline{\varphi^-}]=0$. *Then* $\mathcal{Y}^-(\varphi^-)$ *and* $\mathcal{Y}^-(\varphi^-\omega)$ *are cyclic over* $W[[H]]$.

Proof. By Proposition 6.2, we have

$$\dim_{\mathbb{F}}\mathrm{Hom}_{W[[H]]}(\mathcal{Y}^-(\varphi^-\omega),\mathbb{F})\cong\mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_F^{\mathbb{Q}}(\overline{\varphi^-}\,\overline{\omega}))\le 1.$$

Thus $\dim_{\mathbb{F}}\mathcal{Y}^-(\varphi^-\omega)\otimes_{W[[H]]}\mathbb{F}\le 1$, and by Nakayama's lemma, $\mathcal{Y}^-(\varphi^-\omega)$ is cyclic over $W[[H]]$. Then by Theorem B (or Theorem 5.4), we obtain the desired assertion. □

Actually we also have

Lemma 6.4. *If* $p\nmid h_F$, *we have* $\mathrm{Sel}^{\perp}_{\emptyset}(\overline{\chi\omega})=0$; *so,* $r_+=0$.

Proof. By Proposition 3.6, $\mathrm{Sel}^{\perp}_{\emptyset}(\overline{\chi\omega})$ is isomorphic to the $\mathbb{F}$-dual of the $\overline{\chi\omega}$-eigenspace of the ray class group modulo p^∞ of the splitting field of $\chi\omega$ (which is the maximal totally real subfield of $F(\mu_p)$). 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, §7]). □

7. Cyclicity for a $\mathbb{Z}_p$-extension $K_{/F}$

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

$$L/F_\infty F(\phi)\ (\text{resp. } L^+/F^+_\infty F(\phi),\ L^-/F^-_\infty F(\phi),\ L^K/KF(\phi))$$

be the maximal p-abelian extension unramified outside $\mathfrak{p}$. By adding subscript "*sp*" (resp. "*tsp*"), we define maximal sub-extension of L, $L^\pm$ and L^K over $F_\infty F(\phi)$, $F^\pm_\infty F(\phi)$, $KF(\phi)$, respectively, in which $\overline{\mathfrak{p}}$ totally splits (resp. all the prime factors of $N\overline{\mathfrak{p}}$ totally split). Define

$$\begin{aligned}Y&=\mathrm{Gal}(L/F_\infty F(\phi)),\ Y^\pm=\mathrm{Gal}(L^\pm/F^\pm_\infty F(\phi)),\ Y_K=\mathrm{Gal}(L^K/KF(\phi)),\\ Y_{sp}&=\mathrm{Gal}(L_{sp}/F_\infty F(\phi)),\ Y^\pm_{sp}=\mathrm{Gal}(L^\pm_{sp}/F^\pm_\infty F(\phi)),\ Y^{sp}_K=\mathrm{Gal}(L^K_{sp}/KF(\phi)),\\ Y_{tsp}&=\mathrm{Gal}(L_{tsp}/F_\infty F(\phi)),\ Y^\pm_{tsp}=\mathrm{Gal}(L^\pm_{tsp}/F^\pm_\infty F(\phi)),\ Y^{tsp}_K=\mathrm{Gal}(L^K_{tsp}/KF(\phi)).\end{aligned}\tag{7.1}$$

Via canonical splitting

$$\mathrm{Gal}(F_\infty F(\phi)/F)=\mathbf{\Gamma}_F\times\mathrm{Im}(\phi),$$
$$\mathrm{Gal}(F^\pm_\infty F(\phi)/F)=\Gamma_\pm\times\mathrm{Im}(\phi)\ \text{and}\ \ \mathrm{Gal}(KF(\phi)/F)=\Gamma_K\times\mathrm{Im}(\phi)$$

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

$$\begin{aligned}Y(\phi)&=Y\otimes_{\mathbb{Z}_p[\mathrm{Im}(\phi)],\phi}W,\ Y^\pm(\phi)=Y^\pm\otimes_{\mathbb{Z}_p[\mathrm{Im}(\phi)],\phi}W,\ Y_K(\phi)=Y_K\otimes_{\mathbb{Z}_p[\mathrm{Im}(\phi)],\phi}W,\\ Y_{sp}(\phi)&=Y_{sp}\otimes_{\mathbb{Z}_p[\mathrm{Im}(\phi)],\phi}W,\ Y^\pm_{sp}(\phi)=Y^\pm_{sp}\otimes_{\mathbb{Z}_p[\mathrm{Im}(\phi)],\phi}W,\ Y^{sp}_K(\phi)=Y^{sp}_K\otimes_{\mathbb{Z}_p[\mathrm{Im}(\phi)],\phi}W,\\ Y_{tsp}(\phi)&=Y_{tsp}\otimes_{\mathbb{Z}_p[\mathrm{Im}(\phi)],\phi}W,\ Y^\pm_{tsp}(\phi)=Y^\pm_{tsp}\otimes_{\mathbb{Z}_p[\mathrm{Im}(\phi)],\phi}W,\ Y^{tsp}_K(\phi)=Y^{tsp}_K\otimes_{\mathbb{Z}_p[\mathrm{Im}(\phi)],\phi}W.\end{aligned}$$

Similarly, we define $\mathcal{Y}^-_{sp}(\phi)$ and $\mathcal{Y}^-_{tsp}(\phi)$ replacing F^-_∞ in the above definition by $K^-_\emptyset$.

Proposition 7.1. *Suppose* (h0) *and* (h4), *and write* ϕ *for any character of conductor a factor of* $N_{F/\mathbb{Q}}(\mathfrak{c})\mathfrak{p}$ *of order prime to* p *non-trivial over* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/F_{\overline{\mathfrak{p}}})$. *Then we have* $Y(\phi)=Y_{sp}(\phi)=Y_{tsp}(\phi)$, $Y^-_{tsp}(\varphi^-\omega)=Y^-(\varphi^-\omega)$ *and* $Y^{sp}_K(\phi)=Y_K(\phi)$. *Similarly we have* $\mathcal{Y}^-_{tsp}(\varphi^-\omega)=\mathcal{Y}^-_{sp}(\varphi^-\omega)=\mathcal{Y}^-(\varphi^-\omega)$ *and* $\mathcal{Y}^-_{sp}(\varphi^-)=\mathcal{Y}^-(\varphi^-)$.

Since the proof is essentially the same for Y and $\mathcal{Y}$, we only give a detailed proof for Y touching briefly $\mathcal{Y}$ at the end.

Proof. Let $\mathfrak{l}$ be a prime factor of $N\overline{\mathfrak{p}}$, and write $(l)=\mathfrak{l}\cap\mathbb{Z}$. We first give a proof for the $\mathbb{Z}_p^2$-extension F_∞. In F_∞/F, we have a $\mathbb{Z}_p$-extension K unramified outside $\mathfrak{l}$. Since $\mathrm{Gal}(F_\infty/F)$ contains $1+pO_p$ as an open subgroup, the decomposition group of $\mathfrak{l}$ in $\mathrm{Gal}(F_\infty/F)$ contains a subgroup generated by $1+\mathfrak{p}O_{\mathfrak{p}}$ and $\alpha^{\mathbb{Z}_p}$ for a generator α of $\mathfrak{l}^{h_F(p-1)}$; so, we can find a $\mathbb{Z}_p$-extension K/F unramified at $\mathfrak{l}$ whose residual extension is a still $\mathbb{Z}_p$-extension over $\mathbb{F}_l$. Therefore the residual p-extension is exhausted in $F_\infty F(\phi)/F(\phi)$; so, $L(\phi)=L_{sp}(\phi)=L_{tsp}(\phi)$ and hence $Y^{sp}(\phi)=Y(\phi)$.

We now give a proof for Y_K for a general $\mathbb{Z}_p$-extension $K_{/F}$. If K localized at $\mathfrak{l}$ contains the unramified local $\mathbb{Z}_p$-extension, we are done by the same argument as above. In particular, F^-_∞ localized at $\mathfrak{l}$ contains the unramified local $\mathbb{Z}_p$-extension if $\mathfrak{l} \nmid Dp$.

For a prime factor $\mathfrak{l}|N$, $(l) = \mathfrak{l} \cap \mathbb{Z}$ splits into $\mathfrak{l}\overline{\mathfrak{l}}$ in F. Then $\mathfrak{l}^{(p-1)h_F}$ is generated by $\alpha \in O$. Consider the subgroup $\alpha^{\mathbb{Z}_p}$ inside $1+pO_p \subset \mathrm{Gal}(F_\infty/F)$. Unless $\alpha^{\mathbb{Z}_p} \subset \mathrm{Gal}(F_\infty/K)$, K localized at $\mathfrak{l}$ contain the unramified $\mathbb{Z}_p$-extension. If $\alpha^{\mathbb{Z}_p} \subset \mathrm{Gal}(F_\infty/K)$, $\mathfrak{l}$ splits totally in K/F.

Thus we may assume that $\mathfrak{l}|N$ totally splits in K/F, and we need to show that $Y^-_{tsp}(\varphi^-\omega) = Y^-(\varphi^-\omega)$. Take $K = F^-_\infty$, and assume $\mathfrak{l}|D$ as the case $\mathfrak{l}|N_{F/\mathbb{Q}}(\mathfrak{c})$ is already taken care of. In this case, $\mathfrak{l}$ totally splits in F^-_∞/F. Since φ^- is anticyclotomic, we have $\varphi^-(\mathfrak{l}) = 1$, and $F^-_\infty F(\varphi^-)/F$, $\mathfrak{l}$ totally splits. Take a prime $\mathfrak{L}_0$ of $F^-_\infty F(\varphi^-)$ above $\mathfrak{l}$. Then we have $F^-_\infty F(\varphi^-)_{\mathfrak{L}_0} = F_{\mathfrak{l}}$. Pick a prime $\mathfrak{L}$ of $L^K(\varphi^-\omega)$ above $\mathfrak{l}$. Then any sub p-abelian extension X of $F_{\mathfrak{l}}$ in the extension $L^K(\varphi^-\omega)_{\mathfrak{L}}/F_{\mathfrak{l}}$ is inside a Kummer extension $F_{\mathfrak{l}}[\mu_p][\sqrt[p]{\varpi}]$ for a prime element ϖ of $F_{\mathfrak{l}}$ by $p \nmid (l-1)$. Then $X_{/F_{\mathfrak{l}}}$ totally ramifies at $\mathfrak{l}$; so, no residual extension. Thus we conclude $L^K(\varphi^-\omega) = L^K_{tsp}(\varphi^-\omega)$, once we prove $L^K(\varphi^-\omega) = L^K_{sp}(\varphi^-\omega)$.

Thus from now on we study the behavior of $\overline{\mathfrak{p}} = \mathfrak{p}^c$. By definition, we can realize $Y^{sp}_K(\phi)$ (resp. $Y_K(\phi)$) as the Galois group $\mathrm{Gal}(L^K_{sp}(\phi)/KF(\phi)))$ (resp. $\mathrm{Gal}(L^K(\phi)/KF(\phi)))$ for a sub-extension $L^K_{sp}(\phi)$ (resp. $L^K(\phi)$) of L^K_{sp} (resp. L^K). Localizing at $\overline{\mathfrak{p}} = \mathfrak{p}^c$ and at a prime $\mathfrak{P}|\overline{\mathfrak{p}}$ of $L^K_{sp}(\phi)$, the Galois group $\mathrm{Gal}(F(\phi)_{\mathfrak{P}}/F_{\overline{\mathfrak{p}}})$ acts on $\mathrm{Gal}(L^K(\phi)_{\mathfrak{P}}/L^K_{sp}(\phi)_{\mathfrak{P}})$ by conjugation.

Suppose that ϕ is unramified at $\overline{\mathfrak{p}}$ and $\mathrm{Gal}(L^K(\phi)_{\mathfrak{P}}/L^K_{sp}(\phi)_{\mathfrak{P}}) \neq 1$. Since Frob_p generates $\mathrm{Gal}(F(\phi)_{\mathfrak{P}}/F_{\mathfrak{P}})$, conjugation action of $\mathrm{Gal}(F(\phi)_{\mathfrak{P}}/F_{\mathfrak{P}})$ on $\mathrm{Gal}(L^K(\phi)_{\mathfrak{P}}/L^K_{sp}(\phi)_{\mathfrak{P}})$ factors through the abelian group $\mathrm{Frob}_p^{\widehat{\mathbb{Z}}}$ and hence is trivial, a contradiction (as $\phi(\mathrm{Frob}_p) \neq 1$). Thus $L^K_{sp}(\phi)_{\mathfrak{P}} = L^K(\phi)_{\mathfrak{P}}$ for any $\mathfrak{P}|\overline{\mathfrak{p}}$ and hence $L^K_{sp}(\phi) = L^K(\phi)$ which implies $Y^{sp}_K(\phi) = Y_K(\phi)$.

Suppose now that $F(\phi)^{I_{\overline{\mathfrak{p}}}} \neq F$ and $L^K_{sp}(\phi)_{\mathfrak{P}} \neq L^K(\phi)_{\mathfrak{P}}$). Let $\mathfrak{P}_{sp}$ (resp. $\mathfrak{P}_K$, $\mathfrak{P}_\phi$) be the primes below $\mathfrak{P}$ of L^K_{sp} (resp. $KF(\phi)$, $F(\phi)$). Write $\mathbb{F}_X$ for the residue field of X for the prime ideal $X = \mathfrak{P}, \mathfrak{P}_{sp}, \mathfrak{P}_K, \mathfrak{P}_\phi$. Consider the residual extension $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{P}_{sp}}/\mathbb{F}_{\mathfrak{P}_K}/\mathbb{F}_{\mathfrak{P}_\phi}$. Then $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}_\phi}/\mathbb{F}_p)$ acts trivially on $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{P}_{sp}})$ by conjugation. Since the action factors through the restriction of ϕ to the Galois group of maximal $\mathfrak{P}$-unramified sub-extension of $F(\phi)/F$ (which is non-trivial). Thus we have $\mathbb{F}_{\mathfrak{P}} = \mathbb{F}_{\mathfrak{P}_{sp}}$, which implies $L^K(\phi) = L^K_{sp}(\phi)$ and hence $Y^{sp}_K(\phi) = Y_K(\phi)$.

Finally we assume that $F(\phi)/F$ fully ramify at $\overline{\mathfrak{p}}$. If K/F is unramified at $\overline{\mathfrak{p}}$ (so, $\mathrm{Gal}(K/F)$ contains $1+\mathfrak{p}O_{\mathfrak{p}}$ as an open subgroup), the decomposition group of $\overline{\mathfrak{p}}$ in $\mathrm{Gal}(K/F)$ contains $\alpha^{\mathbb{Z}_p} \in 1+\mathfrak{p}O_{\mathfrak{p}}$ for a generator α of $\overline{\mathfrak{p}}^{h_F(p-1)}$; so, it is open in $\mathrm{Gal}(K/F)$. Therefore the residual p-extension is exhausted in $KF(\phi)/F(\phi)$; so, $L^K(\phi) = L^K_{sp}(\phi)$ and hence $Y^{sp}_K(\phi) = Y_K(\phi)$. Thus we may assume that the $\overline{\mathfrak{p}}$-inertia subgroup I of $\mathrm{Gal}(KF(\phi)/F)$ is an open subgroup. Then over the I-fixed field $(KF(\phi)_{\mathfrak{P}})^I$, $K_{\mathfrak{P}}$ and the maximal unramified extension $L^{ur}_{\mathfrak{P}}$ inside $L^K_{\mathfrak{P}}$ are linearly disjoint, and $L^K_{\mathfrak{P}} = L^{ur}_{\mathfrak{P}} K_{\mathfrak{P}}$; so, $\mathrm{Gal}(L^K_{\mathfrak{P}}/(KF(\phi)_{\mathfrak{P}})^I) \cong I \times \mathrm{Gal}(L^{ur}_{\mathfrak{P}}/\mathbb{Q}_p)$. This shows the Galois group $\mathrm{Gal}(F(\phi)/F) \hookrightarrow I$ acts again trivially on $\mathrm{Gal}(L^K/L^K_{sp})$ and hence $Y^{sp}_K(\phi) = Y_K(\phi)$.

We can take $K^-_\emptyset$ in place of K as above, and the same argument proves $\mathcal{Y}^-_{tsp}(\varphi^-\omega) = \mathcal{Y}^-(\varphi^-\omega)$ and $\mathcal{Y}^-_{sp}(\varphi^-) = \mathcal{Y}^-(\varphi^-)$. □

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 $\mathcal{L}_\infty/F_\infty\mathbb{H}(\phi)$ (resp. $\mathcal{L}^+_\infty/F^+_\infty\mathbb{H}(\phi)$, $\mathcal{L}^-_\infty/F^-_\infty\mathbb{H}(\phi)$, $\mathcal{L}^K_\infty/K\mathbb{H}(\phi)$) be the maximal p-abelian extension unramified outside $\mathfrak{p}$. Put

$$\mathcal{H} = \mathrm{Gal}(\mathcal{L}_\infty/F_\infty\mathbb{H}(\phi)),\ \mathcal{H}^\pm = \mathrm{Gal}(\mathcal{L}^\pm_\infty/F^\pm_\infty\mathbb{H}(\phi)),\ \mathcal{H}_K = \mathrm{Gal}(\mathcal{L}^+_\infty/K\mathbb{H}(\phi)).$$

Lemma 7.2. *Assume $p \nmid h_F$ and (h0–4). Let $\phi = \varphi^-$ or $\varphi^-\omega$. Lifting the character ϕ to $\mathrm{Gal}(\mathbb{H}(\phi)/F)$ for the composite $\mathbb{H}(\phi) = \mathbb{H}F(\phi)$, we have*

$$Y^-(\phi) \cong \mathcal{H}^- \otimes_{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{H}(\phi)/F)],\phi} W,\ Y(\phi) \cong \mathcal{H} \otimes_{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{H}(\phi)/F)],\phi} W$$
$$\text{and}\ \ Y(\phi) \cong \mathcal{H} \otimes_{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{H}(\phi)/F)],\phi} W,\ Y_K(\phi) \cong \mathcal{H}_K \otimes_{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{H}(\phi)/F)],\phi} W.$$

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

$$Y(\phi) \cong \mathcal{H} \otimes_{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{H}(\phi)/F)],\phi} W.$$

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

$$Y_K(\phi) \cong \mathcal{H}_K \otimes_{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{H}(\phi)/F)],\phi} W$$

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 $K := F^{\pm}_\infty$). □

Let $\mathfrak{a}_\mp = \mathrm{Ker}(W[[\mathbf{\Gamma}_F]] \twoheadrightarrow W[[\Gamma_\pm]])$ and $\mathfrak{a}_K = \mathrm{Ker}(W[[\mathbf{\Gamma}_F]] \twoheadrightarrow W[[\Gamma_K]])$. Then we have a natural $W[[\mathbf{\Gamma}_F]]$-linear maps

$$\pi_+ : Y/\mathfrak{a}_+ Y \to Y^+,\ \pi_K : Y/\mathfrak{a}_K Y \to Y_K \ \text{ and } \ \pi_- : Y/\mathfrak{a}_- Y \to Y^-.$$

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

Theorem 7.3 (K. Rubin)**.** *Suppose $p \nmid h_F$ and* (h0–4)*, and let $\phi = \varphi^-$ or $\varphi^-\omega$. Let K/F be a $\mathbb{Z}_p$-extension. Then $\pi_\pm$ and π_K are all surjective. If either F_∞/K is unramified outside $\mathfrak{p}$ or ϕ is non-trivial on* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$*, we have*

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

as $W[[\mathbf{\Gamma}_F]]$-modules.

Proof. Under the assumption of the theorem, the character ϕ is non-trivial. Indeed, if $\phi = \varphi^-$, the non-triviality follows from (h3). If $\phi = \varphi^-\omega$ is trivial, $\varphi^- = \omega^{-1}$ which is anti-cyclotomic and cyclotomic; so, has order ≤ 2 against (h3). Thus ϕ is non-trivial in this case also. Then by Rubin [Ru91, Theorem 5.3 (i)-(ii)], the corresponding assertions hold between

$$\mathcal{H}(\phi) := \mathcal{H} \otimes_{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{H}(\phi)/\mathbb{H})],\phi} W \ \text{ and } \ \mathcal{H}_K(\phi) := \mathcal{H}_K \otimes_{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{H}(\phi)/\mathbb{H})],\phi} W.$$

This is equivalent to the assertion of the theorem by Lemma 7.2. □

Corollary 7.4. *Assume $p \nmid h_F$ and* (h0–4)*. Let $\phi = \varphi^-$ or $\varphi^-\omega$ and $K_{/F}$ be a $\mathbb{Z}_p$-extension.*

(1) *If either F_∞/K is unramified outside $\mathfrak{p}$ or ϕ is non-trivial on* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/F_{\overline{\mathfrak{p}}})$*, then cyclicity for $Y_K(\phi)$ over $W[[\Gamma_K]]$, cyclicity of $Y^-(\phi)$ over $W[[\Gamma_-]]$ and cyclicity of $Y(\phi)$ over $W[[\mathbf{\Gamma}_F]]$ are all equivalent.*

(2) *Cyclicity of $Y(\phi)$ over $W[[\mathbf{\Gamma}_F]]$ implies cyclicity $Y_K(\phi)$ of $W[[\Gamma_K]]$.*

(3) *If further $(Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F})[\overline{\varphi}^-] = 0$, $Y_K(\phi)$ over $W[[\Gamma_K]]$, $Y^-(\phi)$ over $W[[\Gamma_-]]$ and $Y(\phi)$ over $W[[\mathbf{\Gamma}_F]]$ are cyclic.*

Proof. By Nakayama's lemma applied to $W[[\mathbf{\Gamma}_F]]$, as long as $Y(\varphi^-)/\mathfrak{a}_K Y(\varphi^-) \cong Y_K(\varphi^-)$, cyclicity of $Y(\varphi^-)$ over $W[[\mathbf{\Gamma}_F]]$ is equivalent to that of $Y_K(\varphi^-)$. This holds in particular for $K = F^-_\infty$ as F_∞/F^-_∞ is unramified everywhere. Then the first assertion follows from the above theorem.

If $Y(\varphi^-)$ is cyclic over $W[[\mathbf{\Gamma}_F]]$, cyclicity $Y_K(\varphi^-)$ over $W[[\Gamma_K]] = W[[\mathbf{\Gamma}_F]]/\mathfrak{a}_K$ follows from the surjectivity the projection: $Y(\varphi^-)/\mathfrak{a}_K Y(\varphi^-) \to Y_K(\varphi^-)$. Thus again the second assertion follows from the above theorem.

The assertion (3) then follows from (1) and (2) combined with Proposition 7.1. Indeed we have $\mathrm{Hom}_{W[[H]]}(Y^-(\phi), \mathbb{F}) \cong \mathrm{Hom}_{W[[H]]}(Y(\phi), \mathbb{F})$ by Proposition 7.1, as ϕ is non-trivial over $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ by (h4). Thus $Y(\phi)$ is cyclic over $W[[H]]$ if and only if $Y^-(\phi)$ is cyclic over $W[[H]]$. □

8. Degree of CM components over the Iwasawa algebra

We continue to assume that F is imaginary. Let $\mathrm{Spec}(\mathbb{T})$ 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 $\mathrm{Spec}(\mathbb{T})$ is contained in $\mathrm{Spec}(W[[H]])$ (and $\mathbb{T} = W[[H]] \Leftrightarrow L_p \in W[[H]]^\times$). Since $\iota : Z \cong H$ by (1.6), H canonically contains $\iota(\Gamma)$ for $\Gamma = 1 + p\mathbb{Z}_p$ embedded into $O^\times_{\mathfrak{p}}$. We identify Γ and $\iota(\Gamma) \subset H$. Thus decomposing $H = \Gamma_- \times \Delta$ for the torsion-free subgroup $\Gamma_- \supset \Gamma$ and a finite group Δ, each irreducible CM component is isomorphic to $\mathrm{Spec}(W[[\Gamma_-]])$. Since $\Gamma_- \cong \mathbb{Z}_p$, we find that $\dim_{\mathbb{K}} \mathrm{Frac}(W[[\Gamma_-]]) = [\Gamma_- : \Gamma] = p^m$ for some $m \geq 0$. Recall $C := \mathrm{Gal}(F_{\mathfrak{c}\mathfrak{p}}/F)$ for the maximal p-abelian extension $F_{\mathfrak{c}\mathfrak{p}}/F$ of conductor dividing $\mathfrak{c}\mathfrak{p}$. Since the image $\Gamma_-/\Gamma \hookrightarrow C$ and $C \hookrightarrow Cl_F$ (under (h0)) for the class group Cl_F of F, if $h_F = p^h\eta$ $(h, \eta \in \mathbb{Z})$ with $p \nmid \eta$ for the class number $h_F = |Cl_F|$, we have $0 \leq m \leq h$. If we find an O-ideal $\mathfrak{a}$ prime to p such that $\mathfrak{a}^{p^n} = (\alpha)$ with $\alpha \in O$ (for $0 \leq n \leq h$) with $\alpha^{p-1} \not\equiv 1 \mod \mathfrak{p}^2$, we find that $m \geq n$. Thus we get

Proposition 8.1. *Let the notation be as above. Assume* (h0–4). *For a CM component $\mathbb{I}$ of* $\mathbf{h}$, *we have* $\dim_{\mathbb{K}} \mathrm{Frac}(\mathbb{I}) = p^m$ *with* $0 \le m \le h$. *If we find an O-ideal $\mathfrak{a}$ prime to p such that* $\mathfrak{a}^{p^n} = (\alpha)$ *with $\alpha \in O$ (for $0 \le n \le h$) with* $\alpha^{p-1} \not\equiv 1 \mod \mathfrak{p}^2$, *we find that $m \ge n$.*

By the last assertion of the above proposition, we can easily create many examples of CM components with $\mathrm{Frac}(\mathbb{I}) \neq \mathbb{K}$. An interesting point is that the dimension $\dim_{\mathbb{K}} \mathrm{Frac}(\mathbb{I})$ is a p-power, while non CM component we studied earlier often satisfies $\dim_{\mathbb{K}} \mathrm{Frac}(\mathbb{I}) = 2$. As shown in [KhR15], there are also examples of non CM component with arbitrary large degree over Λ.

Take an irreducible component $\mathrm{Spec}(\mathbb{I})$ of $\mathrm{Spec}(\mathbb{T})$, and write its complementary (reduced) component as $\mathrm{Spec}(\mathbb{I}^{\perp})$. Thus we have $\mathrm{Spec}(\mathbb{T}) = \mathrm{Spec}(\mathbb{I}^{\perp}) \cup \mathrm{Spec}(\mathbb{I})$, and $\mathrm{Spec}(\mathbb{I} \otimes_{\mathbb{T}} \mathbb{I}^{\perp}) = \mathrm{Spec}(\mathbb{I}) \cap \mathrm{Spec}(\mathbb{I}^{\perp})$ has codimension ≥ 1 in $\mathrm{Spec}(\mathbb{T})$. Suppose that $\mathbb{I}$ is Gorenstein. This is true for CM components as it is isomorphic to the regular ring $W[[\Gamma_-]]$. If $\mathbb{T}^{\mathrm{ncm}}$ is non-trivial and integral, $\mathbb{I} = \mathbb{T}^{\mathrm{ncm}}$ is Gorenstein (as we proved that $\mathbb{T}^{\mathrm{ncm}}$ 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], $\mathbb{I} \otimes_{\mathbb{T}} \mathbb{I}^{\perp} = \mathbb{I}/(L_p(Ad(\rho_{\mathbb{I}})))$ for a p-adic L-function $L_p(Ad(\rho_{\mathbb{I}})) \in \mathbb{I}$ interpolating $L(1, Ad(\rho_P))$ divided the canonical period for P running through arithmetic points of $\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$.

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

9. Divisibility of the adjoint p-adic L-function

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

$$\widetilde{\mathbb{T}} \cong \mathrm{Hom}_{\Lambda}(\mathbb{T}, \Lambda) \otimes_{\Lambda} \widetilde{\mathbb{I}} \cong \mathrm{Hom}_{\Lambda}(\mathbb{T} \otimes_{\Lambda} \widetilde{\mathbb{I}}, \widetilde{\mathbb{I}}). \tag{9.1}$$

This follows from the fact that $\widetilde{\mathbb{I}}$ is Λ-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, (5.5b)]). We fix the identification (9.1). Decompose $\mathrm{Frac}(\widetilde{\mathbb{T}}) = \mathrm{Frac}(\mathbb{I}) \oplus S$ as a $\mathbb{K}$-algebra direct sum, and define $\mathbb{I}^{\perp}$ for the image of $\widetilde{\mathbb{T}}$ in S, where $\lambda : \widetilde{\mathbb{T}} \to \mathrm{Frac}(\mathbb{I})$ is induced by the projection $\widetilde{\mathbb{T}} = \mathbb{T} \otimes_{\Lambda} \widetilde{\mathbb{I}}$ given by $t \otimes \widetilde{i} = \pi(t)\widetilde{i} \in \widetilde{\mathbb{I}}$. Regarding $\lambda : \widetilde{\mathbb{T}} \to \widetilde{\mathbb{I}}$, we take adjoint $\lambda^* : \widetilde{\mathbb{I}} = \mathrm{Hom}_{\widetilde{\mathbb{I}}}(\widetilde{\mathbb{I}}, \widetilde{\mathbb{I}}) \to \mathrm{Hom}_{\widetilde{\mathbb{I}}}(\widetilde{\mathbb{T}}, \widetilde{\mathbb{I}}) = \widetilde{\mathbb{T}}$. Then define $L_p(Ad\rho_{\mathbb{I}}) := \lambda \circ \lambda^* \in \mathrm{Hom}_{\widetilde{\mathbb{I}}}(\widetilde{\mathbb{I}}, \widetilde{\mathbb{I}}) = \widetilde{\mathbb{I}}$. As shown in [H86c, Lemma 1.6] (or [MFG, §5.3.3]), we have $C_0(\lambda, \widetilde{\mathbb{I}}) := \mathbb{I}^{\perp} \otimes_{\widetilde{\mathbb{T}}} \widetilde{\mathbb{I}} \cong \widetilde{\mathbb{I}}/(L_p(Ad(\rho_{\mathbb{I}})))$ as $\widetilde{\mathbb{I}}$-modules. This $L_p(Ad(\rho_{\mathbb{I}}))$ interpolates the adjoint L-values $L(1, Ad(\rho_P))/\Omega_P$ for arithmetic points P for the canonical period Ω_P written as $U_{\infty}(f_P)U_p(f_P)$ in [H88b, Theorem 0.1] and coincides with the one introduced in the previous section if $\mathbb{I}$ is Gorenstein (i.e., $L_p(Ad(\rho_{\mathbb{I}}))$ is contained in $\mathbb{I}$ if $\mathbb{I}$ 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 $\mathbf{h}$ is reduced (for example, N is cube-free; see [H13, Section 1]). To see this, we consider the jacobian variety $J_1(Xp^r)$ 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 $\{T_p J_1(Np^r)^{\mathrm{ord}}\}_r$. Put $L := \varprojlim_r T_p J_1(Np^r)^{\mathrm{ord}}$. Then as shown in [H86b] (see also [H14, Sections 4–5]), L is naturally an $\mathbf{h}$-module and is also Λ-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 $\mathbf{h}$-modules:

$$0 \to \mathbf{h} \to L \to \mathbf{h}^{\vee} \to 0. \tag{9.2}$$

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, §6.5.5] for more details of this).

We want to prove

Theorem 9.1. *Suppose $p \geq 5$, let* $\mathrm{Spec}(\mathbb{I})$ *be an irreducible non CM component of* $\mathrm{Spec}(\mathbb{T})$ *satisfying* (h0–4)*, and write $\widetilde{\mathbb{I}}$ be the normalization of $\mathbb{I}$ in* $\mathrm{Frac}(\mathbb{I})$*. Then, under the equivalent conditions of* Theorem 5.4*, we have*

1. *If* $\mathrm{Spec}(\mathbb{J})$ *is a CM component of* $\mathrm{Spec}(\mathbb{T})$ *and $\overline{\varphi}$ ramifies at p, then the ideal $(L_p(Ad(\rho_{\mathbb{J}})))$ of $\mathbb{J}$ is generated by the φ^--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 $\sqrt{L_p(\varphi^-)} \in \widetilde{\mathbb{I}}$, $\mathrm{rank}_\Lambda \widetilde{\mathbb{I}} \geq 2$, the p-adic L-function $L_p(Ad(\rho_{\mathbb{I}}))$ is a non-unit in $\widetilde{\mathbb{I}}$, and $\sqrt{L_p(\varphi^-)}$ divides $(L_p(Ad(\rho_{\mathbb{I}})))$ in $\widetilde{\mathbb{I}}$. If further* $\mathrm{rank}_\Lambda \mathbb{T}^{\mathrm{ncm}} = 2$*, then $\mathbb{I} = \widetilde{\mathbb{I}} = \Lambda[\sqrt{L_p(\varphi^-)}]$ and $(L_p(Ad(\rho_{\mathbb{I}}))) = (\sqrt{L_p(\varphi^-)})$.*

The example given in [H85, (10a,b)] shows the case (2) in the above theorem actually occurs, and indeed, in this case, $\mathbb{T} = \Lambda[\sqrt{L_p}]$ and (L_p) 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 $\widetilde{\mathbb{T}} = \mathbb{T} \otimes_\Lambda \widetilde{\mathbb{I}} \to \mathbb{I} \otimes_\Lambda \widetilde{\mathbb{I}} \xrightarrow{m} \widetilde{\mathbb{I}}$ as λ, where the right most arrow is the multiplication ($a \otimes b \mapsto ab$). Since $\widetilde{\mathbb{T}} = \mathbb{T} \otimes_\Lambda \widetilde{\mathbb{I}}$ surjects down to $\mathbb{I} \otimes_\Lambda \widetilde{\mathbb{I}}$, we have $\mathrm{Spec}(\widetilde{\mathbb{I}}) \subset \mathrm{Spec}(\mathbb{I} \otimes_\Lambda \widetilde{\mathbb{I}}) \subset \mathrm{Spec}(\widetilde{\mathbb{T}})$. Consider the congruence modules (see [MFG, §5.3.3] for congruence modules)

$$C_0(\lambda; \widetilde{\mathbb{I}}) := \mathbb{I}^\perp \otimes_{\widetilde{\mathbb{T}},\lambda} \widetilde{\mathbb{I}} \text{ and } C_0(m; \widetilde{\mathbb{I}}) = \mathbb{I}' \otimes_{\widetilde{\mathbb{T}},m} \widetilde{\mathbb{I}}$$

for $\mathbb{I}'$ given by $\mathrm{Spec}(\mathbb{I}') = \mathrm{Spec}(\mathbb{I}^\perp) \cap \mathrm{Spec}(\mathbb{I} \otimes_\Lambda \widetilde{\mathbb{I}})$ (i.e., $\mathrm{Spec}(\mathbb{I}')$ is the complementary component of $\mathrm{Spec}(\widetilde{\mathbb{I}})$ in $\mathrm{Spec}(\mathbb{I} \otimes_\Lambda \widetilde{\mathbb{I}})$). Note that $C_0(\lambda; \widetilde{\mathbb{I}}) = \mathbb{I}^\perp \otimes_{\mathbb{T}} \widetilde{\mathbb{I}} \cong \widetilde{\mathbb{I}}/(L_p(Ad(\rho_{\mathbb{I}}))$ by definition. Thus we have a surjective $\widetilde{\mathbb{I}}$-linear map $C_0(\lambda, \widetilde{\mathbb{I}}) = \widetilde{\mathbb{I}}/(L_p(Ad(\rho_{\mathbb{I}})) \twoheadrightarrow C_0(m, \widetilde{\mathbb{I}})$ as $\mathrm{Spec}(\mathbb{I}^\perp) \cap \mathrm{Spec}(\widetilde{\mathbb{I}}) \supset \mathrm{Spec}(\mathbb{I}') \cap \mathrm{Spec}(\widetilde{\mathbb{I}})$.

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

If further $\mathbb{T}^{\mathrm{ncm}} = \mathbb{I}$ and $\mathrm{rank}_\Lambda \mathbb{T}^{\mathrm{ncm}} = 2$, then $\mathbb{I} = \Lambda[\sqrt{L_p(\varphi^-)}]$, and by the semi-simplicity conjecture, $\mathbb{I}$ is integrally closed; so, $\widetilde{\mathbb{I}} = \mathbb{I}$. Then, from $W[[H]]/(L_p(\varphi^-)) \cong \mathbb{I}/(\sqrt{L_p(\varphi^-)})$, we find that

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

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

10. 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 developped by Hartshorne [RDD] and Kleiman [Kl80]. Let S be a base local ring. For any S-module M, we define $M^\dagger := \mathrm{Hom}_S(M, S)$.

Lemma 10.1. *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. *$A^\dagger \cong A$ 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 ω_A given by $\mathrm{Hom}_S(A, \omega_S)$. 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 ω_R of R. Since $\omega_S \cong S$, we find $\omega_A \cong A^\dagger$, and hence A is Gorenstein if and only if $A^\dagger \cong A$. □

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 $\sigma \in \mathrm{Aut}(A)$ be an S-algebra involution. We allow the case where σ acts non-trivially on S. Put $A_\pm := \{x \in A | \sigma(x) = \pm x\}$. Then by Lemma 10.1, we get $A^\dagger \cong A$ as A-modules. Since σ acts by duality on $A^\dagger$, we have $A^\dagger_\pm = (A^\dagger)_\pm := \{x \in A^\dagger | \sigma(x) = \pm x\}$. Note that $A^\dagger_\pm \cong \mathrm{Hom}_S(A_\pm, S)$. Thus σ acts on $\mathrm{Hom}_A(A^\dagger, A)$ and $\mathrm{Isom}_A(A^\dagger, A)$ 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 ϕ^σ is A-linear. We then consider the $\pm$-eigenspace $\mathrm{Hom}_A(A^\dagger, A)^\pm$ for $a \in A$ and $\mathrm{Isom}_A(A^\dagger, A)^\pm := \mathrm{Hom}_A(A^\dagger, A)^\pm \cap \mathrm{Isom}_A(A^\dagger, A)$. Here $\mathrm{Isom}_A \subset \mathrm{Hom}_A$ is made up of A-linear isomorphisms. The set $\mathrm{Isom}_A(A^\dagger, A)^\pm$ could be empty.

If σ fixes S point by point, we have $(A^\dagger)_\pm = (A_\pm)^\dagger$, which we just write $A^\dagger_\pm$.

Lemma 10.2. *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 $\sigma \in \mathrm{Aut}_S(A)$ be an algebra involution fixing S point by point.*

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

Proof. Since A is Gorenstein, we have $A^\dagger \cong A$ as A-modules by Lemma 10.1. Thus we conclude $\mathrm{Isom}_A(A^\dagger, A) \neq \emptyset$. Pick $\phi \in \mathrm{Isom}_A(A^\dagger, A)$. Let $\phi^\pm = \phi \pm \phi^\sigma$. Then for $a \in A$, we have

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

Then $\phi^+ + \phi^- = 2\phi$. If one ϕ^ε of $\phi^\pm$ is not onto, we conclude $\mathrm{Im}(\phi^\varepsilon) \subsetneq A$ is a proper A-submodule of A; so, $\mathrm{Im}(\phi^\varepsilon) \subset \mathfrak{m}_A$. This shows $\phi^{-\varepsilon} = 2\phi - \phi^\varepsilon \equiv 2\phi \mod \mathfrak{m}_A$, which implies $\phi^{-\varepsilon}$ is onto (as $p > 2$). Identifying $A^\dagger$ with A, we can iterate $\Phi := \phi^{-\varepsilon}$, and $\mathrm{Ker}(\Phi^n)$ is an ascending sequence of A-ideals. Since A is noetherian, for some $n \gg 0$, we have $\mathrm{Ker}(\Phi^n) = \mathrm{Ker}(\Phi^{n+1})$. Thus we conclude

$$\Phi : A = \mathrm{Im}(\Phi^n) = A/\mathrm{Ker}(\Phi^n) \underset{\sim}{\xrightarrow{\Phi}} A/\mathrm{Ker}(\Phi^{n+1}) = \mathrm{Im}(\Phi^{n+1}) = A$$

and hence $\phi^{-\varepsilon}$ is an isomorphism.

If $\mathrm{rank}_S A_+ > \mathrm{rank}_S A_-$, by A_+-indecomposability of A_+ as A_+-modules, the Krull-Schmidt theorem tells us $A^\dagger_+ \cong A_+$ and hence $A^\dagger_- \cong A_-$. 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 $\phi \in \mathrm{Isom}_A(A^\dagger, A)$ is forced to preserve A_+ and A_-; so, we have $\mathrm{Isom}_A(A^\dagger, A)^+ \neq \emptyset$ and $\mathrm{Isom}_A(A^\dagger, A)^- = \emptyset$. Thus we get $A^\dagger_+ \cong A_+$ as A_+-modules (i.e., A_+ is Gorenstein).

Now suppose $\mathrm{rank}_S A_+ = \mathrm{rank}_S A_-$ and $\mathrm{Isom}_A(A^\dagger, A)^\varepsilon \neq \emptyset$. Thus $A_\pm \cong A^\dagger_{\varepsilon\pm}$ as A_+-modules, and $\mathrm{Isom}_A(A_\dagger, A)^+ \neq \emptyset$ implies $A^\dagger_+ \cong A_+$ as A_+-modules (i.e., A is Gorenstein). Similarly $\mathrm{Isom}_A(A^\dagger, A)^+ = \emptyset$ implies $\mathrm{Isom}_A(A^\dagger, A)^- \neq \emptyset$ by (1), and $A^\dagger_+ \cong A_-$ as A_+-modules.

Since $\mathrm{Frac}(A)$ is a product of fields, for each simple component K of $\mathrm{Frac}(A)$, 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

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

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 $X := \mathrm{Spec}(A) \xrightarrow{f} \mathrm{Spec}(B) =: Y$ 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 $\mathrm{Hom}_A(F, f^!N) = \mathrm{Hom}_B(f_*F, N)$ 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 $\omega_{A/B} = f^!(\mathcal{O}_Y) = \mathrm{Hom}_B(A, B)$ as A-modules. As shown in [Kl80, (21)], $\mathrm{Spec}(A) \xrightarrow{f} \mathrm{Spec}(B)$ 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 $\omega_{A/B} := \mathrm{Hom}_B(A, B)$ generally.

Suppose that we have an involution $\sigma \in \mathrm{Aut}(A/B)$. Let $A_+ = A^{\mathcal{G}}$ for the order 2 subgroup $\mathcal{G}$ of $\mathrm{Aut}(A/B)$ generated by σ. 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 ring,
(4) A/B is generically étale (i.e., $\mathrm{Frac}(A)$ is reduced separable over $\mathrm{Frac}(B)$),

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 $\mathrm{Frac}(\square)$. 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 $\omega_{C/B} := \mathrm{Hom}_B(C, B)$ in general. Suppose that $\mathrm{Frac}(C)/\mathrm{Frac}(B)$ is étale; so, we have a well defined trace map $\mathrm{Tr} : \mathrm{Frac}(C) \to \mathrm{Frac}(B)$, and $\omega_{\mathrm{Frac}(C)/\mathrm{Frac}(B)} = \mathrm{Frac}(C)\mathrm{Tr}$ by the trace pairing $(x, y) \mapsto \mathrm{Tr}(xy)$. We define an C-fractional ideal by

$$\mathfrak{d}^{-1}_{C/B} := \{x \in C | \mathrm{Tr}(xC) \subset B\}.$$

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

Proposition 10.3. *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* $\mathrm{Frac}(D)$ *is* $\mathrm{Frac}(C)$*-free. Then we have $\mathfrak{d}^{-1}_{D/C}\mathfrak{d}^{-1}_{C/B} = \mathfrak{d}^{-1}_{D/B}$ and $\omega_{D/C} \otimes_C \omega_{C/B} \cong \omega_{D/B}$.*

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

Lemma 10.4. *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) $\mathrm{Frac}(A)/\mathrm{Frac}(A_+)$ is an étale extension,
(3) $\mathrm{Frac}(A)$ is free of rank 2 over $\mathrm{Frac}(A_+)$,
(4) $\mathfrak{d}_{A/A_+} \subset \mathfrak{m}_A$ 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 $\sigma(\delta) = -\delta$.

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

Proof. From Lemma 10.1, we conclude $A^* \cong \omega_{A/A_+} \cong A$. Thus we conclude

$$\omega_{A/A_+} \cong \mathfrak{d}^{-1}_{A/A_+} = A\theta^{-1}$$

with a non-zero divisor $\theta \in A$. Similarly $\mathfrak{d}^{-1}_{A/S} = A\theta^{-1}_{A/S}$ and $\mathfrak{d}_{A_+/S} = \theta^{-1}_{A_+/S}A_+$. We may assume that $\theta\theta_{A_+/S} = \theta_{A/S}$ by Proposition 10.3. Define $[x, y] := \mathrm{Tr}_{A/A_+}(\theta^{-1}xy)$, which induces the self A_+-duality on A. If $\theta \in A_+$, we have $\mathrm{Tr}_{A/A_+}(\theta^{-1}xy) = \theta^{-1}\mathrm{Tr}_{A/A_+}(xy)$; so,

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

Thus θ is a unit. The multiplication of θ gives rise to $\mathrm{Isom}_A(A^*, A) \cong \mathrm{Isom}_A(\mathfrak{d}^{-1}_{A/A_+}, A)$.

Suppose $\mathfrak{d}_{A/A_+} \subset \mathfrak{m}_A$. Then θ cannot be a unit. We conclude $\theta \notin A_+$; so, $\mathrm{Isom}_A(A^*, A)^+ = \emptyset$. Thus by Lemma 10.2, $\mathrm{Isom}_A(A^*, A)^- \neq \emptyset$. In other words, writing $f(x)$ for the minimal monic quadratic polynomial of θ in $A_+[x]$, we have $\mathfrak{d}_{A/A_+} = A\delta$ with $\delta = f'(\theta) = \theta - \sigma(\theta)$ (i.e., the multiplication of δ gives rise to an element in $\mathrm{Isom}_A(A^*, A)^-$. Indeed, by the trace pairing $[x, y] = \mathrm{Tr}_{A/A_+}(xy)$, we have the identity $\mathfrak{d}^{-1}_{A/A_+} \cong A^* = A^*_+ \oplus A^*_-$ and $A^*_- \cong A_+\delta^{-1}$ under this isomorphism. Taking the dual under the trace pairing, we get $A_- = (A^*_-)^* = A_+\delta$ and $A = A_+ \oplus A_-$; so, $A_- = A_+\delta$ and $A = A_+ \oplus A_+\delta$, as desired.

Under flatness of A over A_+, plainly by (3), A_- is generated by a single element δ. The assertion is plain in the case where $A_- = A_+\theta$. □

References

Books

[BAL] N. Bourbaki, *Algèbre*, Chapitre 2, Hermann, Paris, 1962.

[CMA] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics, **150**. Springer-Verlag, New York, 1995.

[CPI] K. Iwasawa, *Collected Papers*, I, II, Springer, New York, 2001.

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

[EAI] H. Hida, *Elliptic Curves and Arithmetic Invariants*, Springer Monographs in Mathematics, 2013.

[GME] H. Hida, *Geometric Modular Forms and Elliptic Curves*, second edition, World Scientific, Singapore, 2012.

[HMI] H. Hida, *Hilbert Modular Forms and Iwasawa Theory*, Oxford Mathematical Monographs, Oxford University Press, 2006 (a list of errata posted at `www.math.ucla.edu/~hida`).

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

[KDF] E. Kunz, *Kähler differentials*, Advanced lectures mathematics, Vieweg, 1986, DOI 10.1007/978-3-663-14074-0 (posted at `www.uni-regensburg.de/Fakultaten/nat_Fak_I/kunz/index.html`).

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

[LPL] K. Iwasawa, Lectures on p-adic L-functions, Annals of Math. Studies **74**, Princeton University Press, 1972.

[MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, Cambridge University Press, Cambridge, England, 2000 (a list of errata posted at `www.math.ucla.edu/~hida`).

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

[RDD] R. Hartshorne, *Residues and duality.* Lecture notes of a seminar on the work of A. Grothendieck, given at Harvard 1963/64. With an appendix by P. Deligne. Lecture Notes in Mathematics, No. **20** Springer-Verlag, Berlin-New York 1966.

[RDF] E. Kunz and R. Waldi, *Regular Differential Forms*, Contemporary Math. **79**, AMS, 1988.

[RDP] E. Kunz, *Residues and Duality for Projective Algebraic Varieties*, University Lecture Series **47**, AMS, 2009.

Articles

[CV03] S. Cho and V. Vatsal, Deformations of Induced Galois Representations, J. reine angew. Math. **556** (2003), 79–97.

[DHI98] K. Doi, H. Hida, and H. Ishii, Discriminants of Hecke fields and the twisted adjoint L-values for GL(2), Inventiones Math. **134** (1998), 547–577.

[DFG04] F. Diamond, M. Flach and L. Guo, The Tamagawa number conjecture of adjoint motives of modular forms. Ann. Sci. École Norm. Sup. (4) **37** (2004), 663–727.

[Fu06] K. Fujiwara, Deformation rings and Hecke algebras in totally real case, preprint, 2006 (arXiv.math.NT/0602606)

[H81] H. Hida, Congruences of cusp forms and special values of their zeta functions, Inventiones Math. **63** (1981), 225–261.

[H82] H. Hida, Kummer's criterion for the special values of Hecke L–functions of imaginary quadratic fields and congruences among cusp forms, Inventiones Math. **66** (1982), 415–459.

[H85] H. Hida, Congruences of cusp forms and Hecke algebras, Séminare de Theéorie des Nombres, Paris 1983–84, Progress in Math. **59** (1985), 133–146.

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

[H86b] H. Hida, Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, Inventiones Math. **85** (1986), 545–613.

[H86c] H. Hida, Hecke algebras for GL_1 and GL_2, Sém. de Théorie des Nombres, Paris 1984-85, Progress in Math. **63** (1986), 131–163.

[H88a] H. Hida, A p–adic measure attached to the zeta functions associated with two elliptic modular forms II, Ann. l'institut Fourier **38** (1988), 1–83.

[H88b] H. Hida, Modules of congruence of Hecke algebras and L–functions associated with cusp forms, Amer. J. Math. **110** (1988), 323–382.

[H89] H. Hida, On nearly ordinary Hecke algebras for GL(2) over totally real fields, Adv. Studies in Pure Math. **17** (1989), 139–169.

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

[H06] H. Hida, Anticyclotomic main conjectures, Ducumenta Math. Volume Coates (2006), 465–532.

[H10] H. Hida, The Iwasawa μ–invariant of p–adic Hecke L–functions, Ann. of Math. **172** (2010), 41–137.

[H13] H. Hida, Image of Λ-adic Galois representations modulo p, Inventiones Math. **194** (2013), 1–40.

[H14] H. Hida, Λ-adic Barsotti–Tate groups, Pacific J. Math. **268** (2014), 283–312.

[H15] H. Hida, Big Galois representations and p-adic L-functions, Compositio Math. **151** (2015), 603–664.

[H16] H. Hida, Arithmetic of adjoint L-values, in "p-Adic aspects of modular forms, Chapter 6," Pune IISER conference Proceedings, pp.185–236, 2016.

[HT94] H. Hida and J. Tilouine, On the anticyclotomic main conjecture for CM fields, Inventiones Math. **117** (1994), 89–147.

[Hu89] R. Hübl, On the transitivity of regular differential forms, Manuscripta Math. **65** (1989), 213–224.

[Ka78] N. M. Katz, p-adic L-functions for CM fields, Inventiones Math. **49** (1978), 199–297.

[KhR15] C. Khare and R. Ramakrishna, Lifting torsion Galois representations, Forum of Mathematics, Sigma (2015), **3**, 37 pages doi:10.1017/fms.2015.17

[Kl80] S. L. Kleiman, Relative duality for quasicoherent sheaves, Compositio Math. **41** (1980), 39–60.

[Ku93] M. Kurihara, Ideal class groups of cyclotomic fields and modular forms of level 1. J. Number Theory **45** (1993), 281–294.

[MR70] B. Mazur and L. Roberts, Local Euler characteristics, Invent. Math. **9** (1970), 201–234.

[MT90] B. Mazur and J. Tilouine, Représentations galoisiennes, différentielles de Kähler et "conjectures principales", Publication IHES **71** (1990), 65–103.

[O03] M. Ohta, Congruence modules related to Eisenstein series. Ann. Sci. École Norm. Sup. (4) **36** (2003), 225–269.

[Ru88] K. Rubin, On the main conjecture of Iwasawa theory for imaginary quadratic fields. Invent. Math. **93** (1988), 701–713.

[Ru91] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Inventiones Math. **103** (1991), 25–68.

[TW95] R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke algebras, Ann. of Math. **141** (1995), 553–572.

[T89] J. Tilouine, Sur la conjecture principale anticyclotomique, Duke Math. J. **59** (1989), 629–673.

[Wa15] P. Wake, Eisenstein Hecke algebras and conjectures in Iwasawa theory, Algebra and Number Theory **9** (2015), 53–75.

[WE15] P. Wake and C. Wang-Erickson, Pseudo-modularity and Iwasawa theory, preprint, 2015, arXiv:1505.05128v1 [math.NT].

[Wi95] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. **141** (1995), 443–551.

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