CYCLICITY OF ADJOINT SELMER GROUPS AND FUNDAMENTAL UNITS

HARUZO HIDA

ABSTRACT. Combining an idea of Vatsal–Cho [CV03] with a modified Taylor–Wiles patching argument in [H17], under mild assumptions, we show that for the universal minimal ordinary Galois deformation $\rho_\tau$ of an induced representation $\text{Ind}_F^Q \phi$ from a real quadratic field $F$ with values in $GL_2(\mathbb{Q})$ of a local ring $\mathbb{T}$ of a Hecke algebra, the Pontryagin dual of the adjoint Selmer group of $\rho_\tau$ is canonically isomorphic to $\mathbb{T}/(L)$ for a non-zero divisor $L \in \mathbb{T}$ which is a generator of the different $\mathfrak{d}_{/A}$ of $A$. Moreover, defining $\langle \rho \rangle := (1 + T)^{\log_p(c)/\log_p(1+p)}$ for a fundamental unit $c$ of the real quadratic field $F$, we show following Cho–Vatsal that the Selmer group of $\text{Ind}_F^Q \phi$ for the (minimal) universal character $\phi$ deforming $\phi$ is isomorphic to $\Lambda/(\langle c \rangle - 1)$ as $\Lambda$-modules.

Pick a prime $p > 3$. Let $F = \mathbb{Q}[\sqrt{D}]$ be a real quadratic field with discriminant $D > 0$ and integer ring $O$. Assume that $(p)$ splits into $(p) = p'p''$ in $O$ with $p \neq p'$. In our previous article [H17], we have studied anti-cyclotomic cyclicality of Iwasawa modules over the anticyclotomic $\mathbb{Z}_p$-extension over an imaginary quadratic field. In this paper, combining with an idea of Cho-Vatsal [CV03], we explore what a similar technique produces for a real quadratic field $F$.

Let $\zeta$ be the generator of $\text{Gal}(F/\mathbb{Q})$. Take an anticyclotomic branch character $\phi : \text{Gal}(\overline{\mathbb{Q}}/F) \to \overline{\mathbb{Q}}^\times$. Here $\phi$ “anti-cyclotomic” means that for any lift $\zeta \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with $\zeta|_F = \zeta$, we have $\phi(\zeta \zeta^{-1}) = \phi(\zeta)^{-1}$ for all $\zeta \in \text{Gal}(\overline{\mathbb{Q}}/F)$. Regard it as a finite order idele character $\phi : F_k^\times/F^\times \to \overline{\mathbb{Q}}^\times$ such that $\phi(x') = \phi^{-1}(x)$. Often we find a finite order character $\phi$ of $F_k^\times/F^\times$ such that $\phi = \phi^\prime$, where $\phi^\prime(x) = \phi(x)\phi(x')^{-1}$. Note that $\phi = \phi^\prime \Leftrightarrow \phi|_{k^\times} = 1$. Suppose

(h1) We have $\phi = \phi^\prime$ for a character $\phi$ of order prime to $p$ ramifying at one infinite place of $F$ and of conductor $f$ such that $\phi^\prime|_{\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \neq 1$ and $f|_p$ prime to $p$,
(h2) $N = DN_{F/\mathbb{Q}}(c)$ for an $O$-ideal $c$ prime to $D$ with square-free $N_{F/\mathbb{Q}}(c)$ (so, $N$ is cube-free),
(h3) $p$ is prime to $N \prod_{l \mid N}(l - 1)$ for prime factors $l$ of $N$,
(h4) the character $\phi^\prime$ has order at least $3$,
(h5) the class number of $F$ is prime to $p$,
(h6) the class number of the splitting field $F(\phi^\prime) = \overline{\mathbb{Q}}^{\ker(\phi^\prime)}$ of $\phi^\prime$ is prime to $p$.

We study the local ring of the Hecke algebra associated to $\text{Ind}_F^Q \phi$. We write $Z_p[\phi]$ for the subring of $\overline{\mathbb{Q}}_p$ generated by the values of $\phi$ over $Z_p$. As a base ring, we take $W = Z_p[\phi]$. Put $\Gamma := 1 + pZ_p$ as a $p$-profinite cyclic group. 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 $h$ (over $\Lambda$) of prime-to-$p$ level $N$ and the character $\psi$ whose definition (including its CM components) will be recalled in the following section. We just mention here the following three facts

1. $h$ is a reduced algebra flat over $\Lambda$ interpolating $p$-ordinary Hecke algebras of varying level $Np^{k+1}$, weight $k + 1 \geq 2$ and Neben characters;
2. Each prime $P \in \text{Spec}(h)$ has a unique (continuous) Galois representation $\rho_P : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\kappa(P))$ for the residue field $\kappa(P)$ of $P$;
3. $\rho_P$ restricted to $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ (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 $\overline{\rho} = \rho_{\mathfrak{m}_T} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}})$ for the residue field $\mathbb{F} = \mathbb{T}/\mathfrak{m}_T$. If $\overline{\rho} = \text{Ind}_F^Q \overline{\varphi}$ for the reduction $\overline{\varphi}$ modulo $p$ of $\varphi$, we have an involution

Date: July 16, 2017.
2010 Mathematics Subject Classification. primary 11R23, 11F25, 11F33, 11F80; secondary 11F11, 11G18, 11F27.

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

1
σ ∈ Aut(T/A) such that σ ◦ ρ_p ≃ ρ_p ⊗ χ for χ := (\frac{p}{\mathcal{O}_A}). For a subscheme Spec(A) ⊂ Spec(T) stable under σ, we put A_± := \{x ∈ A|σ(x) = ±x\}. Then A_+ ⊂ A is a subring and A_- is an A_+-module.

We prove

**Theorem A:** Let Spec(T) be a connected component of Spec(h) associated to the induced Galois representation \overline{\varphi} = Ind_{\mathcal{O}_A}^T \varphi for the reduction \varphi modulo m_W of \varphi for the maximal ideal m_W of \varphi. Suppose (h4)–(h6). Then the following two equivalent assertions hold:

1. The rings T and T_+ are both local complete intersections free of finite rank over \Lambda.
2. The T-ideal I = T(σ − 1)T ⊂ T is principal and is generated by a non-zero-divisor θ ∈ T_− = \langle θ^2 \rangle in T_. The element θ generates the T+-module T_− which is free over T_+ and \T = T_+[θ] is free of rank 2 over T_+.

The implication (1) ⇒ (2) follows from [H17, Lemma 10.4], and the converse follows by [H17, Lemma 5.5] from the fact that T/(θ) ∼= T_+/(θ^2) is isomorphic to the group ring W[H] as in Corollary 2.3; so, we do not directly deal with the equivalence of the two assertions in this paper. An assertion slightly weaker that Theorem A is given in [CV03, Theorem 2.1 (2)] in the case where f = 1.

We actually prove a stronger fact than (1) which asserts that T ∼= Λ[[T_-]]/(S_+) and T_+ ∼= Λ[[T^2_+]]/(S_+) for a one variable power series ring Λ[[T_-]] over Λ with S_+ ⊂ Λ[[T^2_+]]. The relative different \mathcal{O}_T/T_{\mathfrak{m}} for T over T_+ (defined in [MR70, Appendix]) is generated by the image \theta of T_- in T. The condition (h4) combined with (p) = pp^x implies an assumption for “R = T^y” theorems of Wiles and Taylor et al [Wi95] and [TW95]:

(W) \overline{\varphi} restricted to Gal(\overline{Q}/M) for M = Q[\sqrt{−1(p−1)/2}]p] is absolutely irreducible, and the main reason for us to assume (h4) is the use of the “R = T^y” theorem for the minimal universal deformation ring R of \overline{\varphi} (see Theorem 2.1). The universal representation ρ_T : Gal(\overline{Q}/Q) → GL_2(R) = GL_2(T) is obtained patching together the representations ρ_p associated to arithmetic primes P ∈ Spec(T). The condition (W) is equivalent to the condition that the representation \overline{\varphi} is not of the form Ind_{\mathcal{O}_A}^{T_{\mathfrak{m}}} ξ for a character ξ : Gal(\overline{Q}/M) → F^× by Frobenius reciprocity. The implication: (h4) ⇒ (W) follows from [H15, Proposition 5.2]. For a deformation ρ : Gal(\overline{Q}/Q) → GL_2(A) of \overline{\varphi}, we let Gal(\overline{Q}/M) act on s_{2,1}(A) by x → ρ(τ)xρ(τ)^{-1} and write this 3-dimensional representation as Ad(ρ).

Under (h5), the universal ring deforming the mod p character \overline{\varphi} requiring deformations to have prime to p-conductor ε is isomorphic to Λ/((ε − 1) for a fundamental unit ε ∈ O^× and ε = (1 + T)^{log_p(ε)/log_p(1+p)} (see [CV03] and Corollary 2.3 in the text).

By a theorem of Mazur, the differential module \Omega_{T/\mathfrak{m}} has a description as (the Pontryagin dual of) an adjoint Selmer group, and by Theorem A, one can prove cyclicity of \Omega_{T/\mathfrak{m}} as T-modules. After stating a cyclicity result on our Selmer group (and \Omega_{T/\mathfrak{m}}), we recall our definition of the Selmer group which could be slightly smaller than the usual Greenberg’s Selmer groups when either \varphi^- is unramified at p or \varphi^- \mid_{Gal(\overline{Q}/\varphi)} has order 2. Since T is shown to be a quotient of Λ[[T_-]] by Theorem A, we obtain a cyclicity result for the adjoint Selmer group:

**Corollary B:** Let the notation and the assumptions be as in Theorem A and as above. Put

ε = \frac{t^{log_p(ε)/log_p(1+p)}}{1 + T} \quad (t = 1 + T ∈ Λ)

for a fundamental unit ε of F. Then we have

1. a canonical isomorphism T/(θ) ∼= (θ)/(θ^2) ∼= Λ/((ε − 1) for θ ∈ T in Theorem A (2),
2. the Pontryagin dual module Sel_Ω(Ad(ρ_T)) of the adjoint Selmer group Sel_Ω(Ad(ρ_T)) is cyclic isomorphic to T/(θ) as T-modules for a non-zero divisor L with (θ) ⊃ (L),
3. The Selmer group Sel_Ω(Ad(Ind_{ind}^T Φ)) of the adjoint Selmer group Sel_Ω(Ad(ρ_T)) has natural surjection of T-modules from Sel_Ω(Ad(ρ_T)).

Moreover we have \mathcal{O}_{T/\Lambda} = (L) for the different \mathcal{O}_{T/\Lambda} relative to the extension T/\Lambda, and the above surjection comes from the natural surjection T/\mathcal{O}_{T/\Lambda} → T/\mathcal{O}_{T/\mathfrak{m}} by the transition formula \mathcal{O}_{T/\Lambda} = \mathcal{O}_{T/\mathfrak{m}} \mathcal{O}_{T+/\Lambda} of different with T/\mathcal{O}_{T/\mathfrak{m}} = T/(θ) ∼= Λ/((ε − 1)).
By the \( R = T \) theorem, \( T \) is the minimal universal deformation ring for \( \text{Ind}_F^Q \overline{\tau} \), and this is equivalent to
\[
\text{Sel}_Q(Ad(\rho_T))^\vee \otimes_T T/(\varnothing) \cong \text{Sel}_Q(Ad(\text{Ind}_F^Q \Phi)) \cong (\varnothing^2) \cong T/(\varnothing) \cong \Lambda/(\varepsilon - 1),
\]
which implies the cyclicity by Nakayama’s lemma. To pin-down the generator of the annihilator of \( \text{Sel}_Q(Ad(\rho_T))^\vee \) in \( T \) as the different \( \varnothing_{\tau/A} \) (which is principal), the theory of dualizing modules of complete intersection rings given by Tate in an appendix to [MR70] plays an important role. Plainly for each irreducible component \( \text{Spec}(I) \), we had given an example of a geometrically irreducible quadratic extension of \( \Lambda \) for the discriminant \( D \) is the Pontryagin dual of \( \vee \). Keeping in mind the fact that the Galois representation \( \rho \) is conjectured in [H98] that \( \text{dim} \text{Res}_F^Q(\rho) \) has to have values in upper triangular matrices under a choice of the basis of \( \text{Ad}(\rho) \) so that \( \rho \) is upper triangular over \( \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \) with quotient character is given by \( \delta \). For a Galois \( A \)-module \( M \), define \( M^* := M \otimes_A A^\vee \) for the Pontryagin dual \( A^\vee \) of \( A \). The Galois group acts on \( M^* \) though the factor \( M \). Define
\[
\text{Sel}(Ad(\rho)) = \text{Ker}(H^1(Q, Ad(\rho)^*)) \to \frac{H^1(Q_p, Ad(\rho)^*)}{F^+ H^1(Q_p, Ad(\rho)^*)} \times \prod_{l|p} H^1(I_l, Ad(\rho)^*),
\]
where \( A^\vee \) is the Pontryagin dual of \( A \) and \( F^+ H^1(Q_p, Ad(\rho)^*) \) is defined as follows. The classes in \( F^+ H^1(Q_p, Ad(\rho)^*) \) come from local cocycles with values in \( F_-(\rho)^* \) whose restriction to \( I_p \) have values in \( F_+(\rho)^* \). Thus we have
\[
F^+ H^1(Q_p, Ad(\rho)^*) = \text{Res}_{D_p/I_p}^{-1}(H^1(I_p, F_+(\rho)^*)) \subset H^1(Q_p, F_-(\rho)^*).
\]
From the cohomology sequence attached to the exact sequence \( F_+(\rho^*) \to Ad(\rho)^* \to Ad(\rho)^*/F_+(\rho)^* \), we can replace \( \frac{H^1(Q_p, Ad(\rho)^*)}{F^+ H^1(Q_p, Ad(\rho)^*)} \) in the above definition of the Selmer group by \( H^1(I_p, \frac{Ad(\rho)^*}{F_+(\rho)^*}) \). Indeed, any global cocycle upper nilpotent with values in \( F_+(\rho)^* \) over \( I_p \) has to have values in upper triangular matrices over \( \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \) as \( \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \) normalizes \( I_p \); so, we have
\[
\text{Sel}(Ad(\rho)) = \text{Ker}(H^1(Q, Ad(\rho)^*)) \to H^1(I_p, \frac{Ad(\rho)^*}{F_+(\rho)^*}) \times \prod_{l|p} H^1(I_l, Ad(\rho)^*).
\]
A close relation of \( T \) and \( \varepsilon \) is conjectured in [H98] that \( \theta = \sqrt{\varepsilon - 1} \), and by Corollary B, we come close to the conjecture under (h1–6). Just before the theory of \( h \) was established in [H86a] and [H86b], we had given an example of a geometrically irreducible quadratic extension of \( \Lambda \) appearing as a quotient of \( h \) (see [H85, (10a,b)]). This example is actually a proto-typical one, and we exhibit infinitely many such examples systematically. The fact 2 \( \text{dim} \text{Frac}(\mathbb{K}) = \text{Frac}(\Lambda) \) for each irreducible component \( \text{Spec}(\mathbb{K}) \) of \( \text{Spec}(T) \) is proven in [BD15], and there is another series of examples of different nature in [Ra14] and [KR15] with degree arbitrarily large over \( \Lambda \). Assuming \( N = D \) for the discriminant \( D \) of the real quadratic field \( F \) and the Gorenstein property for the subring \( \mathbb{T}_+ \) of \( T \), Cho and Vatsal [CV03] proved 2 \( \text{dim} \text{Frac}(\mathbb{K}) \) essentially, after some work by the author [H85] and [H98], though in [CV03], the phenomenon: \( \mathbb{K} \neq \Lambda \) is not much emphasized.

**CONTENTS**

1. Big Hecke algebra 4
2. The \( R = T \) theorem and an involution of \( R \) 7
1. Big Hecke algebra

We briefly recall the theory of $h$. We assume that the starting prime-to-$p$ level $N$ is as in (h2); 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 $F$ is equal to $\mathbb{T}/\mathfrak{m}_\mathbb{T}$ for the maximal ideal of the connected component $\text{Spec} (\mathbb{T})$ (of our interest) in $\text{Spec} (\mathbb{h})$.

We consider the following traditional congruence subgroups

\begin{align}
\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{align}

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 $(p, N, r \geq 0)$, and consider the space of elliptic cusp forms $S_{k+1}(\Gamma_0(Np^r+1), \psi)$ with character $\psi$ as defined in [IAT, (3.5.4)].

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

\begin{align}
\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{align}

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

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

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

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

which is canonically isomorphic to the maximal $p$-abelian quotient of $\Gamma_0(N)/\Gamma_1(N)$ 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 $\Gamma_1(Nq^p) \subset \Gamma_{Q,r} = \Gamma_0(Nq^p)$ for $Nq := N \prod_{q \in Q} q$.

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

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

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

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

Here $h_k(\Gamma_{Q,r}, \psi; W)$ acts on $S_{k+1}(\Gamma_{Q,r}, \psi; W)$ which is the space of cusp forms defined over $W$ (under the rational structure induced from the $q$-expansion at the infinity cusp; see, [MFG, §3.1.8]). More generally for a congruence subgroup $\Gamma$ containing $\Gamma_1(Np^r)$, we write $h_k(\Gamma, \psi; W)$ for the Hecke algebra on $\Gamma$ with coefficients in $W$ acting on $S_{k+1}(\Gamma, \psi; W)$. The algebra $h_k(\Gamma, \psi; W)$ can be also realized as $W[T(n) | n = 1, 2, \ldots] \subset \text{End}_W(S_{k+1}(\Gamma, \psi; W))$. When we need to indicate that our $T(l)$ is the Hecke operator of a prime factor $l$ of $Np^r$, we write it as $U(l)$, since $T(l)$ acting on a subspace $S_{k+1}(\Gamma_0(N'), \psi) \subset S_{k+1}(\Gamma_0(Np^r), \psi)$ of level $N'|Np$ prime to $l$ does not coincide with $U(l)$ on $S_{k+1}(\Gamma_0(Np^r), \psi)$. The ordinary part $h_{Q,k,\psi/W} \subset h_{Q,k,\psi/W}$ is the maximal ring direct summand on which $U(p)$ is invertible. If $Q = \emptyset$, we simply write $h_{k,\psi/W}$ for $h_{k,\psi/W}$. We write $e$ for the idempotent of $h_{Q,k,\psi/W}$, and hence $e = \lim_{n \to \infty} U(p)^n$ under the $p$-adic topology of $h_{Q,k,\psi/W}$. The
idemponent $e$ 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 $S_{k+1}(\Gamma_{Q,r}, \psi, \mu_{p})$ to $S_{k+1}(\Gamma_{Q,r}, \psi, \mathbb{Q})$ and ascends to $S_{k+1}(\Gamma_{Q,r}, \psi)$). We write the image $M_{ord} := e(M)$ of the idemponent attaching the superscript “ord” (e.g., $S_{k+1}^{ord}$).

Fix a character $\psi_{0}$ modulo $Np$, and assume now $\psi_{0}(-1) = -1$. Let $\omega$ be the modulo $p$ Teichmüller character. Recall the multiplicative group $\Gamma := 1 + pZ_{p} \subset Z_{p}^{\times}$ and its topological generator $\gamma = 1 + p$.

Then the Iwasawa algebra $\Lambda = W[[\Gamma]] = \lim_{\leftarrow n} W[\Gamma/\Gamma^{p^{n}}]$ 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 $h^{Q}$ (of level $\Gamma_{Q,\infty}$). We write $h$ for $h^{Q}$.

Since $Np = DN_{F/Q}(\epsilon)p \geq Dp > 4$, the algebra $h^{Q}$ 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) $h^{Q}$ is free of finite rank over $\Lambda$ equipped with $T(n) \in h^{Q}$ 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 $\epsilon : Z_{p}^{\times} \to \mu_{p}$ is a finite order character,

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

for $\psi_{k} := \psi_{0}\omega^{-k}$, sending $T(n)$ to $T(n)$ (and $U(l)$ to $U(l)$ for $l | Np$).

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

**Lemma 1.1.** The Hecke algebra $h^{Q}$ is flat over $\Lambda[\Delta_{Q}]$ with $h^{Q}/\mathfrak{A}_{\Delta_{Q}}h^{Q} \cong h^{Q}$ 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 $k = 0$, abusing the notation, we put $h_{Q,k,\epsilon,\psi_{k}} := h^{Q}/(t - \epsilon(\gamma)\gamma^{k})h^{Q}$ which acts on $p$-ordinary $p$-adic cup forms of weight $k$ and of Neben character $\psi_{k}$. By the above lemma, $h_{Q,k,\epsilon,\psi_{k}}$ is free of finite rank $d$ over $W[\Delta_{Q}]$ whose rank over $W[\Delta_{Q}]$ is equal to rank$_{V} h_{\phi,k,\epsilon,\psi_{k}}$ (independent of $Q$).

Since $N_{Q}$ is cube-free, by [H13, Corollary 1.3], $h^{Q}$ is reduced. Let $\text{Spec}(\mathcal{I})$ be an irreducible component of Spec($h^{Q}$). Write $a(n)$ for the image of $T(n)$ in $\mathcal{I}$ (so, $a(p)$ is the image of $U(p)$).

If a point $P$ of $\text{Spec}(\mathcal{I})(\overline{Q})$ 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 $p^{\epsilon_{P}}(P)$ for the order of $\epsilon_{P}$. If $P$ is arithmetic, by (C2), we have a Hecke eigenform $f_{P} \in S_{k+1}(\Gamma_{Q,r},\epsilon,\psi_{k})$ such that its eigenvalue for $T(n)$ is given by $a_{P}(n) := P(a(n)) \in \overline{Q}$ for all $n$. Thus $I$ gives rise to a family $\mathcal{F} = \{ f_{P}[\text{arithmetic \ } P \in \text{Spec}(\mathcal{I})] \}$ of Hecke eigenforms. We define a $p$-adic analytic family of slope $0$ (with coefficients in $\mathcal{I}$) to be the family as above of Hecke eigenforms associated to an irreducible component Spec($\mathcal{I}$) $\subset$ Spec($h^{Q}$). We call this family slope $0$ because $|a_{P}(p)|_{p} = 1$ for the $p$-adic absolute value $| \cdot |_{p}$ of $\overline{Q}_{p}$ (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 Spec($\mathcal{I}$). Identify Spec($\mathcal{I})(\overline{Q}_{p})$ with $\text{Hom}_{W_{alg}}(\mathcal{I}, \overline{Q}_{p})$, so that each element $a \in \mathcal{I}$ gives rise to a “function” $a : \text{Spec}(\mathcal{I})(\overline{Q}_{p}) \to \overline{Q}_{p}$ whose value at $(P : \mathcal{I} \to \overline{Q}_{p}) \in \text{Spec}(\mathcal{I})(\overline{Q}_{p})$ is $a_{P} := P(a) \in \overline{Q}_{p}$. Then $a$ is an analytic function of the rigid analytic space associated to Spec($\mathcal{I}$). Taking a finite covering Spec($\mathcal{I}$) of Spec($\mathcal{I}$) with surjection Spec($\mathcal{I}$)$(\overline{Q}_{p}) \to$ Spec($\mathcal{I}$)$(\overline{Q}_{p})$, abusing slightly the definition, we may regard the family $\mathcal{F}$ as being indexed by arithmetic points of Spec($\mathcal{I}$)$(\overline{Q}_{p})$, where arithmetic points of Spec($\mathcal{I}$)$(\overline{Q}_{p})$ are made up of the points above arithmetic points of Spec($\mathcal{I}$)$(\overline{Q}_{p})$. The choice of $\mathcal{I}$ is often the normalization of $\mathcal{I}$ or the integral closure of $\mathcal{I}$ in a finite extension of the quotient field of $\mathcal{I}$.

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

$$(\text{Gal}) \quad \text{Tr}(\rho_{\mathcal{I}}(\text{Frob}_{l})) = a(l) \quad (l \nmid Np), \quad \rho_{\mathcal{I}}([\gamma^{s}, Q_{p}]) \sim (t^{s}_{0}1) \quad \text{and} \quad \rho_{\mathcal{I}}([p, Q_{p}]) \sim (a_{\phi(p)}).$$
where \( \gamma^* = (1 + p)^* = \sum_{n=0}^{\infty} (\binom{x}{n}) p^n \in \mathbb{Z}_p^\times \) 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 \( \mathfrak{p}(\text{Frob}_q) \) has two distinct eigenvalues, we have

\[
\rho_l([z, \mathbb{Q}_q]) \sim \begin{pmatrix} \alpha(z) & 0 \\ 0 & \beta(z) \end{pmatrix}
\]

with characters \( \alpha_q \) and \( \beta_q \) of \( \mathbb{Q}_q^\times \) for \( z \in \mathbb{Q}_q^\times \), where one of \( \alpha_q \) and \( \beta_q \) is unramified (e.g., [MFG, Theorem 3.32 (2)] or [HMI, Theorem 3.75]). For each prime ideal \( P \) of \( \text{Spec}(\mathbb{L}) \), writing \( \kappa(P) \) for the residue field of \( P \), we also have a semi-simple Galois representation \( \rho_P : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\kappa(P)) \) unramified outside \( NPP \) such that \( \text{Tr}(\rho_P(\text{Frob}_P)) \) is given by \( a(l)P \) for all primes \( l \mid NqPP \). If \( P \) is the maximal ideal \( \mathfrak{m}_P \) of \( \mathfrak{p}(\text{Frob}_P) \), we write \( \mathfrak{p} \) for \( \rho_P \) which is called the residual representation of \( \rho_P \). The residual representation \( \mathfrak{p} \) is independent of \( \mathfrak{p} \) as long as \( \text{Spec}(\mathbb{L}) \) belongs to a given connected component \( \text{Spec}(\mathbb{T}) \) of \( \text{Spec}(\mathbb{R}) \). Indeed, \( \text{Tr}(\rho_P) \mod \mathfrak{m}_P = \text{Tr}(\mathfrak{p}) \) for any \( P \in \text{Spec}(\mathbb{T}) \). If \( P \) is an arithmetic prime, we have \( \det(\rho_P) = \epsilon_P \psi_k \nu_P \) for the \( p \)-adic cyclotomic character \( \nu_P \) (regarding \( \epsilon_P \) and \( \psi_k \) 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]).

We describe how to construct residue rings of \( \mathfrak{q}^{\infty} \) whose Galois representation is induced from a quadratic field \( F \) (see [LFE, §7.6] and [HMI, §25.4]). Here we allow \( F \) to be imaginary also. We write \( \zeta \) for the generator of \( \text{Gal}(F/\mathbb{Q}) \) as before. Let \( \zeta \) be the prime-to-\( p \) conductor of a character \( \mathfrak{p} \) as in (h1−2). Put \( C = \mathfrak{c} \cap \mathfrak{c}^\vee \). Assume that \( \mathfrak{c} \) is a square free integral ideal of \( F \) with \( \mathfrak{c} \cap \mathfrak{c}^\vee = O \) (i.e., (h2)). Since \( Q \) is outside \( N \), \( Q \) is a finite set of rational primes unramified in \( F/\mathbb{Q} \) prime to \( \mathfrak{p} \). Let \( Q^+ \) be the subset in \( Q \) made up of primes split in \( F \). We choose a prime factor \( \mathfrak{q} \) of \( \mathfrak{q} \) for each \( q \in Q^+ \) (once and for all), and put \( \mathfrak{Q}^+ := \prod_{q \in Q^+} q \). We put \( C_{Q^+} := C \prod_{q \in Q^+} q \). We simply write \( C \) for \( C_{Q^+} \). Consider the ray class group \( \text{Cl}(\mathfrak{a}) \) (of \( F \)) modulo \( \mathfrak{a} \) for an integral ideal \( \mathfrak{a} \) of \( O \), and put

\[
Cl(C_{Q^+}^{\infty}) = \varprojlim r Cl(C_{Q^+}^{r}\mathfrak{p}^r), \quad \text{and } Cl(C_{Q^+}^{\infty}) = \varprojlim r Cl(C_{Q^+}^{r}\mathfrak{p}^r).
\]

On \( Cl(C_{Q^+}^{\infty}) \), the automorphism \( \zeta \) acts as an involution.

**Definition 1.2.** An abelian extension \( K/F \) Galois over \( Q \) is called anticyclotomic if \( \zeta^\tau \zeta^{-1} = \tau^{-1} \) for all \( \tau \in \text{Gal}(K/F) \). 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 \( \mathfrak{c}^{\infty} \prod_{q \in Q^+} q \) for \( C := C \cap \mathfrak{c}^\vee \), and let \( K_Q^\infty \) (resp. \( K_Q^\infty \)) be the maximal \( p \)-abelian anticyclotomic sub-extension of \( K_Q/F \) (resp. the intersection of \( K_Q^\infty \) with the ray class field over \( F \) of conductor \( \mathfrak{c}^{\infty} \prod_{q \in Q^+} q \)). Put \( H_Q = \text{Gal}(K_Q/F) \) and \( C_Q = \text{Gal}(K_Q^{\infty}/F) \). When \( Q \) is empty, we drop the subscript \( Q \) (so, \( H = H_\emptyset \)).

Note here \( H_Q = H_{Q^+} \) by definition and that \( H_Q \) (and hence \( C_Q \)) is a finite group.

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

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

Recall \( p > 3 \); so, the projection \( \pi^- \) induces an isomorphism \( 3_{Q^+}^{1-\infty} = \{\epsilon z^{-1} | z \in 3_{Q^+} \} \to Z_{Q^+}^{-\infty} \). Thus \( \pi^- \) induces an isomorphism between the \( p \)-profinite groups \( Z_{Q^+}^{-\infty} \) and \( 3_{Q^+}^{1-\infty} \). Similarly, \( \pi \) induces \( \pi : 3_{Q^+}^{1-\infty} \cong Z_{Q^+}^{\infty} \). Thus we have for the Galois group \( H_Q \) in Definition 1.2

\[
\iota : Z_{Q^+} \cong Z_{Q^+} \cong H_Q
\]

by first lifting \( z \in Z_{Q^+} \) to \( \tilde{z} \in 3_{Q^+} \) and taking its square root and then project down to \( \pi^- (\tilde{z})^{1/2} = \tilde{z}^{(1-\iota)/2} \). Here the second isomorphism \( Z_{Q^+} \cong H_Q \) is by Artin symbol of class field theory. The isomorphism \( \iota \) identifies the maximal torsion free quotients of the two groups \( Z_{Q^+} \) and \( Z_{Q^+}^{-\infty} \) which we have written as \( \Gamma_- \). This \( \iota \) also induces \( W \)-algebra isomorphism \( W[Z_{Q^+}] \cong W[Z_{Q^+}] \) which is again written by \( \iota \).
Let $\phi$ be the Teichmüller lift of $\overline{\varphi}$ as in Theorem B. Recall that $N = N_{F/Q}(\epsilon)D$. Then we have a unique continuous character $\Phi : \text{Gal}(\overline{Q}/F) \to W[Q_{2}]$ characterized by the following two properties:

1. $\Phi$ is unramified outside $c\Omega^{+}p$,
2. $\Phi(\text{Frob}_{l}) = \varphi(\text{Frob}_{l})[l]$ for each prime $l$ outside $N_{p}$ and $\Omega^{+}$, where $[l]$ is the projection to $\mathbb{Z}$ of the class of $l$ in $\text{Cl}(c\Omega^{+}p^{\infty})$.

The character $\Phi$ is uniquely determined by the above two properties because of Chebotarev density. We can prove the following result in the same manner as in [H86c, Corollary 4.2]:

\textbf{Theorem 1.3.} Suppose that $\overline{\varphi}(\text{Frob}_{q}) \neq \overline{\varphi}(\text{Frob}_{q^{*}})$ for all $q|\Omega^{+}$. Then we have a surjective $\Lambda$-algebra homomorphism $h^{Q_{2}} \to W[Q_{2}]$ such that

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

If $F$ is real, the above homomorphism factors through the weight $1$ Hecke algebra $h^{Q_{2}}/(p^{m} - 1)h^{Q_{2}}$ for a sufficiently large $m \geq 0$.

2. The $R = \mathbb{T}$ theorem and an involution of $R$

In this section, we assume that $F$ is a real quadratic extension over $\mathbb{Q}$ and that the residue field of $W$ is given by $F = \mathbb{T}/m_{\mathbb{T}}$. Let $\mathbb{T}$ be as in Theorem A. We fix a weight $k \geq 0$. Let $\theta(\varphi) \in S_{1}(\mathcal{O}_{N}(N_{p}), \psi)$ for the corresponding theta series (see [HMI, Theorem 2.7]). Then $\psi = \psi_{0}$, where we define $\psi_{k}$ to be given by $\psi_{k} = \chi \varphi |_{\mathbb{A}^{2}} \omega^{-k}$ for the Teichmüller character. Recall the identity $\psi_{k} \equiv \nu_{p} \mod m_{W}$ for the $p$-adic cyclotomic character $\nu_{p}$; so, $\psi_{0}$ is the Teichmüller lift of $\nu_{p}$. By the existence of a lift of Hasse invariant, we can find a Hecke eigenform $f \in S_{k+1}(\mathcal{O}_{N}(N_{p}), \psi_{k})$ congruent to $\theta(\varphi)$ modulo $p$, and hence the Hecke algebra $\mathcal{T}\overline{\mathbb{T}} = \mathcal{T}/(t - \gamma^{k})\mathcal{T}$ (resp. $\mathcal{T}^{Q}/(t - \gamma^{k})\mathcal{T}^{Q}$) is a local ring of $h_{0,k,\psi_{k}}$ (resp. $h_{Q,k,\psi_{k}}$).

Writing $c$ for the prime-to-$p$ conductor of $\overline{\varphi}$, by (h2), $N_{F/Q}(\epsilon)D = N$ for the discriminant $D$ of $F$ (cf. [GME, Theorem 5.1.9]). By (h2), the conductor $c$ is square-free and only divisible by split primes in $F/Q$. Since $\overline{\varphi} = \text{Ind}_{F}^{Q} \varphi$, for $l|N$, the prime $l$ either splits in $F$ or ramifies in $F$. Write $l$ for the prime factor of $(l)$ in $F$. If $(l)$ splits into $\mathfrak{l}$, we may assume that the character $\overline{\varphi}$ ramifies at $\mathfrak{l}$ and is unramified at $\mathfrak{l}$, and hence $\overline{\varphi}(\text{Gal}(Q_{N}/Q_{l})) \cong \mathcal{T}\overline{\mathbb{T}} / \mathcal{T}\overline{\mathbb{T}}$. If $(l) = l^{2}$ ramifies in $F$, we have $\overline{\varphi}|_{I_{l}} \cong 1 + \overline{\mathfrak{x}}$ with $\overline{\mathfrak{x}} = (\chi \mod p)$ for the quadratic character $\chi = \left(\frac{F}{Q_{N}}\right)$. Here $I_{l}$ is the inertia subgroup of $\text{Gal}(Q_{N}/Q)$.

Write $CL_{W}$ for the category of $p$-profinite local $W$-algebras with residue field $F := W/m_{W}$ whose morphisms are local $W$-algebra homomorphisms. Let $Q_{N}(N_{p}) \subset Q_{N}$ be the maximal extension of $Q_{N}$ unramified outside $N_{p}\mathbb{C}$. Consider the following deformation functor $D : CL_{W} \to \text{SETS}$ given by

$$D(A) = D^{\theta}(A) := \{\rho : \text{Gal}(Q_{N}(N_{p})/Q) \to \text{GL}_{2}(A) : \text{a representation satisfying } (D1-4)\}/
\cong .$$

Here are the conditions (D1–4):

(D1) $\rho \mod m_{A} \cong \overline{\varphi}$ (i.e., there exists $a \in \text{GL}_{2}(F)$ such that $a\overline{\varphi}(\sigma)a^{-1} = (\rho \mod m_{A})$ for all $\sigma \in \text{Gal}(Q/F)$).

(D2) $\rho|_{\text{Gal}(Q_{N}(N_{p})/Q)} \cong (\overline{\varphi}^{\delta})$ with $\delta$ unramified and $\delta(p, Q_{p}) \equiv \varphi_{p}(\nu_{p}, Q_{p}) \mod m_{A}$.

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

(D4) $\det(\rho)|_{I_{p}} \equiv \psi|_{I_{p}} \mod m_{A}$ (which is equivalent to $\epsilon_{I_{p}} \equiv \psi|_{I_{p}} \mod m_{A}$).

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

$$D^{Q}(A) := \{\rho : \text{Gal}(Q_{N}(Q_{N_{p}})/Q) \to \text{GL}_{2}(A) : \text{a representation satisfying } (D1-4) \text{ and } (UQ)\}/
\cong ,$$

where

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

We may also impose another condition if necessary:

\[(\text{det}) \det(\rho) = \iota_A \circ \nu_p^k \psi_k \text{ for the } p\text{-adic cyclotomic character } \nu_p,\]

and consider the functor

\[D_{Q,k,\psi_k}(A) := \{\rho : \text{Gal}(Q^{(Q_N^p)}/Q) \to \text{GL}_2(A) : \text{a representation satisfying (D1–4) and (det)}/\cong \}.\]

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 \(\psi_k\); strictly speaking, if \(k = 0\), we allow non-classical \(p\)-adic cusp forms. We often write simply \(D_{k,\psi_k}\) for \(D_{\emptyset,k,\psi_k}\) when \(Q\) is empty. For each prime \(q\), we write \(D^q_{Q,k,\psi_k}\) for the deformation functor of \(\overline{\rho}\) being a representation satisfying the local condition (D2–4) which applies to \(q\).

By our choice of \(\overline{\rho} = \text{Ind}^Q_F \overline{\gamma}\), we have \(\overline{\rho}|_{\text{Gal}(\overline{\mathbb{Q}}_l/Q)} \cong \left( \begin{array}{cc} \tau_q & 0 \\ 0 & \tau_q \end{array} \right)\) for two local characters \(\tau_q, \overline{\tau}_q\) for all primes \(q|Qp\). If \(\delta_q \neq \tau_q\) and \(\tau_q(\text{Frob}_q) \neq \overline{\tau}_q(\text{Frob}_q)\) for all \(q \in Q, D, D^Q, D_{k,\psi_k}\) and \(D_{Q,k,\psi_k}\) are representable by universal objects \((R, \rho) = (R^\theta, \rho^\theta), (R^Q, \rho^Q), (R_0, \rho_0)\) and \((R_Q, \rho_Q)\), respectively (see [MFG, Proposition 3.30] or [HMI, Theorem 1.46 and page 186]).

Here is a brief outline of how to show the representability of \(D\). It is easy to check the deformation functor \(D^{ord}\) only imposing (D1–2) is representable by a \(W\)-algebra \(R^{ord}\) . The condition (D4) is actually redundant as it follows from the universality of the Teichm"uller lift and the conditions (D1–2). Since \(N\) is the prime-to-\(p\) conductor of \(\det(\rho)\) (h1–2) and \(p\) is unramified in \(F/Q\), if \(l\) is a prime factor of \(N\), writing \(\rho|_{I_l}\) for its semi-simplification of \(\rho\) over \(I_l\), we see from (h3) that \(\rho|_{I_l}^{\sigma_p} = \epsilon_l \oplus \delta_l\) for two characters \(\epsilon_l\) and \(\delta_l\) (of order prime to \(p\)) with \(\delta_l\) unramified and \(\epsilon_l \equiv \psi|_{I_l} \mod m_A\). Thus by the character \(\iota_{N} := \prod_{l|N} \epsilon_l\) 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 \(R = R^{ord} \otimes W[I_N] \psi_{1,N} W\), where the tensor product is taken over the algebra homomorphism \(W[I_N] \rightarrow W\) induced by the character \(\psi_{1,N}\). Since \(\overline{\rho}\) is an induced representation, \(\overline{\rho}|_{I_l}\) is semi-simple and \(\overline{\rho}|_{I_l} = \tau_l \oplus \delta_l\). Similarly one can show the representability of \(D^Q\) and \(D_{Q,k,\psi_k}\).

Let \(\mathcal{T}\) be the local ring of \(h = h^\theta\) as in Theorem B whose residual representation is \(\overline{\rho} = \text{Ind}^Q_F \overline{\gamma}\). The ring \(\mathcal{T}\) is uniquely determined by (h1–3), as the unramified quotient of \(\overline{\rho}\) at each \(l|N\) is unique. At \(p\), to have a universal ring and to have uniquely defined \(\mathcal{T}\), we need to specify in the deformation problem the unramified quotient character and for \(\mathcal{T}\), the residue class of \(U(p)\)-eigenvalue given by \(\overline{\rho}^{(p^s)}\). The unramified quotient is unique if \(\varphi\) ramifies at \(p\). However if \(\varphi\) is unramified at \(p\), we need to fix the residue class of \(U(p)\) as above because of the existence of companion forms.

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

**Theorem 2.1.** Assume (h1–4). Then the morphism \(\pi : R \rightarrow \mathcal{T}\) is an isomorphism, and \(\mathcal{T}\) is a local complete intersection over \(\Lambda\).

See [Wi95, Theorem 3.3] and [DFG04] for a proof (see also [HMI, §3.2] or [MFG, Theorem 3.31] for details of how to lift the results in [Wi95] to the (bigger) ordinary deformation ring with varying determinant character). These references require the assumption (W) which is absolute irreducibility of \(\overline{\rho}|_{\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}\) for \(M = \mathbb{Q}[\sqrt{p^s}]\) with \(p^s := (-1)^{(p-1)/2}.p\). To eliminate the assumption (h3), 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 \(R = \mathcal{T}\) (or work with \(\Gamma_l\)-level Hecke algebra), which not only complicates the setting but also the identification of \(\mathcal{T}/I \cong W[H]\) (for \(I = \mathcal{T}(\sigma - 1)\mathcal{T}\) as in Theorem A) could fail if (h3) fails (so, we always assume (h3); see Lemma 2.2).

We will recall the proof of Theorem 2.1 in the following Section 3 to good extent in order to facilitate a base for a finer version (in Section 6) of the patching argument by Taylor–Wiles we study there.
Since $\overline{\pi} = \operatorname{Ind}_F^G(\overline{\chi})$, for $\chi = \left( \frac{E}{Q} \right)$, $\overline{\pi} \otimes \overline{\chi} \cong \overline{\pi}$. By assumption, $p$ splits in $F$; so, $\chi$ is trivial on $\operatorname{Gal}(\overline{\mathbb{Q}}_{l}/\mathbb{Q})$ for prime factors $l$ of $pN_F/Q(c)$ and ramified quadratic on $\operatorname{Gal}(\overline{\mathbb{Q}}_{l}/\mathbb{Q})$ for $l|D$. Thus $\rho \mapsto \rho \otimes \chi$ is an automorphism of the functor $D^Q$ and $D_{Q,k,\psi_\chi}$, and $\rho \mapsto \rho \otimes \chi$ induces automorphisms $\sigma_Q$ of $R_Q$ and $R^Q$. We identify $R$ and $T$ now by Theorem 2.1; in particular, we have an automorphism $\sigma = \sigma_0 \in \operatorname{Aut}(T)$ as above.

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

We now study the closed subscheme $\operatorname{Spec}(T)^G$ fixed by $G := \langle \sigma \rangle \subset \operatorname{Aut}(T/A)$. Consider the functor $D_F, D^G_F : \text{CL}_W \rightarrow \text{SETS}$ defined by

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

and

$$D^G_F(A) = \{\lambda : \operatorname{Gal}(\overline{\mathbb{Q}}/F) \rightarrow A^\times|\lambda \equiv \overline{\pi} \mod m_A \text{ has conductor a factor of } cp^\infty\}.$$ Let $F_{cp}$ be the maximal abelian $p$-extension of $F$ inside the ray class field of conductor $cp$. Put $C = C_0 := \operatorname{Gal}(F_{cp}/F)$. Similarly, write $F_{cp}^\infty$ for the maximal $p$-abelian extension inside the ray class field $F \otimes \mathbb{Q}_{p}$ of $F$. Put $H := \operatorname{Gal}(F_{cp}^\infty/F)$. Note that $F_{cp}^\infty/F$ is a finite extension as $F$ is real. Then $D_F$ is represented by $(W[C], \Phi)$ where $\Phi(x) = \varphi(x)x$ for $x \in C$, where $\varphi$ is the Teichmüller lift of $\overline{\chi}$ with values in $W^\times$. Similarly $D^G_F$ is represented by $W[H]$.

In Definition 2.2, we defined $H$ as the anticyclotomic $p$-primary part $\operatorname{Gal}(K^{-1}/F)$ of the Galois group of the ray class field $K$ of conductor $(c \cap \mathfrak{c})^p\mathfrak{c}$. The present definition is a bit different from the one given there. However, the present $H$ is isomorphic to the earlier $\operatorname{Gal}(K^{-1}/F)$ by sending $\tau$ to $\tau^{(1-\chi)/2} = \sqrt{\tau \zeta_{CT^{-1}}e^{-T}}$ (see (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]:

**Lemma 2.2.** Assume (h1–4) and $p > 3$. Then the natural transformation $\lambda \mapsto \operatorname{Ind}_{F_{cp}}^F \lambda$ induces an isomorphism $D_F \cong D^G_F$ and $D^G_F \cong D^G$, where

$$D^G_F(A) = \{\rho \in D(A)|\rho \otimes \chi \cong \rho\} \text{ and } D^G_F(A) = \{\rho \in D^G(A)|(C(\det \rho)) \cap (Np)\}$$

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 $D^G_F \cong D^G$. By [DH98, Lemma 3.2], we have $\rho \otimes \chi \cong \rho$ for $\rho \in D(A)$ is equivalent to having $\lambda : \operatorname{Gal}(\overline{\mathbb{Q}}/F) \rightarrow A^\times$ such that $\rho \cong \operatorname{Ind}_{F_{cp}}^F \lambda$. We can choose $\lambda$ so that $\lambda$ has conductor a factor of $cp^\infty$ by (D4) and $C(\det \rho)|Np^\infty$. Then $\lambda$ is unique by (D2–3) and (h3). Thus we get the desired isomorphism. \(\square\)

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

**Corollary 2.3.** Assume (h1–4). Then we have $T/I \otimes \Lambda/(T) \cong W[C]$ and $T/I \cong W[H]$ canonically. If further $p \nmid h_F$ (h5), we have $W[C] = \Lambda/(\langle \zeta \rangle - 1)$.

In the proof of Theorem 2.1, Taylor and Wile considered an infinite sets $Q$ made up of finite sets $Q$ of primes $q \equiv 1 \mod p$ outside $Np$ such that $\overline{\pi}(\text{Frob}_q) \sim \left( \begin{array}{c} \pi \alpha_0 \pi_q \end{array} \right)$ with $\overline{\pi}_q \neq \overline{\pi}_q \in \mathfrak{p}$. Over the inertia group $I_q$, $\rho^Q$ has the following shape by a theorem of Faltings

$$\rho^Q/I_q = \left( \begin{array}{c} \delta_q \alpha_0 \delta_q \end{array} \right)$$

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

We can choose infinitely many distinct $Q$s with $\overline{\pi}(\text{Frob}_q)$ 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 $\overline{\pi}_q$ of $\overline{\pi}(\text{Frob}_q)$ for each $q \in Q$, we have a unique Hecke algebra local factor $\mathbb{T}_Q$ of the Hecke algebra $h_{Q,k,\psi_q}$, whose
residual representation is isomorphic to $\overline{\eta}$ and $U(q) \mod m_\eta$ is the chosen eigenvalue $\overline{\eta}$. This follows in the following way: We choose $\overline{\eta}$ for $q \in Q^-$. For $q \in Q^+$, we choose a unique prime factor $q'|q$ so that $\overline{\eta}(Frob_{q'}) = \overline{\eta}$. In this way, we get a local factor $T^Q$ of $h^Q$ which covers the local ring $W[Z_Q]$ as in [H17, Corollary 1.3].

Define

$$T_Q = T^Q/(t - \gamma^k)T^Q$$

which is a local factor of $h_{Q,k,\psi_k}$ as in (C1) in Section 1 with the prescribed mod $p$ eigenvalues of $U(q)$ for $q \in Q$.

By absolute irreducibility of $\overline{\eta}$, the theory of pseudo representation tells us that the Galois representation $\rho_{\overline{\eta}}$ in Section 1 can be arranged to have values in $GL_1(T^Q)$ (e.g., [MFG, Proposition 2.16]). The isomorphism class of $\rho_{\overline{\eta}}$ as representation into $GL_1(T^Q)$ is unique by a theorem of Carayol–Serre [MFG, Proposition 2.13], as $\text{Tr}(\rho_{\overline{\eta}}(Frob_1))$ is given by the image of $T(1)$ in $T^Q$ for all primes $l$ outside $N_Qp$ by (Gal) in Section 1 (and by Chebotarev density theorem). We need to twist $\rho_{\overline{\eta}}$ slightly by a character $\delta$ to have $\rho_{\overline{\eta}} \otimes \delta$ satisfy (UQ). This twisting is done in the following way:

By $(\text{Gal}_q)$, write $\rho_{\overline{\eta}} \sim \left( \begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix} \right)$ as a representation of the inertia group $I_q$ for $q \in Q$. Then $\epsilon_q \equiv 1 \mod m_\eta$ as $\overline{\eta}$ is unramified at $q$. Thus $\epsilon_q$ has a $p$-power order factoring through the maximal $p$-abelian quotient $\Delta_q$ of $\overline{\eta}$; so, it has a unique square root $\sqrt{\epsilon_q}$ with $\sqrt{\epsilon_q} \equiv 1 \mod m_\eta$. Since $\Delta_q$ is a unique quotient of $(\mathbb{Z}/q\mathbb{Z})^\times = Gal(Q(\mu_q)/Q)$, we can lift $\sqrt{\epsilon_q}$ to a unique global character of $Gal(Q(\mu_q)/Q)$. Write $\sqrt{\epsilon} := \prod_{q \in Q} \sqrt{\epsilon_q}$ as a character of $Gal(Q(\mu_q)_{q \in Q}/Q) \cong \prod_{q \in Q} (\mathbb{Z}/q\mathbb{Z})^\times$. Then we define

$$(2.2) \quad \rho^Q := \rho_{\overline{\eta}} \otimes \sqrt{\epsilon}^{-1}.$$ 

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

By local class field theory, we identify $\Delta_q$ with the $p$-Sylow subgroup of $\mathbb{Z}_q^\times$. Define $\Delta_Q := \prod_{q \in Q} \Delta_q$. By Lemma 1.1, the inertia action $I_q \rightarrow R^Q \rightarrow T^Q$ makes $T^Q$ free (of finite rank) over $W[\Delta_Q]$, and hence $\Delta_Q \rightarrow R^Q$ and $\Delta_Q \rightarrow T^Q$. The character $\delta_q : I_q \rightarrow (R^Q)^\times$ (resp. $\delta_q^{-1} : I_q \rightarrow (R^Q)^\times$) extends uniquely to $\delta_q : Gal(T_q/Q) \rightarrow R^Q$ (resp. $\delta_q^{-1} : Gal(T_q/Q) \rightarrow R^Q$) so that

$$(2.3) \quad \rho^Q|_{Gal(T_q/Q)} = \begin{pmatrix} \delta_q & 0 \\ 0 & \delta_q^{-1} \end{pmatrix}$$

with $\delta_q(\phi_q) \mod m_{R^Q} = \overline{\eta}$ (resp. $\delta_q^{-1}(\phi_q) \mod m_{R^Q} = \overline{\eta}$) for any $\phi_q \in Gal(T_q/Q)$ with $\phi_q \mod I_q = Frob_q$ (e.g., [MFG, Theorem 3.32] or [HMI, Theorem 3.75]).

We choose $q|q$ for $q \in Q^+$ so that $\overline{\eta}(Frob_q) = \overline{\eta}$, and define $\Omega_+$ by the product over $q \in Q^+$ of $q$ thus chosen. Define the functor $D^\infty_{F,Q} : CLW \rightarrow SETS$ by

$$D^\infty_{F,Q}(A) = \{ \lambda : Gal(T/F) \rightarrow A^\times ; \lambda \equiv \overline{\eta} \mod m_A \text{ has a conductor a factor of } \Omega_+ \phi^{\infty} \}.$$ 

Hereafter we simply write $Z_Q$ for $Z_{Q^+}$. Then plainly $D^\infty_{F,Q}$ is representable by $W[Z_Q] \cong W[H_Q]$. Here is a generalization of Corollary 2.3:

**Proposition 2.4.** Assume (h1–4). Let $I^Q = R^Q(\sigma_Q - 1)R^Q$. Then we have

$$R^Q/I^Q \cong W[H_Q] \quad \text{and} \quad R^Q/I^Q \otimes_A \Lambda(\tau) \cong W[C_Q]$$

for $C_Q$ as in Definition 1.2.

**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 $\text{Spec}(A)$ over a base ring $B$, the functor $\text{Spec}(A)^G : C \mapsto \text{Spec}(A)(C)^G = \text{Hom}_{B-\text{alg}}(A,C)^G$ sending $B$-algebras $C$ to the set of fixed points is a closed subscheme of $\text{Spec}(A)$ represented by $A_G := A/\sum_{g \in G} A(g-1)A$; i.e., $\text{Spec}(A)^G = \text{Spec}(A_G)$. Thus we need to prove that the natural transformation $\lambda \mapsto \text{Ind}_C^A \lambda$ induces an isomorphism $D^\infty_{F,Q} \cong (D^Q)^\delta$, where $(D^Q)^\delta(A) = \{ \rho \in D^Q(A) | \rho \otimes \chi \equiv \rho \}$. If $\rho \in D^Q(A)$, we have a unique algebra homomorphism $\phi : R^Q \rightarrow A$ such that $\rho \cong \phi \circ \rho^Q$ and $\rho|_{I_q} \cong \left( \begin{smallmatrix} \phi \delta|_{I_q} & 0 \\ 0 & (\phi \delta|_{I_q})^{-1} \end{smallmatrix} \right)$. This implies $\rho \otimes (\phi \circ \delta)|_{I_q} \cong \left( \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)$ for the global character $\delta : Gal(Q(\mu_q)_{q \in Q}/Q) \rightarrow (R^Q)^\times$, and hence its prime-to-$p$ conductor is a factor of $N_Q$. On the other hand, for $\rho = \text{Ind}_C^A \lambda$ in $D^Q(A)$, if $\rho$ ramifies at $q \in Q^-$, the $q$-conductor of $\rho \otimes (\phi \circ \delta)$ is $N_{F/Q}(q) = q^2$, a contradiction as $q^2 \nmid N_Q$. Thus $\lambda$ is
unramified at $q \in Q^-$, and we may assume $\lambda \in D^*_{F,Q}(A)$. Indeed, among $\lambda, \lambda_e$ for $\lambda_e(\sigma) = \lambda(\sigma^e - 1)$, we can characterize $\lambda$ uniquely (by (h3)) so that $\lambda \mod \mathfrak{p} = \mathfrak{p}$. Thus $D^*_{F,Q}(A) \to (D^Q)^G(A)$ is an injection. Surjectivity follows from [DHI98, Lemma 3.2].

3. The Taylor–Wiles system

In their proof of Theorem 2.1, Taylor and Wiles used an infinite family $Q$ of finite sets $Q$ made of primes $q \equiv 1 \mod p$ outside $N$. We can choose infinitely many distinct $Q$s with $\mathfrak{p}((\text{Frob}_q))$ for $q \in Q$ having two distinct eigenvalues. Recall $\chi = \left(\frac{F}{q}\right)$ and $\mathfrak{p} = \text{Ind}_F^Q \mathfrak{p}$ for real quadratic $F$ as in Theorem A. We split $Q = Q\uparrow \sqcup Q\downarrow$ so that $\mathfrak{p} = \{ q \in Q | \chi(q) = \pm 1 \}$. By fixing a weight $k > 0$ and choosing an eigenvalue $\tau_q$ of $\mathfrak{p}(\text{Frob}_q)$ for each $q \in Q$, we have a unique local factor $T Q$ (resp. $T Q$) of the Hecke algebra $HQ$ (resp. $HQ, k, x^e$) as in [H17, (1.7)], whose residual representation is isomorphic to $\mathfrak{p}$ and $U(q)$ ($\mod \mathfrak{m} Q$) is the chosen eigenvalue $\tau_q$.

To describe the Taylor–Wiles system used in the proof of Theorem 2.1 (with an improvement due to Diamond and Fujiwara), we need one more information of a $T Q$-module $M Q$ in the definition of the Taylor–Wiles system in [HMI, §3.2.3] and [MFG, §3.2.6]. Here we choose $M Q := T Q$ which is the choice made in [MFG, §3.2.7] (and [HMI, page 198]).

The Hecke algebra $h_k(\Gamma Q, \psi; W)$ has an involution coming from the action of the normalizer of $\Gamma Q$. Taking $\gamma \in SL_2(\mathbb{Z})$ such that $\gamma \equiv \left(\begin{smallmatrix} 1 & 0 \\ q & 1 \end{smallmatrix}\right) \mod D^2$ and $\gamma \equiv 1 \mod (N Q/D)^2$, put $\eta := \gamma(\frac{D}{q})$. Then $\eta$ normalizes $\Gamma Q$, and the action of $\eta$ satisfies $\eta^2 = 1, \eta U(l)\eta^{-1} = \chi(l)U(l)$ for each prime $l \mid N Q/D$ and $\eta T(l)\eta^{-1} = \chi(l)T(l)$ for each prime $l \not\mid N Q$ (see [FMF, (4.6.22), page 168]). Thus the conjugation of $\eta$ induces an involution on $T Q$ compatible with $\mathfrak{p} Q$ under the canonical surjection $R Q \to T Q$. Note that $\mathfrak{p} Q(U(\eta)) = -U(\eta)$ for $q \in Q^-$; so, the role of $\tau_q$ will be played by $-\tau_q = \beta q$. This affects on the inertia action of $\Delta_q$ at $q$ by $\delta q \to \delta q 1 - 1$ for $q \in Q^-$, because the action is normalized by the choice of $\tau_q$ with $\tau_q := U(q) \mod \mathfrak{m} Q$ (see Lemma 3.1 and [HMI, Theorem 3.7.4]). Since $T Q$ is the local component of the big Hecke algebra of tame level $\Gamma Q$ whose reduction modulo $t - \gamma$ is $T Q$, again $T Q$ has involution $\mathfrak{p} Q$ induced from $\eta$. We write $T Q$ (resp. $T Q$) for the fixed subring of $T Q$ (resp. $T Q$) under the involution.

Since we follow the method of Taylor–Wiles for studying the local complete intersection property of $R_+ \cong T_+$, we recall here the Taylor–Wiles system argument (which proves Theorem 2.1) formulated by Fujiwara [Fu6] (see also [HMI, §3.2.3]). Identify the image of the inertia group $\iota_q$ for $q \in Q$ in the Galois group of the maximal abelian extension over $Q_q$ with $\mathbb{Z}^\infty_q$ by the $q$-adic cyclotomic character. Let $\Delta_q$ be the $p$-Sylow subgroup of $\mathbb{Z}^\infty_q$, and put $\Delta_q := \prod_{q \in Q} \Delta_q$ as in (1.4). If $q \equiv 1 \mod p^m$, for $m > 0$ for all $q \in Q$, $\Delta_q/\Delta_q^{p^m}$ for $0 < n \leq m$ is a cyclic group of order $p^n$. We put $\Delta_n = \Delta_n Q := \prod_{q \in Q} \Delta_q/\Delta_q^{p^n}$. By Lemma 1.1, the inertia action $I_q \to \mathbb{Z}^\infty_q \to R Q \to T Q$ makes $T Q$ free of finite rank over $W[\Delta Q]$. Then they found an infinite sequence $Q = \{ Q_m | m = 1, 2, \ldots \}$ of ordered finite sets $Q = Q_m$ of primes $q$ (with $q \equiv 1 \mod p^m$) which produces a projective system:

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

made of the following objects:

1. $R_{n,m} := T_{Q_m}/(p^n, \delta_q^{p^n} - 1/q \in Q_m \mathfrak{R}_{Q_m}$ 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 $T_{Q_m}$ in $\text{End}_{W[\Delta_n]}(M_{n,m})$ for $M_{n,m} := M_{Q_m}/(p^n, \delta_q^{p^n} - 1/q \in Q_m \mathfrak{R}_{Q_m}$, but by our choice $M_Q = T_Q$, the image is identical to $T_{Q_m}/(p^n, \delta_q^{p^n} - 1/q \in Q_m \mathfrak{R}_{Q_m}$.

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

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

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

Thus for each $n > 0$, the projection $\pi_n^{n+1} : R_{n+1,m(n+1)} \to R_{n,m}$ is compatible with all the data in the system (3.1) (the meaning of this compatibility is specified below) and induces the
projection \( \tilde{\pi}^{n+1}_n : \tilde{R}_{n+1,m(n+1)} \to \tilde{R}_{n,m(n)} \). In [HMI, page 191], there is one more datum of an algebra homomorphism \( \beta : R_{n,m} \to \operatorname{End}_\mathbb{Q}(M_{n,m}) \subset \operatorname{End}_{W[\Delta_0]}(M_{n,m}) \). Since we have chosen \( M_Q \) to be \( \mathbb{T}_Q \), \( M_{n,m} \) is by definition \( R_{n,m} \); so \( \beta \) is just the identity map (and hence we forget about it).

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

(Q2) \( q \equiv 1 \mod p^m \) and \( \mathfrak{p}(\text{Frob}_q) \sim \left( \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right) \) with \( \mathfrak{p}_q \neq \overline{\mathfrak{p}}_q \in \mathbb{F} \) if \( q \in Q_m \) (so, \( |\Delta_q| = : p^e_q \geq p^m \)).

Actually as we will see later in Lemma 4.1, we can impose a slightly stronger condition: \( q \equiv 1 \mod Cp^m \) for \( C = N_{F'/\mathbb{Q}}(\epsilon) \).

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

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

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

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

(Q4) There exists an ordered set of generators \( \{ f_1^{(n)}, \ldots, f^{(n)}_r \} \subset 
\mathfrak{m}_{R_{n,m(n)}} \) of \( R_{n,m(n)} \) over \( W \) for the integer \( r \) in (Q1) such that \( \pi_{n}^{(j)} = (f_1^{(n+1)} - f_1^{(n)}) = f_1^{(n)} \) for each \( j = 1, 2, \ldots, r \).

(Q5) \( R_\infty := \lim_n R_{n,m(n)} \) is isomorphic to \( W[[T_1, \ldots, T_r]] \) by sending \( T_j \) to \( f_j^{(\infty)} := \lim_n f_1^{(n)} \) for each \( j \) (e.g., [HMI, page 193]).

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

(Q7) \( R_\infty/(S_1, \ldots, S_r) \cong \lim_n \tilde{R}_{n,m(n)} \cong R_0 \cong \mathbb{T}_0 \), where \( R_0 \) is the universal deformation ring for the deformation functor \( D_{\mathfrak{m}_0,k,\psi_0} \) and \( \mathbb{T}_0 \) is the local factor of the Hecke algebra \( \mathfrak{h}_{0,k,\psi_0} \) whose residual representation is isomorphic to \( \overline{\mathfrak{p}} \).

(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 \( \mathfrak{A}_{Q_m} := ((1 + S_j) / \Delta_{q_j}^{(n)} - 1)_{j = 1, 2, \ldots, r} \) 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 \( \chi := \left( \begin{array}{cc} F & Q \\ 0 & 0 \end{array} \right) \) as before. Then the involution \( \sigma_{Q_m} \) on \( \mathbb{T}_{Q_m} \) acts on \( \delta_{q_j}|_{I_q} \) (the image of \( s_q = 1 + S_q \) for \( q \in Q_m \) by \( \sigma_{Q_m} \mid_{I_q} = (\delta_{q_j}|_{I_q})^{\chi(q)} \). In particular, the ideal \( p^n, \delta_{q_j} - 1 \in Q_m \) of \( \mathbb{T}_{Q_m} \) is stable under \( \chi_{Q_m} \), and the involution \( \sigma_{Q_m} \) induces an involution \( \sigma = \sigma_{s_q} \) of \( R_n = R_{n,m} \).

**Proof.** For each \( q \in Q \), by (2.1), the restriction of \( \mathfrak{p}^Q \) to the inertia group \( I_q \subset \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) has the form \( \left( \begin{array}{cc} \delta_q & 0 \\ 0 & \delta_q^{-1} \end{array} \right) \) and the choice of the eigenvalue \( \overline{\mathfrak{p}}_q \) determines the character \( \delta_q \) (i.e., \( \overline{\mathfrak{p}}_q \)-eigenspace of \( \mathfrak{p}(\text{Frob}_q) \) is the image of \( \delta_q^{-1} \)-eigenspace in \( \overline{\mathfrak{p}} \) by (2.3); see also [MFG, Theorem 3.32 and its proof] or [HMI, Theorem 3.75]). By tensoring \( \chi, \overline{\mathfrak{p}}_q \) is transformed to \( \chi(q) \overline{\mathfrak{p}}_q = \overline{\mathfrak{p}}_q \), and hence \( \delta_q \) will be transformed to \( \delta_q^{\chi(q)} \) under \( \sigma_{Q_m} \). 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 \( (p^n, \delta_q^{p^n} - 1) \) of \( \mathbb{T}_{Q_m} \) is stable under \( \chi_{Q_m} \). Therefore \( \sigma_{Q_m} \in \text{Aut}(\mathbb{T}_{Q_m}) \) induces an involution \( \sigma_n \) on \( R_n = R_{n,m} = \mathbb{T}_{Q_m}/(p^n, \delta_q^{p^n} - 1) \). \( \square \)
We will prove in Lemma 6.1 that we can add the following compatibility (Q9) to the above list of the conditions (Q0–8):  

(Q9) $\pi_{n+1}^n \circ \sigma_{n+1} = \sigma_n \circ \pi_{n+1}^n$, and the set $\{f_1^{(n)}, \ldots, f_r^{(n)}\}$ is made of eigenvectors of $\sigma_n$ for all $n$ (i.e., $\sigma_n(f^{(n)}_j) = \pm f^{(n)}_j$).

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

Set (3.2)  

$$\Delta := \Delta(\Delta) = \lim_{\Delta} W[\Delta/\Delta_n^n] = \lim_{\Delta} W[\Delta_n]$$

for the $p$-profinite group $\Delta = \lim_{\Delta} \Delta_n \cong \mathbb{Z}_p$ with $\Delta = \Delta_+ \times \Delta_-$ and $A$ be a local $S$-algebra. Thus by identifying $\Delta/\Delta_n^n \cong \mathbb{Z}_p$ with $\Delta = \Delta_+ \times \Delta_-$ and $A$ be a local $S$-algebra. The image $S_n := W_n[\Delta_n]$ $(W_n = W/p^nW)$ of $S$ in $R_n$ is a local complete intersection and hence Gorenstein. We assume that the ordering of (Q3) is given as $Q_m := \{q_1, \ldots, q_r\}$ and $Q_n := \{q_{r+1} = : q_1^*, \ldots, q_r = q_r^*\}$.

4. Taylor–Wiles primes

We recall the way Wiles chose the sets $Q$ as we compute later cohomologically the $\pm$ eigenspace of the tangent space of $R_Q$ using the Wiles’s choice here. Write $Ad$ for the adjoint representation of $\tilde{\rho}$ acting on $\text{st}(\tilde{\rho})$ 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  

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

$$\beta'_Q : H^1(Q(Qn)p/Q, Ad^*(1)) \to \prod_{q \in Q} H^1(Q_q, Ad^*(1)).$$

Here is a lemma due to A. Wiles [Wi95, Lemma 1.12] on which the existence proof of the sets $Q_m$ is based. We state the lemma slightly different from [Wi95, Lemma 1.12], and for that, we write $K_1 = W_1^{\text{Ker}Ad}$ (the splitting field of $Ad = Ad(\tilde{\rho})$). Since $Ad \cong \chi \otimes \text{Ind}_F^\mathbb{F} \tilde{\rho}$, we have $K_1 = F(\varphi^-)$.

**Lemma 4.1.** Assume (W). Pick $0 \neq x \in \text{Ker}(\beta'_Q)$, and write  

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

for the restriction of the cocycle representing $x$ to $\text{Gal}(Q(Qn)p/K_1(\mu_p))$. Let $\tilde{\rho}$ be the composite of $\tilde{\rho}$ with the projection $\text{GL}_2(\mathbb{F}) \to \text{PGL}_2(\mathbb{F})$, and pick a positive integer $C$ which is a product of primes $l \neq p$ split in $F/Q$. Then, $f_x$ factors through $\text{Gal}(Q(Qn)p/K_1(\mu_p))$, and there exists $a_x \in \text{Gal}(Q(Qn)p/K_1(\mu_p))$ such that

1. $\tilde{\rho}(\sigma_x) \neq 1$ (so, $Ad(\varepsilon_x) \neq 1$).
2. $\sigma_x$ fixes $\mathbb{Q}(\mu_{cpm})$ for an integer $m > 0$.
3. $f_x(\sigma_x^a) \neq 0$ for $a : = \text{ord}(\tilde{\rho}(\sigma_x)) = \text{ord}(Ad(\varepsilon_x))$.

Strictly speaking, [Wi95, Lemma 1.12] gives the above statement replacing $K_1$ by the splitting field $K_0$ of $\tilde{\rho}$. Since the statement is about the cohomology group of $Ad^*(1)$, we can replace $K_0$ in his argument by $K_1$. We note also Ker($Ad(\tilde{\rho})$) = Ker($\beta$) as the kernel of the adjoint representation: $\text{GL}(2) \to \text{GL}(3)$ is the center of $\text{GL}_2$ (so it factors through $\text{PGL}_2$).

**Proof.** Since $x \in \text{Ker}(\beta'_Q)$, $f_x$ is unramified at $q \in Q$; so, $f_x$ factors through $\text{Gal}(Q(Qn)p/K_1(\mu_p))$. We have two possibilities of $F' := K_1 \cap Q(\mu_{cpm})$; i.e., $F' = Q$ or a quadratic extension of $Q$ disjoint from $F$. Indeed, the maximal abelian extension of $Q$ inside $K_1$ is either $F$ (when ord($\tilde{\rho}$) is odd > 1) or a composite $F'$ of the quadratic extensions $F$ and $F'$ over $Q$ (if ord($\tilde{\rho}$) is even $2n > 2$). If $\tilde{\rho}$ has odd order, $F' = Q(\mu_{cpm}) \cap K_1 = Q$ as it is a subfield of $F$ and $Q(\mu_{cpm})$ (because $(C, D) = 1$ and $F \cap Q(\mu_p) = \mathbb{Q}$).
Assume that \(\text{ord}(\overline{\varphi}) = 2n > 2\). Let \(D := \text{Gal}(K_1/Q)\) and \(C := \text{Gal}(K_1/F)\). Then \(C\) is a cyclic group of order \(2n\). Pick a generator \(g \in C\). Then \(D = C \cup Cg\) for a lift \(\zeta\) of \(\zeta\), and we have a characterization \(C_C = \{\tau \in D: \tau g^{-1} = g^{-1}, \tau^2 = 1\}\). For the derived group \(D'\) of \(D\), we have \(D'^{ab} := D/D' \cong (Z/2Z)^2\). We have \(K_1^{D'}\) is equal to \(C^2 \times \langle \zeta \rangle\) (a dihedral group of order \(2n\)). If \(n > 2\) (so, \(n > 4\)), \(\text{Ind}_F^{D'}\) restricted to \(D_1/K_1/F)\) is still irreducible isomorphic to \(\text{Ind}_F^{D'}\). If \(n = 2\), \(F'\) is a unique quadratic extension in \(K_1^{D'}\) unramified at \(D'\). In any case, \(F' \neq F\) which is quadratic over \(Q\). Since \(F' = \overline{Q}(\mu_{C_2^n})\cap K_1\) is at most quadratic disjoint from \(F\), we can achieve (1)-(2) by picking up suitable \(\sigma_x\) in \(C^2 \times \langle \zeta \rangle\) because \(Ad = \overline{\chi} \oplus \text{Ind}_F^{D'}\).

Let \(M_x := \overline{Q}_{\text{ker}(f_x)}\). Then \(Y := \text{Gal}(M_x/K_1(\mu_{p^n}))\) is embedded into \(Ad^*(1)\) by \(f_x\) and \(f_x\) is equivariant under the action of \(Gal(K_1(\mu_{p^n})/Q)\) which acts on \(Y\) by conjugation. Since \(Ad = \overline{\chi} \oplus \text{Ind}_F^{D'}\), we have two irreducible invariant subspaces \(X \subset Ad^*(1)\): \(X = \overline{\chi}w\) and \(\text{Ind}_F^{D'}(\overline{\chi}w)\). Thus \(f_x(Y)\) contains one of \(X\) as above. By (1), we have \(\overline{\chi}(\sigma) = (\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix})\) with \(\alpha \neq \beta\). By (2), we have \(\alpha/\beta = \det(\overline{\chi})|_{\text{Gal}(\overline{Q}(\mu_{C_2^n}))}(\sigma) = \overline{\chi}(\alpha)\) for some \(k_0\) (since \(\det(\overline{\chi})|_{\text{Gal}(\overline{Q}(\mu_{C_2^n}))}\) is equal to \(\overline{\chi}\) up to a power of \(w\). The eigenvalue of \(Ad^*(1)\) is therefore \(\overline{\chi}(\sigma), 1, \alpha^2 - \overline{\chi}(\sigma)\) with \(\alpha^2 = \overline{\chi}(\sigma)\).

If \(f_x(Y) \supset X\), we claim to find \(\sigma\) satisfying (1), (2) and \(\sigma\) has eigenvalue 1 in \(X\) if \(Y = \overline{\chi}w\), the splitting field of \(F\) is \(\mu_{C_2^n}\). Note that \(F(\mu_{C_2^n})\) is abelian over \(Q\). Thus choosing \(\sigma\) fixing \(F(\mu_{C_2^n})\) and \(\sigma \in C^2|K_1\), and having \(\text{ord}(\overline{\chi}(\sigma)) \geq \text{ord}(\mu_{C_2^n}) = |C^2| \geq 2\), we have \(\sigma\) having eigenvalue 1 on \(X = \overline{\chi}w\).

If \(X = \text{Ind}_F^{D'}(\overline{\chi}w)\), we just choose \(\sigma \in \text{Gal}(K_1(\mu_{C_2^n})/Q(\mu_{C_2^n}))\) inducing the non-trivial automorphism on \(F\) (i.e., the projection to the factor \(\langle \zeta \rangle\) of \(C^2 \times \langle \zeta \rangle\) is non-trivial). Since \(\sigma\) fixes \(Q(\mu_{C_2^n})\), we have \(\omega(\sigma) = 1\); so, we forget about \(w\)-twist. Then on \(\overline{\chi}\), \(Ad(\sigma)\) has eigenvalue \(-1\), and hence \(Ad(\sigma)\) has to have the eigenvalue \(-1\) on \(\text{Ind}_F^{D'}(\overline{\chi})\).

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 \(\tau\) commutes with \(\sigma\) in \(\text{Gal}(M_x/\overline{Q})\). This shows \((\sigma\tau)^a = \sigma^a\tau^a\), and \(f_x((\sigma\tau)^a) = f_x(\sigma^a\tau^a) = f_x(\sigma^a) + f_x(\tau^a)\). Since \(f_x(\tau^a) \neq 0\), 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).

Let \(Q = \emptyset\) and choose a basis \(\{x\}\) over \(F\) of the “dual” Selmer group \(S_2^*(Ad^*(1))\) inside \(H^1(Q(\text{Ad}(F(\phi)))\) (see (4.1) below for the definition of the Selmer group). Then Wiles’ choice of \(Q_m\) is a set of primes \(q\) so that \(Frob_q = \sigma_x\) on \(M_x\) as in the above lemma. By Chebotarev density, we have infinitely many sets \(Q_m\) with this property.

**Corollary 4.2.** Let the notation be as in Lemma 4.1 and its proof. If \(0 \neq f_x(Y) \subset \text{Ind}_F^{D'}(\overline{\chi}w)\), the field automorphism \(\sigma\) in Lemma 4.1 satisfies \((\frac{F/\overline{Q}}{\sigma}) = -1\). Otherwise, we can choose \(\sigma\) so that \((\frac{F/\overline{Q}}{\sigma}) = 1\).

**Proof.** In this case, we can have \(X[1] \subset \text{Ind}_F^{D'}(\overline{\chi}w) \neq 0\); so, \(Ad(\sigma)(1) = Ad(\sigma)\) (as \(\omega(\sigma) = 1\)) must have two distinct eigenvalues \(\{1, -1\}\) on \(\text{Ind}_F^{D'}(\overline{\chi})\), which implies \((\frac{F/\overline{Q}}{\sigma}) = -1\) as \(\sigma\) has to have eigenvalues \(-1\) with multiplicity 2.

**Definition 4.3.** Let \(Y^-\) (resp. \(Y^-\)) be the Galois group over \(K^-\) of the maximal \(p\)-abelian extension of \(K^-\) unramified outside \(p\) and totally split at \(p^\infty\) (resp. totally splits at all prime factors of \(p^N\)). Regarding \(\text{Gal}(F(\phi)/F)\) as a subgroup of \(\text{Gal}(K^-F(\phi)/F) \cong \text{Gal}(F(\phi)/F) \times \text{Gal}(K^-/F)\), define \(Y^- = Y^- \otimes_{\text{Z}_p[\phi]}(\text{Gal}(F(\phi)/F), \phi)\) and \(Y^- = Y^- \otimes_{\text{Z}_p[\phi]}(\text{Gal}(F(\phi)/F), \phi)\).

More generally write \(Y^-\) for the Galois group over \(K^-F(\phi)\) of the maximal \(p\)-abelian extension \(L_Q\) of \(K^-F(\phi)\) unramified outside \(p\) and \(Q\) and totally split at \(p^\infty\). Then define \(Y^- = Y^- \otimes_{\text{Z}_p[\phi]}(\text{Gal}(F(\phi)/F), \phi)\).

Hereafter more generally for a \(\text{Z}_p[\phi]/[\text{Gal}(F(\phi)/F)]\)-module \(X\), we write \(X[\phi] = X \otimes_{\text{Z}_p[\phi]}(\text{Gal}(F(\phi)/F), \phi)\) (the maximal quotient on which the Galois group acts by \(\phi\) after extending scalar to \(W\) containing the values of \(\phi\)). The base ring \(W\) will be clear in the context.
Let $D_Q := D_{Q,k,\psi_k}$ and $D'_Q$ for the corresponding local functor at a prime $l|N_Q P$ defined below (det) in Section 2. Regard $D'_Q(\mathbb{F}[\epsilon])$ for the dual number $\epsilon$ as a subspace of $H^1(\mathbb{Q}_Q, Ad)$ in the standard way: For $\rho \in D'_Q(\mathbb{F}[\epsilon])$, we write $\rho \bar{\psi}^{-1} = 1 + \epsilon u_p$. Then $u_p$ is the cocycle with values in $s_{lQ}(\mathbb{F}) = Ad$. Thus we have the orthogonal complement $D'_Q(\mathbb{F}[\epsilon])^\perp \subset H^1(\mathbb{Q}_Q, Ad^*(1))$ under the Tate local duality. We recall the definition of the Selmer group giving the global tangent space $D_Q(\mathbb{F}[\epsilon])$ and its dual from the work of Wiles and Taylor–Wiles (e.g., [HIM, §3.2.4]):

$$Sel_Q(Ad) := \text{Ker}(H^1(\mathbb{Q}^{QNP}/\mathbb{Q}, Ad) \to \prod_{l|NP} H^1(\mathbb{Q}_l, Ad)/D'_Q(\mathbb{F}[\epsilon])) (\cong D_Q(\mathbb{F}[\epsilon])),$$

(4.1)

$$Sel_Q(Ad^*(1)) := \text{Ker}(H^1(\mathbb{Q}^{QNP}/\mathbb{Q}, Ad^*(1)) \to \prod_{l|NP} H^1(\mathbb{Q}_l, Ad^*(1))/D'_Q(\mathbb{F}[\epsilon])^\perp \times \prod_{q \in Q} H^1(\mathbb{Q}_q, Ad^*(1)).$$

Since $Ad = \chi \oplus \text{Ind}_F^Q \bar{\psi}$ for $\chi := (\chi \text{ mod } p)$, $Sel_Q(Ad)$ (resp. $Sel_Q(Ad^*(1))$) is the direct sum of the Selmer groups $Sel_Q(\chi)$ (resp. $Sel_Q(\chi/\omega)$) and $Sel_Q(\text{Ind}_F^Q \bar{\psi})$ (resp. $Sel_Q(\text{Ind}_F^Q \bar{\psi}/\omega)$). To give a sketch of this direct sum decomposition (first noticed in [CV03, Theorem 3.1]), consider $Sel_Q^p(Ad^*(1))$ (whose decomposition as above is equivalent to (4.2) below). Then $D'_Q(\mathbb{F}[\epsilon])$ is made of classes of cocycles such that $u_p|I_p$ is upper nilpotent with values in $F_+(\rho)$ in the introduction and $u_p|I_p,\mu_p$ is the wild inertia subgroup.

$$D'_Q(\mathbb{F}[\epsilon])^\perp = \left(D'_Q(\mathbb{F}[\epsilon])^\perp \cap H^1(\mathbb{Q}_p, \chi/\omega) \oplus (D'_Q(\mathbb{F}[\epsilon])^\perp \cap H^1(\mathbb{Q}_1, \text{Ind}_F^Q \bar{\psi}/\omega) \right),$$

and $D'_Q(\mathbb{F}[\epsilon])^\perp \cap H^1(\mathbb{Q}_p, \text{Ind}_F^Q \bar{\psi}/\omega)$ is made of upper nilpotent matrices in $Ad^*(1)$ (since Ind$_F^Q \bar{\psi}$ is the direct sum of the upper right nilpotent Lie algebra and lower right nilpotent Lie algebra). This implies

$$(D_p)\text{ the Selmer cocycle }u\text{ for Ind}_F^Q \bar{\psi}/\omega\text{ is possibly ramified at }p\text{ with }u(\phi \tau \phi^{-1}) = \bar{\psi} \omega u(\phi)\text{ for }\tau \in I_p\text{ but trivial over the decomposition group at }p\text{, where }\phi \in \text{Gal}(\mathbb{Q}_p/F_p)\text{ and }I_p \subset I_p\text{ is the wild inertia subgroup.}$$

If $\varphi$ is non-trivial, $\tau \neq \delta$, and the given filtration $\tau_0 \supseteq \tau_1 \supseteq \cdots \supseteq \tau_k$ determines $F_+(\rho)$. Thus the triviality at $p^\omega$ of the Selmer cocycle is automatic as $\text{Gal}(\mathbb{Q}_p/F_p)$ leaves stable $F_+(\rho)$, and hence any deformation local at $p$ of $\bar{\psi}$ having values in $F_+(\bar{\psi})$ over $I_p$ has values in $F_-(\bar{\psi})$ over the entire decomposition group $\text{Gal}(p, \mathbb{Q}_p/F_p)$. Note here that $I_p^w$ fixes $F(\varphi^\omega)$ by (h1), and hence $u_p|I_p^w : I_p^w \to \bar{\psi}^\omega$ is a homomorphism, and the decomposition group acts by such a homomorphism by inner conjugation. Thus the condition $D_p$ requires in particular that $u_p|I_p^w$ is a $F[\text{Gal}(\mathbb{Q}_p/F_p)]$-homomorphism (where we regard $u_p|I_p^w$ as having values in the subspace $F_+(\bar{\psi})$ which is isomorphic to the $\text{Gal}(F(\varphi^\omega/F)-module \bar{\psi}^\omega)$. If $\varphi^\omega$ is ramified at $p$, the conjugation action of the $p$-inertia subgroup $I_{p^w}$ of $\text{Gal}(F_0/F)$ on its wild inertia subgroup $I_{p^w}$ determines the action of the decomposition subgroup $D_{Q_p}$ at $p$ as the inertia eigenspace of Hom($I_{p^w}, \bar{\psi}^\omega$) is automatically an eigenspace under the decomposition group, and the specification of the filtration $\tau_0 \supseteq \tau_1 \supseteq \cdots \supseteq \tau_k$ is automatic so that $\tau$ is ramified. In any case, $D_Q^p(\mathbb{F}[\epsilon])^\perp \cap H^1(\mathbb{Q}_p, \text{Ind}_F^Q \bar{\psi}/\omega)$ is the direct factor $H^1(F_p, \bar{\psi}/\omega)$ of

$$H^1(F_p, \text{Ind}_F^Q \bar{\psi}) = H^1(F_p, \bar{\psi}/\omega) \oplus H^1(F_p, \bar{\psi}^{-1}/\omega),$$

where $\bar{\psi}^\omega(\tau) = \bar{\psi}^{-1} = (\bar{\psi}^\omega)^{-1}(\tau)$.

Since $\bar{\psi}$ is trivial on $\text{Gal}(\mathbb{Q}_p/F_p)$, we have $H^1(\mathbb{Q}_p, \chi) = H^1(\mathbb{Q}_p, \mu_p) \cong \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p$ by Kummer theory. Since $\bar{\psi}$ ramifies at $p$, we have $H^0(I_p, \chi) = 0$, and by inflation and restriction sequence, we have an exact sequence:

$$0 = H^1(F_{p^w}, H^0(I_p, \chi)) \to H^1(\mathbb{Q}_p, \chi) \to H^1(I_p, \mu_p)^{Frob_p = 1} \to H^2(F_{p^w}, H^0(I_p, \chi)) = 0.$$
This implies all non-zero classes in $H^1(Q_p, \overline{\omega})$ is ramified. Similarly, since $\chi$ is unramified and $\hat{Z}$ has cohomological dimension $1$, we have a commutative diagram with exact rows:

\[
\begin{array}{ccc}
H^1(\text{Frob}_p, \chi) & \xrightarrow{i} & H^1(Q_p, \chi) & \xrightarrow{=} & H^1(I_p, \chi)^{\text{Pro}b_{p}=1} \\
\text{Hom}(\text{Frob}_p, F) & \xrightarrow{i} & \text{Hom}(Q_p, F) & \xrightarrow{=} & \text{Hom}(Z_p^\times, F)^{\text{Pro}b_{p}=1}.
\end{array}
\]

By the requirement of the cocycle in $D^p_Q(F[e])$ is upper nilpotent over $I_p$ and is upper triangular over $D_p := \text{Gal}(\overline{Q}_p/Q_p)$, we have $D^p_Q(F[e])$ is $\text{Hom}(\text{Frob}_p, F)$ whose $p$-local Tate dual is $(p^2/p^2) \otimes_Z F \subset (Q_p^\times/(Q_p^\times)^p) \otimes_Z F = H^1(Q_p, \overline{\omega}) \otimes_{Z_p} F$ by Kummer theory. Since $F$-dual of $\text{Hom}(Q_p, F)$ is $(Q_p^\times/(Q_p^\times)^p) \otimes_Z F = H^1(Q_p, \overline{\omega}) \otimes_{Z_p} F$, we have

$$D^p_Q(F[e])^\perp \cap H^1(Q_p, \overline{\omega}) = H^1(I_p, \overline{\omega})^{\text{Pro}b_{p}=1} = (Z_p^\times/(Z_p^\times)^p) \otimes_Z F.$$

So, it is ramified, and hence

(Km) the Selmer cocycle $u_\overline{\chi}$ in $\text{Sel}^1_Q(\overline{\omega})$ for $\overline{\chi}$ can ramify at $p$ and is a Kummer cocycle in $(Z_p^\times/(Z_p^\times)^p) \otimes_{Z_p} F \subset (Q_p^\times/(Q_p^\times)^p) \otimes_{Z_p} F$, projecting down trivially to $F$ by sending $z \in Q_p^\times$ to its $p$-adic valuation modulo $p$.

For a prime $l|N_{F/Q}(c)$, $Ad \cong \overline{\omega} \otimes \overline{\chi} \otimes (\overline{\omega})^{-1}$ and $Ad^*(1) \cong \overline{\chi} \otimes \overline{\chi} \otimes (\overline{\omega})^{-1} \overline{\omega}$ over Gal$(\overline{Q}_p/Q_l)$ (as $F_l = Q_l \otimes Q_l$). Write $\overline{\chi}$ (resp. $\overline{\omega}$) for $\overline{\omega}$ and $\overline{\gamma}$ (resp. $\overline{\gamma}$ and $\overline{\omega}$) in order to treat the two cases at the same time. We normalize $Ad$ so that the character $\overline{\chi}$ is realized on $F(\frac{1}{0}, \frac{0}{1})$ and $\overline{\omega}$ appears on the upper nilpotent matrices and $(\overline{\omega})^{-1}$ acts on lower nilpotent matrices, and we also normalize $Ad^*(1)$ accordingly.

Remark 4.4. By the above normalization, over Gal$(\overline{Q}_p/F)$, $\overline{\gamma}$ at the upper right corner of $Ad$ is paired with $(\overline{\omega})^{-1}\overline{\omega}$ at the lower left corner of $Ad^*(1)$. Thus $\mathcal{Y}(\overline{\gamma})$ is paired with $\mathcal{Y}(\overline{\omega})^{-1}$ over $\mathcal{I}(\overline{Q}_p/F)$, and then we conjugate back to $\mathcal{Y}(\overline{\omega})$ by $\overline{\chi}$. In this way, $\mathcal{Y}(\overline{\omega})$ and $\mathcal{Y}(\overline{\gamma})$ are paired.

Since $H^0(I_l, \varphi) = 0$, we have an isomorphism $H^1(Q_l, \varphi) \cong H^1(I_l, \varphi)^{\text{Pro}b_{l}=1}$ by the restriction map. Since $\overline{\omega}$ is unramified at $l$, we have $\varphi \cong 1 \otimes \varphi |_{l}$. We have the following exact sequence

$$0 \rightarrow H^1(\varphi(I_l), \varphi) \rightarrow H^1(I_l, \varphi) \rightarrow \text{Hom}_{\varphi(I_l)}(\text{Ker}(\varphi|_{I_l}), \varphi) \rightarrow H^2(\varphi(I_l), \varphi).$$

Since $\varphi(I_l)$ has order prime to $p$, we have $H^1(\varphi(I_l), \varphi) = 0$ for all $j > 0$. Thus $H^1(I_l, \varphi) \cong \text{Hom}_{\varphi(I_l)}(\text{Ker}(\varphi|_{I_l}), \varphi)$. Since any elements in $\text{Hom}_{\varphi(I_l)}(\text{Ker}(\varphi|_{I_l}), \varphi)$ factors through the $l$-adic quotient of $I_l$ which is abelian, the conjugation action of $\varphi(I_l)$ on $\text{Ker}(\varphi|_{I_l})$ is trivial, while $\varphi$ is non-trivial; so, we conclude $H^1(I_l, \varphi) \cong \text{Hom}_{\varphi(I_l)}(\text{Ker}(\varphi|_{I_l}), \varphi)$ vanishes. Thus we get

$$H^1(Q_l, Ad) = \text{Hom}(\text{Gal}(\overline{Q}_l/Q_l), F(\frac{1}{0}, \frac{0}{1})) \cong F$$

and $H^1(Q_l, Ad^*(1)) = H^1(Q_l, F(\frac{1}{0}, \frac{0}{1}) \otimes \varphi) = H^1(\text{Frob}_p, F(\frac{1}{0}, \frac{0}{1}) \otimes \varphi) \cong F$, which is the Tate dual of $H^1(Q_l, Ad)$. This tell us that the Selmer cocycle $u_p$ giving a class in $D^p_Q(F[e])$ for $Ad$ has values in $F(\frac{1}{0}, \frac{0}{1})$ over Gal$(\overline{Q}_l/Q_l)$ and is unramified. In other words, we have $D^p_Q(F[e]) = H^1(Q_l, Ad)$; so, again the direct sum decomposition (4.2) holds, and we find $D^p_Q(F[e])^\perp = H^1(Q_l, Ad^*)^\perp = 0$.

At $l|D, \overline{\gamma} = \text{Gal}(\overline{Q}_l/Q_l)$ is trivial. Thus we have $Ad \cong \overline{\chi} \otimes \text{Ind}_{\chi}^\overline{\chi} \overline{\chi} \cong \overline{\chi} \otimes 1 \otimes \overline{\chi}$ over Gal$(\overline{Q}_l/Q_l)$. The first factor $\overline{\chi}$ is realized in $F(\frac{1}{0}, \frac{0}{1})$, the last factor $\overline{\chi}$ is realized on $F(\frac{0}{1}, \frac{1}{0})$ and the middle factor $1$ is realized on $Ad^{(l)} = F(\frac{1}{0}, \frac{0}{1})$. Arguing in the same way as we showed $H^1(Q_l, \overline{\omega}) = 0$, replacing $\overline{\omega}$ by $\overline{\chi}$, we find that $H^1(Q_l, \overline{\gamma}) = 0$. By Shapiro's lemma, we have $H^1(Q_l, \text{Ind}^Q_l 1) = H^1(F_l, F) = \text{Hom}(F_l^\times, F) \cong F$ by (h3). Thus the cohomology classes in $H^1(Q_l, Ad)$ is represented by cocycles with values in $F(\frac{0}{1}, \frac{1}{0})$. Therefore we get $H^1(Q_l, Ad) = \text{Hom}(\text{Gal}(\overline{Q}_l/Q_l), F(\frac{1}{0}, \frac{0}{1}))$, and $\rho \in D^p_Q(F[e])$ if and only if $\rho|_p$ has image in $\text{Ad}(F^{(l)}) = F(\frac{1}{0}, \frac{0}{1})$ and is unramified. In particular, $D^p_Q(F[e]) = H^1(Q_l, Ad) \cong F$ and $D^p_Q(F[e])^\perp = 0$. Thus we get

(D_N) Cohomology classes in $\text{Sel}^1_Q(\text{Ad} \otimes \overline{\gamma})$ is trivial at all primes $l|N$.

By the same argument applied to $Ad^*(1)|_{\text{Gal}(\overline{Q}_l/Q_l)} = \overline{\chi} \otimes \overline{\chi} \otimes \overline{\chi}$ with $H^1(Q_l, \overline{\omega}) = 0$, Kummer's theory tells us that $H^1(Q_l, Ad^*(1)) = Q_l^\times/(Q_l^\times)^p \otimes_{Z_p} F \cong F$, which is represented by cocycle with $\overline{\chi}$.
values in $F(\frac{1}{p})$ on which $Gal(\overline{Q}/Q)$ acts by $\omega$ as a factor of $Ad^*(1)$. Therefore the direct sum decomposition (4.2) holds, and $D_Q^e(F[\epsilon]) = H^1(\Omega, Ad) = 0$. Thus, for the dual Selmer groups of $Ind_{F}^{L} \varphi \omega$ and $\varphi \omega$, triviality at $l/N$ is imposed (by $(D_N)$). In particular, for the splitting field $K$ of $\chi \omega$, writing $Cl_{\chi \omega}(p^{\infty}) := \lim_n Cl_{\chi \omega}(p^n)$ for the ray class group modulo $p^n$ ($n = 0, \ldots, \infty$) of $K$, we have

$$Sel_{\omega}^{\chi \omega}(\varphi \omega) \hookrightarrow \text{Hom}(Cl_{\chi \omega}(p^{\infty}), F)[\varphi \omega],$$

where $\text{Hom}(Cl_{\chi \omega}(p^{\infty}), F)[\varphi \omega]$ is the $\varphi \omega$-eigenspace of $\text{Hom}(Cl_{\chi \omega}(p^{\infty}), F)$ under the action of $Gal(F(\chi \omega)/Q)$. Note that $\varphi \omega$ ramifies both at two primes $\mathfrak{q}$ and $\mathfrak{f}$ over $l|N_{F/Q}(\mathfrak{c})$. Since $\varphi$ is anti-cyclotomic, any prime $l|D$ is completely split in $F(\varphi \omega)/F$.

Let $F^Q$ be the maximal extension of $K_0$ unramified outside $Q$ and $p$. By (h3), all deformations of $\overline{\varphi} = Ind_{F}^{L} \varphi$ satisfying (D1–4) factors through $Gal(F^Q/Q)$. Write $L_{Q}^{\varphi \omega}$ for the maximal $p$-abelian extension of $F(\varphi \omega)$ inside $F^Q$ totally split at $p^N$ and unramified outside $Q$ and $p$. By (h3), $L_{Q}^{\varphi \omega}/F(\varphi \omega)$ is unramified at all $l|N$. Thus we conclude

$$Sel_{\omega}^{\chi \omega}(Ind_{F}^{L} \varphi \omega) \cong Sel_{\omega}^{\chi \omega}(\varphi \omega) = \text{Hom}_{Gal(F(\varphi \omega)/F)}(Gal(L_{Q}^{\varphi \omega}/F(\varphi \omega)), \varphi \omega) \mid [p,F].$$

Here the condition $[p,F] = \varphi \omega(\mathfrak{p},\mathfrak{f}) = \varphi \omega(\mathfrak{p},\mathfrak{f})$ is automatic if $\varphi \omega$ ramifies at $\mathfrak{p}$ as already explained. Since $p \nmid h_F$, $K_0/F$ is fully wild $\mathfrak{p}$-ramified, while $F(\varphi \omega)$ is at most tamely $\mathfrak{p}$-ramified. Therefore the inertia subgroup of $\mathfrak{p}^+$ for the extension $K_0^0 F(\varphi \omega)/F(\varphi \omega)$ is the entire Galois group $Gal(K_0^0/F(\varphi \omega)/F(\varphi \omega))$. This tells us that $L_{Q}^{\varphi \omega} \cap K_0^0 F(\varphi \omega) = F(\varphi \omega)$. Thus, we have the vanishing of the $\varphi \omega$-eigenspace

$$Coker(Y_{sp} \xrightarrow{Res} Gal(L_{Q}^{sp}/F(\varphi \omega))) \mid [\varphi \omega]$$

and we find

$$Gal(L_{Q}^{sp}/F(\varphi \omega)) \mid [\varphi \omega] = Y_{sp}(\varphi \omega)_{H} = H_0(H, Y_{sp}(\varphi \omega))$$

and

$$\text{Hom}_{Gal(F(\varphi \omega)/F)}(Gal(L_{Q}^{sp}/F(\varphi \omega)), \varphi \omega) = \text{Hom}(Y_{sp}(\varphi \omega)_{H}, F) = \text{Hom}_{W[H]}(Y_{sp}(\varphi \omega), F).$$

Proposition 4.5. Let $Cl_{Q^+} = \{ x \in Cl_Q : |x(x)| = x^{-1} \}$, and write $Cl_{Q(\chi \omega)}(p^{\infty})$ for the class group of the splitting field of $\chi \omega$. Then, under $(h1–4)$, we have $Y_{sp}(\varphi \omega) = Y^{-}(\varphi \omega)$ for $Q \in Q$,

$$Sel_{Q}(Ad) \cong Hom(Cl^{-}_{Q^+}, F) \oplus Hom_{W[H]}(Y^{-}(\varphi \omega), F) \text{ including } Q = 0,$$

and

$$Sel_{\omega}^{\chi \omega}(Ad^*(1)) \cong Sel_{\omega}^{\chi \omega}(\varphi \omega) \oplus Hom_{W[H]}(Y_{sp}^{-}(\varphi \omega), F),$$

and

$$Sel_{\omega}^{\chi \omega}(Ad^*(1)) \cong Sel_{\omega}^{\chi \omega}(\varphi \omega) \oplus Hom_{W[H]}(Y_{sp}^{-}(\varphi \omega), F),$$

where the cocycles in the image of $Sel_{\omega}^{\chi \omega}(\varphi \omega)$ in Hom$(Cl_{Q(\chi \omega)}(p^{\infty}), F)[\varphi \omega]$ give rise to locally at $p$ a Kummer cocycle coming from $Z_{sp}^{\chi \omega}/Z_{sp}^{p} F$. This is almost identical to [H17, Proposition 3.8] which is stated for imaginary quadratic $F$. Since the proof is similar but a bit different, we recall it for the reader’s convenience. Since $F$ is real, $H$ is a finite $p$-abelian group.

Proof. We have already proven the last two identities of (4.4) and the second identity of (4.3). Thus we deal with the rest. The subspace $D_{Q}^{e}(F[\epsilon])$ is made of classes of cocycles with values in $Ad = sp_{2}(F)$ such that $u_{l}|_{D_l}$ is upper nilpotent with values in $F_{l}(\rho)$ in the introduction and $u_{p}|_{D_{p}}$ $(D_{p} := Gal(\overline{Q}_p/Q_p))$ is upper triangular. Similarly $D_{F}^{e}(F[\epsilon])$ for $l|N$ is made of classes of unramified cocycles $u_{p}$ with values in diagonal matrices over $D_{l}$. Then by the same argument proving (4.2) (or by the dual statement of (4.2)), we note that

$$Sel_{Q}(Ad) = Sel_{Q}(\varphi \omega) \oplus Sel_{Q}(Ind_{F}^{L} \varphi \omega),$$

and
where Sel_{Q}(\overline{\chi}) = \text{Ker}(H^1(\mathbb{Q}^{(QN_p)}/\mathbb{Q}, \overline{\chi}) \to \prod_{q|N_p} H^1(I_q, \overline{\chi})) and

\begin{equation}
\text{Sel}_{Q}(\text{Ind}_{F}^{Q}(\overline{\varphi}^-)) = \text{Ker}(H^1(\mathbb{Q}^{(QN_p)}/\mathbb{Q}, \text{Ind}_{F}^{Q}(\overline{\varphi}^-)) \to \prod_{q|N_p} H^1(Q_{I_q}, \text{Ind}_{F}^{Q}(\overline{\varphi}^-)) \to H^1(F_{p^r}, \overline{\varphi}^-) \times \prod_{I} H^1(I, \text{Ind}_{F}^{Q}(\overline{\varphi}^-)).
\end{equation}

By the inflation-restriction sequence,

\text{Sel}_{Q}(\overline{\chi}) \cong \text{Ker}(\text{Hom}_{\text{Gal}(F/\mathbb{Q})}(\text{Gal}(F^Q/F), \chi) \to \prod_{I} H^1(I, \chi)) \cong \text{Hom}(C\text{I}_{Q}, \mathbb{F}).

However the order of \text{Ker}(C\text{I}_{Q^-}, C\text{I}_{Q^+}) is a factor of \prod_{q|D} (q + 1), which is prime to \mathcal{P}; so, we conclude

\text{Sel}_{Q}(\overline{\chi}) \cong \text{Hom}(C\text{I}_{Q^-}, \mathbb{F}) \cong \text{Hom}(C\text{I}_{Q^+}, \mathbb{F}).

Again by the inflation-restriction sequence, identifying \text{Gal}(\overline{\mathbb{Q}}_{\mathcal{P}}/\mathbb{Q}_{\mathcal{P}}) with the decomposition group at \mathcal{P}^\mathcal{P}, we have an exact sequence

\text{H}^1(\text{Frob}_{\mathcal{P}}^{\mathcal{P}}, \text{H}^0(I_{\mathcal{P}}, \overline{\varphi}^-)) \to \text{H}^1(F_{\mathcal{P}^\mathcal{P}}, \overline{\varphi}^-) \to \text{H}^1(I_{\mathcal{P}}, \mathbb{F}(\overline{\varphi}^-))^{\text{Frob}_{\mathcal{P}}^{\mathcal{P}}} = 0.

If \varphi^- is ramified at \mathcal{P} (and hence also at \mathcal{P}^\mathcal{P}), we have \text{H}^0(I_{\mathcal{P}}, \overline{\varphi}^-) = 0 and \text{H}^1(\text{Frob}_{\mathcal{P}}^{\mathcal{P}}, \text{H}^0(I_{\mathcal{P}}, \overline{\varphi}^-)) = 0. Thus we conclude, if \varphi^- is ramified at \mathcal{P},

\text{Ker}(\text{H}^1(F_{\mathcal{P}}, \overline{\varphi}^-) \to \text{H}^1(I_{\mathcal{P}}, \overline{\varphi}^-)) = 0,

and \text{Sel}_{Q}(\text{Ind}_{F}^{Q}(\overline{\varphi}^-)) is actually given (by replacing \text{H}^1(F_{\mathcal{P}}, \overline{\varphi}^-) by \text{H}^1(I_{\mathcal{P}}, \overline{\varphi}^-) in (4.5))

\begin{equation}
\text{Ker}(\text{H}^1(\mathbb{Q}^{(QN_p)}/\mathbb{Q}, \text{Ind}_{F}^{Q}(\overline{\varphi}^-)) \to \text{H}^1(I_{\mathcal{P}}, \overline{\varphi}^-)) \times \prod_{I} H^1(I, \text{Ind}_{F}^{Q}(\overline{\varphi}^-)) \text{ if \varphi^- is ramified at \mathcal{P}.}
\end{equation}

By the inflation-restriction sequence, we have an exact sequence \text{H}^1(\text{Frob}_{\mathcal{I}}^{\mathcal{I}}, (\overline{\varphi}^-)^{I}) \to \text{H}^1(D_{I}, \overline{\varphi}^-) \to \text{H}^1(I, \overline{\varphi}^-) with (\overline{\varphi}^-)^{I} = 0 for I|N, and hence by Shapiro’s lemma (and (h3)), we can rewrite

\text{Sel}_{Q}(\text{Ind}_{F}^{Q}(\overline{\varphi}^-)) \cong \text{Hom}_{W[H_{Q}]}(\mathcal{V}_{Q}^- (\overline{\varphi}^-), \mathbb{F}).

Similarly, \text{Sel}_{Q}(\overline{\chi}) \cong \text{Hom}_{\text{Gal}(F/\mathbb{Q})}(\text{Gal}(\mathbb{Q}^{(QN_p)}/\mathbb{Q}), \overline{\chi}) = \text{Hom}(C\text{I}_{Q}, \mathbb{F}). Therefore the first identity of (4.3) follows if we prove \text{Y}_{Q}^- (\varphi^-) \otimes_{W[H_{Q}]} \mathbb{F} = \text{Y}^- (\varphi^-) \otimes_{W[H]} \mathbb{F}.

To prove \text{Y}_{Q}^- (\varphi^-) \otimes_{W[H_{Q}]} \mathbb{F} = \text{Y}^- (\varphi^-) \otimes_{W[H]} \mathbb{F}, writing \mathcal{I}^{p\text{ab}} for the maximal \mathcal{P}-abelian quotient of the inertia group \mathcal{I}_{Q} \subset \text{Gal}(\mathcal{Q}/K_{Q}F(\varphi^-)) of a prime \mathcal{Q}|q in K_{Q}F(\varphi^-), we have an exact sequence

\prod_{\mathcal{Q}|q \in \mathcal{Q}} \mathcal{I}^{p\text{ab}}_{Q} \to \mathcal{Y}_{Q}^- \to \mathcal{Y}^- \to 0

as \text{Ker}(\mathcal{Y}_{Q}^- \to \mathcal{Y}^-) is generated by the image \mathcal{I}^{p\text{ab}}_{Q} \cong \mathbb{Z}_{\mathcal{P}}. The surjectivity of the restriction map: \mathcal{Y}^- \to \mathcal{Y}^- follows from linear-disjointness of \mathcal{L}_{\mathcal{P}} and K_{Q}F(\varphi^-) over K^-F(\varphi^-) as at least one of \mathcal{Q} \in \mathcal{Q} ramifies in any intermediate field of K_{Q}F(\varphi^-)/K^-F(\varphi^-). Note that \mathcal{Q} \in \mathcal{Q}^- totally splits in K^-F(\varphi^-)/F. Thus \mathcal{I}^{p\text{ab}}_{Q} \cong \prod_{\mathcal{Q}|q} \mathcal{I}^{p\text{ab}}_{Q} for \mathcal{Q} \in \mathcal{Q}^- is isomorphic to

\text{Z}_{\mathbb{P}}^{\text{Gal}(K_{Q}F(\varphi^-)/F)} = \text{Z}_{\mathbb{P}}[[\text{Gal}(K_{Q}F(\varphi^-)/F)]] = \text{Z}_{\mathbb{P}}[H_{Q}][\text{Im}(\varphi^-)]
as \( \mathbb{Z}_p[[\text{Gal}(K_Q F(\varphi^-)/F)]] \)-modules. Since \( I^\text{ab}_Q \cong \mathbb{Z}_p \) is the quotient of the maximal \( q \)-tame quotient of \( I_Q \), \( \text{Frob}_q \) (for the prime \( q | q \in Q^- \) in \( F \)) acts on it via multiplication by \( q^2 \). Since \( \varphi^- (\text{Frob}_q) = 1 \), the map \( I^*_q \otimes \mathbb{Z}_p[\text{Im}(\varphi^*)], \varphi^- W \to \mathcal{Y}_Q(\varphi^-) \) factors through

\[
I^*_q(\varphi^-) = I^*_q \otimes \mathbb{Z}_p[\text{Im}(\varphi^*)], \varphi^- W \cong W[H_Q]/(q^2 - 1).
\]

Thus we have \( I^*_q(\varphi^-) \otimes W[H_Q] \mathbb{F} = \mathbb{F}(\varphi^-) \) (one dimensional space over \( \mathbb{F} \) on which \( \text{Gal}(F(\varphi^-)/F) \) acts by \( \varphi^- \)). Note that \( \text{Frob}_q \) acts on \( I^*_q(\varphi^-) \otimes W[H_Q] \mathbb{F} \) via multiplication by \( q \), which is trivial as \( q \equiv 1 \) mod \( p \). Thus the image of \( I^*_q(\varphi^-) \otimes W[H_Q] \mathbb{F} \) in \( \mathcal{Y}_Q \) is stable under \( \text{Frob}_q = c \), and hence stable under \( \text{Gal}(F(\varphi^-)/Q) \). The \( \text{Gal}(F(\varphi^-)/Q) \)-module \( \text{Ind}^Q_F \varphi^- \) is absolutely irreducible by (h4). Since \( I^*_q(\varphi^-) \otimes W[H_Q] \mathbb{F} = \mathbb{F}(\varphi^-) \), if the image is non-trivial, it must contain the irreducible \( \text{Gal}(F(\varphi^-)/Q) \)-module \( \text{Ind}^Q_F \varphi^- \), which is impossible as the image has dimension \( \leq 1 \). Thus the image of \( I^*_q(\varphi^-) \otimes W[H_Q] \mathbb{F} \) in \( \mathcal{Y}_Q(\varphi^-) \) is trivial.

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

\[
I^*_q := \prod_{\Omega \in \Omega_q^+} I^*_Q(\varphi^-) \cong \mathbb{Z}_p^D \cong \mathbb{Z}_p[\text{Gal}(K_Q F(\varphi^-)/F)/D(\Omega/q)]
\]
on which \( \text{Frob}_q \) acts by \( \sigma D(\Omega/q) \mapsto q \sigma \text{Frob}_q D(\Omega/q) = q \sigma D(\Omega/q) \) for \( \sigma \in \text{Gal}(K_Q F(\varphi^-)/F) \) 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 \( p \)

\[
I^*_q(\varphi^-) \otimes W[H_Q] \mathbb{F} = \begin{cases} 
0 & \text{if } \varphi^- (\text{Frob}_q) \neq 1, \\
\mathbb{F} & \text{if } \varphi^- (\text{Frob}_q) = 1,
\end{cases}
\]

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

\[
\mathcal{Y}_Q \otimes W[H_Q] \mathbb{F} \cong \mathcal{Y}^-(\varphi^-) \otimes W[H] \mathbb{F}
\]
as desired.

The primes \( q \) in \( Q_m \) is indexed by a basis \( \{ x \}_x \) of the Selmer group \( \text{Sel}^D(A d^*(1)) \) so that \( f_x \) as in Lemma 4.1 has non-trivial value at \( \text{Frob}_q \). Thus writing \( Q_m^\pm := \{ q \in Q_m \mid \chi(q) = \pm 1 \} \), we get from our choice in Corollary 4.2

(4.7) \[ |Q_m| = \dim \text{Hom}_W[H](\mathcal{Y}_Q^{\varphi^-}(\varphi^- \omega), \mathbb{F}) \] \[ |Q_m^+| = \dim \text{Sel}^D(\chi_W) = \dim \text{Sel}^D(\chi_W).
\]

5. GALOIS ACTION ON UNIT GROUPS

Hereafter we assume that \( F \) is real quadratic over \( Q \). We use notation introduced in Definition 1.2 for abelian extensions of \( F \). Since \( \text{Gal}(F(\varphi^-)/Q) \) is a dihedral group, we can lift the generator \( \zeta \in \text{Gal}(F/Q) \) to an element of order 2 in \( \text{Gal}(F(\varphi^-)/Q) \). We choose one such a lift and write it as \( \tilde{\zeta} \). As before, for any \( W[\text{Gal}(F(\varphi^-)/F)] \)-module \( X \), we write \( X[\varphi^-] \) for the \( \varphi^- \)-eigenspace:

\[
X[\varphi^-] = \{ x \in X | \tau x = \varphi^- (\tau) x \text{ for all } \tau \in \text{Gal}(F(\varphi^-)/F) \}.
\]

We recall from Proposition 4.5

(5.1) \[
\text{Sel}(\mathcal{Y}(\varphi^-)) \cong \text{Hom}_W[H](\mathcal{Y}(\varphi^-), \mathbb{F}) \cong \text{Hom}(\mathcal{Y}(\varphi^-)_H, \mathbb{F}).
\]

Therefore we study the space \( \mathcal{Y}(\varphi^-)_H \) of \( H \)-coinvariants of \( \mathcal{Y}(\varphi^-) \).

Let \( \mathfrak{R} \) be the integer ring of \( F(\varphi^-) \). By (h3), \( \mathcal{Y}(\varphi^-) \) only ramifies at \( p \) and completely split at \( \mathfrak{p}^\prime \). Thus we have \( \text{Frob}_p(\varphi^-) = 1 \) in \( \mathcal{Y}(\varphi^-) \). Write \( D \) for the subgroup of \( CL_{F(\varphi^-)} \) generated by the classes of prime ideals over \( \mathfrak{p}^\prime \). Then we have the following exact sequence:

(5.2) \[
\left( \prod_{\mathfrak{p} | \mathfrak{p}^\prime} (1 + \mathfrak{p} \mathfrak{R}_p) \otimes \mathbb{Z}_p W \right) \varphi^- W \to \mathcal{Y}(\varphi^-)_H \to (CL_{F(\varphi^-),p}/D)[\varphi^-],
\]
where $\mathfrak{P}$ runs over all primes in $\mathfrak{P}$ above $p$ and $\overline{\mathfrak{R}}^\times(p)$ is the closure of the image of $\{\varepsilon \in \mathfrak{R}^\times | \varepsilon \equiv 1 \mod \mathfrak{t} \}$ (for the radical $\mathfrak{t}$ of $p$ in $\mathfrak{R}$) in $\prod_{\mathfrak{p}|p} \overline{\mathfrak{R}}^\times_q$.

Note that $\varphi^-$ is odd at all real places of $F$. As a module over $\text{Gal}(F(\varphi^-)\mathcal{O}_F/\mathcal{O}_F)$, we have $\mathcal{O}_\mathfrak{p} \cong O_p[\text{Gal}(F(\varphi^-)\mathcal{O}_F/\mathcal{O}_F)]$ as $\mathfrak{P}$ is only tamely ramified over $O_p = \mathbb{Z}_p$, and therefore $\mathcal{O}_\mathfrak{p} \cong O_p[\text{Gal}(F(\varphi^-)/M)]$.

Since $\varphi^-$ (resp. $\varphi^-\omega$) is odd (resp. even) at all real places of $F$ as $\text{Ind}_{F}^{Q} \varphi$ is odd at the infinite place of $\mathbb{Q}$. Thus $F(\varphi^-)$ is totally complex. Let $\text{Log} : \mathfrak{R}_p^\times \to \mathfrak{R}_p$ be the $p$-adic logarithm map. The Galois group $\text{Gal}(F(\varphi^-)/\mathbb{Q})$ acts on $\mathfrak{R}_p[\varphi^-] \oplus \mathfrak{R}_p[\varphi^-]$ via $\text{Ind}_{F}^{Q} \varphi^-$, where $\varphi^- = (\varphi^-)^{-1}$.

**Proposition 5.1.** Write $a$ for the order of $\varphi^-$. Then $a$ is even with $a = 2b$ for $0 < b \in \mathbb{Z}$, and we have $\mathfrak{R}^\times \otimes_\mathbb{Z} \mathbb{Q} \cong \chi \oplus \bigoplus_{j=1}^{b-1} \text{Ind}_{F}^{Q}(\varphi^-)^{2j}$ as $\text{Gal}(\mathbb{Q}/F)$-modules.

**Proof.** Since $\det(\text{Ind}_{F}^{Q} \varphi)(\varepsilon) = -1$ for complex conjugation, $\varphi$ ramifies at only one infinite place. Therefore $\varphi^-$ ramifies at the two infinite places of $F$; so, $a = |F(\varphi^-) : F|$ has to be even, and hence $a = 2b$. In particular, complex conjugation $c$ in the cyclic group $\text{Gal}(F(\varphi^-)/F)$ of order 2 and is in the center of the dihedral group $\text{Gal}(F(\varphi^-)/\mathbb{Q})$ [IAT, Proposition 5.11]. Thus $F(\varphi^-)$ is a CM field with maximal totally real field $F((\varphi^-)^2)$; so, $c$ acts trivially on $\mathfrak{R}^\times \otimes_\mathbb{Z} \mathbb{Q}$ and as Galois modules, we have $1 \oplus \mathfrak{R}^\times \otimes_\mathbb{Q} \mathbb{Q} \cong \text{Ind}_{F}^{Q}(\varphi^-)^2$ for the identity character 1. Then the assertion is clear from this expression. □

**Corollary 5.2.** We have $\dim_F \text{Sel}_Q(\text{Ind}_{F}^{Q} \varphi^-) \geq 1$ and $\dim_{\text{Frac}(W)} \text{Sel}_Q(\text{Ind}_{F}^{Q} \varphi^- \otimes_W \text{Frac}(W)) = 1$, where the Selmer group over $\text{Frac}(W)$ is defined by the local data $\mathcal{D}_Q(W|\varepsilon) \otimes_W \text{Frac}(W)$ for primes $l \in Q$ and $l \nmid N_p$.

**Proof.** By (5.2), we have

$$\dim_F \text{Sel}_Q(\text{Ind}_{F}^{Q} \varphi^-) \geq \text{rank}_W \left( \prod_{\mathfrak{P} : \mathfrak{P} | \mathfrak{p}} \frac{(1 + \mathfrak{P} \mathfrak{R}_p)}{\mathfrak{R}^\times (\mathfrak{p})} \otimes_{\mathbb{Z}_p} W \right)[\varphi^-].$$

By $p$-adic logarithm,

$$\prod_{\mathfrak{P} : \mathfrak{P} | \mathfrak{p}} (1 + \mathfrak{P} \mathfrak{R}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \bigoplus_{j=1}^{a} (\varphi^-)^j$$

as $\text{Gal}(F(\varphi^-)/F)$-modules. By Proposition 5.1 (1), $\overline{\mathfrak{P}}^\times(\mathfrak{p}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a surjective image of the Galois module $\bigoplus_{j=1}^{b} (\varphi^-)^{2j}$. Thus the $\varphi^-$-part of the quotient $\frac{\prod_{\mathfrak{P} : \mathfrak{P} | \mathfrak{p}} (1 + \mathfrak{P} \mathfrak{R}_p)}{\mathfrak{R}^\times (\mathfrak{p})} \otimes_{\mathbb{Z}_p} W$ has rank 1, and hence we get the formula over $\mathbb{F}$. Since the class group of $F(\varphi^-)$ is finite, the Selmer group over the characteristic 0 field $\text{Frac}(W)$ has dimension 1 by (5.2). □

Consider the subgroup $E$ of totally positive units in $O^\times$ to study $\text{Sel}_{1}^{1}(\chi\omega)$. Define

$$E(a) := \{ \varepsilon \in E | \varepsilon \equiv 1 \mod a \}$$

and $E_- = E \cap (1 + p^sO_p^\times)^p = E(p^{2s}) = E(p^2)$.  

**Proposition 5.3.** Let the notation be as above, and assume that $p \geq 3$. Then we have

$$\dim_F \text{Hom}(\text{Cl}_Q(\chi\omega), \mathbb{F})[\chi\omega] \geq \dim_{E} E(p^2)/E(p)^p$$

with equality if the class number $h_F = |\text{Cl}_F|$ is prime to $p$, and $E(p^2)/E(p)^p$ is canonically embedded into $\text{Hom}(\text{Cl}_Q(\chi\omega), \mathbb{F})[\chi\omega]$. Similarly, assuming further (h3),

$$\dim \text{Sel}_{1}^{1}(\chi\omega) \geq 1$$

with equality if the class number $h_F = |\text{Cl}_F|$ is prime to $p$, and $E \otimes \mathbb{F} = E/E^p$ is canonically embedded into $\text{Sel}_{1}^{1}(\chi\omega)$.  

Proof. We write \( a \) for the exponent of \( E \) modulo the radical \( \mathfrak{r} \) of \((pN)\) in \( O \) (i.e., \( a \) is the minimal positive integer so that \( \varepsilon^a \equiv 1 \mod \mathfrak{r} \) for all \( \varepsilon \in E \)). Since \(-1 \in E \) and \( p > 2 \), \( a \) is even, and \( a \) is prime to \( p \) by (h3). Let \( E_+ := \{ \varepsilon^a | \varepsilon \in E \} \). Note \( E_+ \subset E(\mathfrak{r}) \). Since \( p \) splits in \( F(q) \), \( F_p = Q_p \) for a prime factor \( p | p \) in \( F \), and hence \( 1 + p^2O_p = (1 + pO_p)^p \). By (h3), \( E_+ \subset (O^*)^p \) for all prime factors \( l | N \); so, \( F_1Q[\varepsilon] = F[\mu_p] \) for all \( \varepsilon \in E_+ \) at all \( l \) (i.e., total splitting at \( l \) or \( N \)).

Thus we conclude
\[
\eta \in U_{\gamma}(\sigma) = \eta_aU_{\gamma}(\sigma) \quad \text{or} \quad \eta = (a_{\mu_p}) \in U_{\gamma}(\sigma)
\]
for all \( \varepsilon \in E_+ \). Thus \( E_+ = U_{\gamma}(\sigma) \). Fix a \( p \)-th primitive root \( \zeta_p \) of unity, and identify \( \mu_p \) with \( F_p \) by \( \zeta_p^m \mapsto m \in F_p \). In this way, we regard \( \mu_p \) as a root of unity, and \( \lim \mu_p \) for some \( \lim \mu_p \) generates \( \zeta_p \) by \( \langle \varepsilon \rangle \) for \( \varepsilon \in \mu_p \) (1). Let \( U_\gamma = U_{\gamma}(\sigma) \) with values in \( \mu \). Then \( U_\gamma \in U_{\gamma}(\sigma) \).

The set of conjugates of \( \varepsilon \) over \( Q \) is given by \( \zeta \varepsilon \zeta^{-1} \zeta \in \mu_{p}(\mathfrak{q}) \) as \( c(\varepsilon) = \varepsilon \). Thus \( L := F(\mu_p) \) is a Galois extension over \( Q \) and \( Gal(L/F) \). Thus \( \gamma \in Gal(L/F) \). Thus for any lift \( \gamma, \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \gamma \ga...
by sending \( \varepsilon \) to \( U^1(\text{Gal}(\mathbb{Q}(\chi_\omega)/\mathbb{Q})) \) which in Case (1) factors through \( Cl_{\mathbb{Q}(\chi_\omega)} = \text{Gal}(H(\chi_\omega)/\mathbb{Q}(\chi_\omega)) \) for the Hilbert class field \( H(\chi_\omega) \) over \( \mathbb{Q}(\chi_\omega) \) and in Case (2) factors through \( Cl_{\mathbb{Q}(\chi_\omega)}(p^\infty) \).

Let \( L/F \) be a \( p \)-abelian extension unramified everywhere. Then we can choose \( \xi \in F_{(p)}^\times \) so that \( L = F[\mu_p][\sqrt[p]{\xi}] \) by Kummer's theory (i.e., \( F[\mu_p]^\times/(F[\mu_p]_p)^p \cong H^1(F,F_{(p)}) \)). Suppose that \( L/Q \) is a Galois extension such that the conjugation action of \( \text{Gal}(L/F) \) on \( \text{Gal}(L/F[\mu_p]) \cong F_p \) is given by \( \overline{\xi} \). Then we have \( F[\mu_p]^\times/(F[\mu_p]_p)^p \cong H^1(L,F[\mu_p]/L) \). The action of \( \tau \in \text{Gal}(F[\mu_p]/L) \) on a cocycle \( u \in \text{Gal}(\mathbb{Q}(L)/F) \rightarrow \mu_p \) is \( \tau \mapsto u(\overline{\tau}^{-1} \sigma \overline{\tau}) \) for a lift \( \overline{\tau} \in \text{Gal}(L/F) \) of \( \tau \in \text{Gal}(F[\mu_p]/F) \). Thus we have

\[
(\overline{\tau}^{-1} \sigma \overline{\tau}) = \overline{(\tau)}(\sigma^{-1})(\overline{\tau}).
\]

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

\[
(\overline{\tau}^{-1} \sigma \overline{\tau}) = (\overline{\tau} \xi). \]

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

\[
1 \rightarrow H^0(F[\mu_p]/F,F[\mu_p]_p^\times/m_p) \xrightarrow{x^{-x^p}} H^0(F[\mu_p]/F,F[\mu_p]^\times) \rightarrow H^0(F[\mu_p]/F,F[\mu_p]^\times/m_p)^p \rightarrow H^1(F[\mu_p]/F,F[\mu_p]^\times/m_p)
\]

combined with the fact that \( H^1(F[\mu_p]/F,F[\mu_p]_p^\times/m_p) \) is killed by \( [F[\mu_p]:F] \) prime to \( p \), we find that \( H^0(F[\mu_p]/F,F[\mu_p]^\times/m_p)^p \cong (F^\times/(F^\times)^p)^p \). Thus we can choose \( \xi \in F^\times \).

Suppose that \( L/F \) is everywhere unramified. Then \( \xi \) is a \( p \)-power as an ideal in \( F[\mu_p] \). Since \( F[\mu_p] \) only ramifies at \( p \) with ramification index prime to \( p \), \( \xi \) is a \( p \)-power as an ideal of \( F \), write \( \xi = \prod_{i} \mathfrak{p}^\ell_i \) for prime ideals \( \mathfrak{p} \) of \( F \). Since \( Gal(F[\mu_p]/Q) \) acts on \( \text{Gal}(L/F[\mu_p]) \) by \( \overline{\xi} \), we have \( (\overline{\xi}) = (\overline{\xi})^\ell \mod \text{prime ideals } \mathfrak{p} \). Thus \( (\overline{\xi}) = (\overline{\xi})^\ell \mod \text{prime ideals } \mathfrak{p} \). This shows \( \xi \equiv \xi \mod (F[\mu_p]^\times)^p \). Thus \( \tau \mapsto \overline{\tau}^{-1} \xi \) is a cocycle with values in \( O^\times \). The exact sequence

\[
1 \rightarrow H^0(F[\mu_p]/F,O^\times \otimes \chi) \xrightarrow{x^{-x^p}} H^0(F[\mu_p]/F,O^\times) \rightarrow H^1(F[\mu_p]/F,O^\times \otimes \chi),
\]

combined with the fact that \( H^1(F[\mu_p]/F,O^\times \otimes \chi) \) is killed by \( [F:Q] = 2 \) prime to \( p \), we find that \( H^0(F[\mu_p]/F,O^\times \otimes \chi) = O^\times/((O^\times)^p) \). Thus we may assume that \( \varepsilon \equiv \varepsilon^{-1} \mod F \); so, \( \varepsilon \in F \), and \( \overline{\xi} \) generates \( L \) over \( Q \). Since \( a \) is prime to \( p \), we may assume that \( \varepsilon \equiv \varepsilon \mod p^\ell \), and we find that \( \varepsilon \) gives rise to a non-trivial class of \( E_{+}(p^\ell)/E_{+}^{\ell} \supset E_{+}^{\ell} \otimes_F \mathbb{Z} \). We thus conclude \( \text{dim}_{p} \text{Hom}(Cl_{Q}(\mathbb{Q}),F_p)(\mathbb{Q}) = \text{dim}_{p} E_{+}(p^\ell)/E_{+}^{\ell} \), which finishes the proof.

For the second assertion, we argue in the same way as above replacing \( L \) by a \( p \)-abelian extension \( L' \) of \( F[\mu_p] \) allowing ramification only at \( p \) as allowed in (Km). Though \( \varepsilon \) has to be in \( O^\times \), by (Km) \( , \) locally at \( p \), \( L_p = Q_p(\mu_p)[\sqrt[p]{\xi}] \) with \( \varepsilon \in \mathbb{Z}^\times_p \), we find \( \varepsilon \equiv \varepsilon \mod O^\times \), and we get the result as \( \text{Ker}(Cl(p) : Cl(p) \rightarrow Cl(p) \) has order prime to \( p \).

Consider \( \mathfrak{a} := \text{Ker}(N_{F(\varepsilon^{-1})}/F : O^\times \rightarrow O^\times) \) to study \( \text{Sel}_F^\infty(\mathfrak{a}) \cap \text{Sel}_F^\infty(\mathfrak{a}) \cong \text{Hom}_{W[H]}(Y^{-}(\varepsilon^{-1}),F) \) for \( H \) as in Definition 1.2. Define

\[ \mathfrak{a}(a) := \{ \varepsilon \in \mathfrak{a} \mid \varepsilon \equiv 1 \mod a \} \]

for an ideal \( a \) of \( F(\varepsilon^{-1}) \) over \( p \).

**Proposition 5.4.** Let the notation be as above, and assume that \( p \geq 3 \). Then we have

\( \text{Sel}_F^\infty(\mathfrak{a}) \cong \text{Hom}_{W[H]}(Y^{-}(\varepsilon^{-1}),F) = 0 \)

if \( (Cl_{F(\varepsilon^{-1})}(\mathfrak{a}) \otimes F\mathfrak{a})[\mathfrak{a}] = 0 \).

Note here the action of \( \gamma \in \text{Gal}(F(\varepsilon^{-1})/F) \) on \( \phi \in \text{Hom}_{W[H]}(Y^{-}(\varepsilon^{-1}),F) \) is given by \( \gamma \phi(x) = \phi(\gamma^{-1}x) = (\overline{\gamma})^{-1}(\gamma)\phi(x) \) and \( \gamma \phi(x) = (\varepsilon^{-1})^{-1}(\gamma) \); so, by applying \( \gamma \), we have \( (Cl_{F(\varepsilon)} \otimes F)[\mathfrak{a}] = 0 \Rightarrow (Cl_{F(\varepsilon^{-1})} \otimes F)(\mathfrak{a}) = 0 \).
Proof. We follow the path of the proof of Proposition 5.3 with some modification. We write $a$ for the exponent of $E$ modulo the radical of $p^k$ in $\mathfrak{K}$ (i.e., $a$ is the minimal positive integer so that $e^a \equiv 1 \mod p^k$ for all $e \in E$). Since $-1 \in E$ (and $p > 2$), $a$ is even, and plainly $a$ is prime to $p$. Let $\mathfrak{E}_- := \{e^a | e \in E\}$. Note that all $e \in \mathfrak{E}_-$ is positive at each real places of $F$, and $\mathfrak{E}_- \subset \mathfrak{E}(\mathfrak{c})$. For each prime factor $\mathfrak{P}|p^k$ in $\mathfrak{K}$, we consider its $\mathfrak{P}$-adic completion $\mathfrak{R}_p$. Then we define $\mathfrak{E}_+ := \mathfrak{E}_- \cap (\mathfrak{P}|p^k(1 + \mathfrak{P}\mathfrak{R}_p)^p \times \prod_{\mathfrak{P}|p^k} \mathfrak{R}_p^\mathfrak{c})$ inside $\prod_{\mathfrak{P}|p^k} \mathfrak{R}_p^\mathfrak{c}$. By definition $\mathfrak{E}_+ \supset \mathfrak{E}_-(\mathfrak{c})$.

We first give a proof very similar to the one for Proposition 5.3 assuming $\mathfrak{c}^\mathfrak{c}$ has values in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and after doing this we shall give a shorter cohomological proof for general $\mathfrak{c}$. Thus we only deal with the case where $\mathfrak{c}^\mathfrak{c}$ has values in $\mathbb{F}_p$. Take $e \in \mathfrak{E}_+$. Suppose that $e \in \mathfrak{E}_+$ represents a non-trivial element in $(\mathfrak{E}_+/\mathfrak{E}_p)^n(\mathfrak{c}^-)^{-1})$. Consider a Kummer extension $F(\mathfrak{c}^-)(\mu_p)[\sqrt{\tau}]/F(\mathfrak{c}^-)(\mu_p)$.

Again, we let the Galois group acts on field elements from the left. Pick a $p$-th root $\epsilon := \sqrt{\tau}$. Since $(\sigma)\epsilon = \epsilon$, we have $\epsilon^{-1} \in \mu_p(\mathbb{Q})$. Then $u = u_e : \sigma \rightarrow \sigma^{-1} \epsilon = \epsilon/\mu_p$ is a cocycle with values in $\mu_p(\mathbb{Q})$ of $Gal(F(\mathfrak{c}^-)(\mu_p)[\sqrt{\tau}]/F(\mathfrak{c}^-)(\mu_p))$ representing the cohomology class of $\epsilon \in F(\mathfrak{c}^-)/(F(\mathfrak{c}^-)\mathfrak{p}) \cong \mathbb{H}^1(F(\mathfrak{c}^-),\mu_p)$. Indeed, for $\sigma, \tau \in Gal(F(\mathfrak{c}^-)(\mu_p)[\sqrt{\tau}]/F(\mathfrak{c}^-))$, we have $u(\sigma\tau) = \sigma^{-1} \epsilon = \sigma^{-1} \epsilon \tau(\sigma)u(\sigma)$.

Fix a $p$-th primitive root $\zeta_p$ of unity, and identify $\mu_p$ with $\zeta_p^a \mapsto m \in \mathbb{F}_p$. In this way, we regard $u_e$ as a cocycle $U = u_e$ with values in $\mu_p(\mathbb{F}_p)$ so that $u_e(\sigma) = \zeta_p^{U(\sigma)}$. Then $U$ satisfies $U(\sigma) = \omega(\sigma)U(\tau) + U(\tau)$. Thus the Galois action on the subgroup $V \cong \mathbb{F}_p^a$ generated by $\epsilon$ and $\zeta_p$ (a primitive roots of unity) inside $F(\mathfrak{c}^-)(\mu_p)[\sqrt{\tau}]/F(\mathfrak{c}^-)(\mu_p)[\sqrt{\tau}]^p$ is given by $\eta = \eta_e = \sigma \rightarrow (\omega \zeta_p^a \zeta_p^{-e})$, which is a Galois representation $Gal(F(\mathfrak{c}^-)(\mu_p)[\sqrt{\tau}]/F(\mathfrak{c}^-)) \rightarrow GL_2(\mathbb{F}_p)$. Note that $u_{-1}(\sigma) = 1^{-1} \epsilon = u_{\sigma}(\sigma)$ and that for any $p$-th root $\zeta$ of unity, $u_{-1}(\zeta) = \sigma^{-1}(\zeta) = \sigma^{-1} \epsilon^{1^{-1}} = \sigma^{-1} \epsilon u_{\zeta}(\sigma)$; so, $U(\sigma) = (1 - \omega(\sigma))b + U(\sigma)$ with $\zeta = \zeta_p^{-b}$. Thus we conclude

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

for $a(b) = (1, 0)$. Since $u_{-1} = u_{b}^a$, we have $U_{a} = aU$, for $a \in \mathbb{Z}$ prime to $p$. Since $U_{a}$ only depends on $a \mod p$, we write $U_{a} = aU$, for $a \in \mathbb{F}_p$.

The set of conjugates of $e$ over $F$ is given by $\{\zeta^\epsilon \}_{e \in Gal(F(\mathfrak{c}^-)/F), \zeta \in \mu_p(\mathbb{Q})}$ as $\tau(\zeta) = \zeta^{-\epsilon} \mod \mathfrak{c}$. Thus $L := F(\mathfrak{c}^-)(\mu_p)[e]$ is a Galois extension over $F$ and $Gal(L/F(\mathfrak{c}^-)) \supseteq Gal(L/F)$. Thus for any lift $\gamma \in Gal(L/F)$ of the generator $\gamma_0$ of $Gal(F(\mathfrak{c}^-)/F)$, we can think of $\eta'(\sigma) := \eta(\gamma\sigma^{-1})$ which is a representation of $Gal(L/F)$ into $GL_2(\mathbb{F}_p)$ with values in the mirabolic subgroup $P := \{(a, b) \in GL_2(\mathbb{F}_p)| a, b \in \mathbb{F}_p\}$.

In other words, the isomorphism $P \cong Gal(L(F(\mathfrak{c}^-)) \xrightarrow{\eta'} P$ induces an automorphism in $Aut_{sp}(P)$.

Since any automorphism of $P$ is inner, we have $\eta' \circ \eta^{-1}(x) = g x g^{-1}$ for $g \in P$. Taking $x$ to be $\eta(\sigma)$, we find $\eta'(\sigma) = g \eta(\sigma)g^{-1}$; so, $\eta'$ and $\eta$ are equivalent as representations. Write $g := (a, b)$, we find $\gamma' = (\omega a^{(1 + b(1 - \omega))})$. Replace $\epsilon$ by $\zeta_p^{-b}e$ (this modification does not change $L$). Then we may assume that $\gamma' = \eta$, and under this choice of $\epsilon$, we find that $\gamma$ commutes with the elements in $Gal(L/F(\mathfrak{c}^-)) \subset Gal(L/F)$. Since $Gal(L/F) = \prod_{p \in \mathfrak{P}} Gal(L/F(\mathfrak{c}^-)) \subgrp$ must be in the center $Z$ of $Gal(L/F)$. Since $P \cong Gal(L/F(\mathfrak{c}^-)$ has trivial center, the intersection $Z \cap Gal(L/F(\mathfrak{c}^-)) = \{1\}$ is trivial. Thus $Z \supseteq Gal(L(F(\mathfrak{c}^-)) \cap Gal(L(F) = Gal(L(\mathfrak{c}^-)) \times Z$.

Thus we may lift the generator $\gamma_0$ of $Gal(F(\mathfrak{c}^-)/F)$ uniquely to a central element $\gamma \in Gal(L/F)$. Write $\mathfrak{c}^{-1}(\tau) \in Z$ representing the mod $p$ class of $\mathfrak{c}(\tau) \in (\mathbb{Z}/p\mathbb{Z})^\times$; so, $\mathfrak{c}^{-1}(\tau)$ is the inverse of the mod $p$ class $\mathfrak{c}(\tau)$ in $\mathbb{Z}/p\mathbb{Z}$. Then define, for $x \in L^\times$, $\mathfrak{c}^{-1}(\tau) := x^{\mathfrak{c}^{-1}(\tau)} \mod x^{\mathfrak{c}}$. This makes sense only modulo $p$-power of $x$. Then

$$\gamma_e := \zeta e^{\mathfrak{c}^{-1}(\gamma_0)} \mod e^{\mathfrak{c}}$$

(as $e^{\mathfrak{c}} = e^\mathfrak{c}$) for some $\zeta \in \mu_p(L)$ since $\gamma_0 \equiv \mathfrak{c}^{-1}(\gamma_0) \mod e^{\mathfrak{c}}$. Then $\gamma \mathfrak{c}^{-1}(\gamma_0) \equiv \zeta \mod e^{\mathfrak{c}}$. The element $\gamma \mathfrak{c}^{-1}(\gamma_0)$ is in the center of the group algebra $\mathbb{Z}_p[Gal(L/F)]$, we have

$$\zeta^{\sigma^{-1}} \equiv \sigma^{-1}(\gamma \mathfrak{c}^{-1}(\gamma_0)) \equiv \gamma \mathfrak{c}^{-1}(\gamma_0) \equiv \zeta \equiv \zeta^{\mathfrak{c}^{-1}(\gamma_0)} \mod e^{\mathfrak{c}}$$

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

$$\gamma_e = \zeta_p^{\mathfrak{c}^{-1}(\gamma_0)} \mod e^{\mathfrak{c}}$$
Thus $\gamma$ acts on $F(\mu_p)$ as $\omega(\varphi^{-1}(\gamma))^{-1}$. Therefore
\begin{equation}
F(\varphi^-)(\mu_p)^Z := H^0(Z, F(\varphi^-)(\mu_p)) = F(\varphi^-)\omega.
\end{equation}

Hence we have a cyclic extension $F_\gamma/F(\varphi^-)$ which is the fixed subfield of $L$ by $\gamma$. Since $\varepsilon$ is a unit, only possible ramification of $L$ over $F(\varphi^-)(\mu_p)$ at finite places is at a prime over $p$. Thus we get an injective homomorphism
\begin{equation}
(\mathcal{E}_+/\mathcal{E}_0)[(\mathfrak{p}^-)^{-1}] \hookrightarrow \text{Hom}(C(\varphi^-)\omega(p^{\infty}), \mathbb{F}_p)[(\mathfrak{p}^-)^{-1}]
\end{equation}
sending $\varepsilon$ to $U_{\varepsilon(Gal(F/\varphi^-))}$ which factors through factors through $C(\varphi^-)\omega(p^{\infty})$. The ray class group $C(\varphi^-)\omega(p^{\infty})/(p^{\infty})$ is the Galois group of the maximal abelian extension of $F(\varphi^-)\omega$ unramified outside $p$ and $\infty$. Since $\varepsilon \in \mathcal{E}_+$ is locally a $p$-power at $\mathfrak{p}^\infty$ by the definition of $\mathcal{E}_+$, the corresponding Kummer cocycle is trivial at $p^{\infty}$. Therefore, by $(D_p)$ and $(D_N)$, the image of $(\mathcal{E}_+/\mathcal{E}_0)[(\mathfrak{p}^-)^{-1}]$ lands in the image of $\text{Sel}_0(\mathfrak{p}^-)$ in $\text{Hom}(C(\varphi^-)\omega(p^{\infty}), \mathbb{F}_p)[(\mathfrak{p}^-)^{-1}]$.

We now prove the equality: $(\mathcal{E}/\mathcal{E}_0)[(\mathfrak{p}^-)^{-1}] \cong \text{Sel}_0(\mathfrak{p}^-)$. 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 $Gal(F(\varphi^-)(\mu_p)/\mathbb{Q})$ on $Gal(L/F(\varphi^-)(\mu_p)) \cong \mathbb{F}_p$ is given by $\mathfrak{p}^-$. By Kummer’s theory, we have
\[F(\varphi^-)(\mu_p)^{\times}/(F(\varphi^-)(\mu_p)^{\times})^p \cong H^1(F(\varphi^-)(\mu_p), \mu_p)^{(\mathfrak{p}^-)},
\]
The action of $\tau \in Gal(F(\varphi^-)(\mu_p)/F(\varphi^-))$ on a cocycle $u : Gal(F/F(\varphi^-)) \rightarrow \mu_p$ is $\tau u : \sigma \rightarrow \tau(u(\bar{\sigma})\bar{\tau})$ giving rise to an $\mathfrak{p}^\infty$-eigen class in $H^1(F(\varphi^-)(\mu_p), \mu_p)^{(\mathfrak{p}^-)}$, we have
\[\tau(\bar{\tau}^{-1} \bar{\sigma}^{-1}(\sqrt[p]{\xi})) \equiv \tau u(\bar{\tau}^{-1} \bar{\sigma}^{-1}) \equiv \bar{\tau}^{(\bar{\sigma})^{-1}}(\sqrt[p]{\xi}) \bmod (F(\varphi^-)(\mu_p)^{\times})^p.
\]
On the other hand, we may choose $\bar{\sigma}$ so that $\bar{\sigma} \equiv \bar{\tau} \equiv \bar{\xi}$, Under this choice, we have
\[\tau(\bar{\tau}^{-1} \bar{\sigma}^{-1}(\sqrt[p]{\xi})) = \bar{\sigma}^{-1} \bar{\xi}^{-1} \sqrt[p]{\xi}.
\]
Thus we get $\tau(\bar{\sigma}^{-1}(\sqrt[p]{\xi})) = \bmod (F(\varphi^-)(\mu_p)^{\times})^p$. This shows $\xi \equiv \bmod (F(\varphi^-)(\mu_p)^{\times})^p$, and $\tau \rightarrow \tau^{-1}$ is a cocycle with values in $F(\varphi^-)(\mu_p)^{\times}$. The exact sequence
\[1 \rightarrow H^0(F(\varphi^-)(\mu_p)/F(\varphi^-), F(\varphi^-)(\mu_p)^{\times}/\mu_p) \rightarrow H^0(F(\varphi^-)(\mu_p)/F(\varphi^-), F(\varphi^-)(\mu_p)^{\times})
\]
combined with the fact that $H^1(F(\varphi^-)(\mu_p)/F(\varphi^-), (\mu_p)^{\times}/\mu_p)$ 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{equation}
H^1(F, \mathfrak{p}^-) \cong H^0(F(\varphi^-)/F, H^1(F(\varphi^-)\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)[(\mathfrak{p}^-)^{-1}],
\end{equation}
as $H^1(F(\varphi^-)/F, H^0(F(\varphi^-), M)) = 0$ with $j > 0$ for any $[F(\varphi^-)/F]$. Thus we may assume that the class $[\xi]$ of $\xi$ is in the $(\mathfrak{p}^-)^{-1}$-eigenspace $(F(\varphi^-)^{\times} \otimes_{\mathbb{Z}} \mathbb{F}_p)[(\mathfrak{p}^-)^{-1}]$. Here the action of $Gal(F(\varphi^-)/F)$ on cohomology is the contravariant action; so we get $(\mathfrak{p}^-)^{-1}$-eigenvector.

Suppose that $L/F(\varphi^-)(\mu_p)$ is trivial at prime factors in $N$ and unramified outside $p$. Then $\mathfrak{R}[\mathfrak{p}^\infty]$ is a $p$-power as a fractional $\mathfrak{R}[\mathfrak{p}^\infty]$-ideal in $F(\varphi^-)(\mu_p)$. Since $F(\varphi^-)(\mu_p)$ only ramifies at $p$ with ramification index prime to $p$, $(\xi)$ is a $p$-power as a fractional $\mathfrak{R}[\mathfrak{p}^\infty]$-ideal of $(F(\varphi^-))$. Write $(\xi) = \prod_i \langle \varepsilon_i \rangle$ for prime ideals $\mathfrak{p}_i$ of $\mathfrak{R}[\mathfrak{p}^\infty]$. If $h = h_{F(\varphi^-)}$ is prime to $p$, we may replace $\xi$ by $\xi^h$ without
changing $F(\varphi^-)_l[\overline{\xi}]$, and then $\prod_i t^{e(i)}$ becomes a $p$-power of a principal ideal $(\xi')$; i.e., $\xi = \varepsilon \xi^{np}$ for $\varepsilon \in \mathcal{R}^{[1/p]}$. Thus we may replace $\xi$ by $\varepsilon \in \mathcal{R}^{[1/p]}$.

We now show that we can replace $\xi$ by $\varepsilon \in \mathcal{R}^{[1/p]}$ under the assumption: $(Cl_{F(\varphi^-)} \otimes \mathbb{F}_p)[(\overline{\xi})] = 0$ milder than $p \nmid h_{\varphi(\varphi^-)}$. Since $Gal(F(\varphi^-)[\mu_p]/F)$ acts on $Gal(L/F(\varphi^-)[\mu_p])$ by $\overline{\xi}$, we have $\prod_i t^{e(i)} = (\varphi/\overline{\xi}) \equiv (\varphi/\overline{\xi}^{\varphi(\varphi^-) \cdot \varepsilon(i)})$ modulo $p$-power of fractional $\mathcal{R}^{[1/p]}$-ideals. Thus we conclude $\varepsilon(i) = [\varphi(\varphi^-)^{-1} \varepsilon(i)] \mod p$ for the generator $\gamma(\overline{\xi}) \neq 1$ of $Gal(F(\varphi^-)/F)$. In particular, $\varepsilon$ is completely split in $F(\varphi^-)/F$ if $\varepsilon(i) \neq 0$, since $\overline{\xi} \neq 1$. Write $Cl'_{\mathcal{X}}$ for the ideal class group of $O_X[1/p]$ 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

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

for $a = \prod_i t^{e(i)}$, the $(Cl'_{F(\varphi^-)} \otimes \mathbb{Z}_p)[(\overline{\xi})] = 0$ by Nakayama’s lemma, and $\prod_i a^{[\varphi(\varphi^-) \varepsilon(i)]}$ is principal generated by $\xi'$. Replacing $\xi$ by the $(\varphi^-)^{-1}$-projection $\prod_{i=1}^{\mu} a^{[\varphi(\varphi^-) \varepsilon(i)]}$ does not affect the corresponding Kummer extension, we may assume that $\xi = \varepsilon \xi^{np}$. Then $\varepsilon \in \mathcal{R}^{[1/p]}$.

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

$$1 \to H^0(F(\varphi^-)/F, \mathcal{R}^{[1/p]} \times \otimes \varphi^-) \xrightarrow{x \mapsto \varphi^{-1}(x)} H^0(F(\varphi^-)/F, \mathcal{R}^{[1/p]} \times \otimes \varphi^-) \to H^1(F(\varphi^-)/F, \mathcal{R}^{[1/p]} \times \otimes \varphi^-),$$

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

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

$$1 \to \mathcal{R}^X \to \mathcal{R}^{[1/p]} \times \to Ind_{\mathcal{Q}}^{\mathcal{R}} Z[Gal(F(\varphi^-)/F)]/D \to C \to 0$$

with $C$ having order prime to $p$ (because $C \to Cl_{F(\varphi^-)}$). Since $\text{Ind}_{\mathcal{Q}}^{\mathcal{R}} Z[Gal(F(\varphi^-)/F)]/D$ is $\mathbb{Z}$-free, after tensoring with $\mathbb{F}$, we still have an exact sequence:

$$0 \to \mathcal{R}^X \otimes \mathbb{F} \to \mathcal{R}^{[1/p]} \times \otimes \mathbb{F} \to \text{Ind}_{\mathcal{Q}}^{\mathcal{R}} Z[Gal(F(\varphi^-)/F)/D] \otimes \mathcal{F} \to 0.$$
as $H^1(F(\varphi^{-})/F, H^0(F(\varphi^{-}), M)) = 0$ for any $F[Gal(\overline{Q}/F(\varphi^{-}))-module M$ because of $p \nmid [F(\varphi^{-}) : F]$.

The last identity follows from the fact that $\tau u(\phi) = \tau u(\tau^{-1}g\tau) = \varphi^{-}(\tau u(\tau^{-1}g\tau))$ for cocycle $u$ giving rise to a class $H^1(F, \pi \mathfrak{m})$ for $\varphi^{-} \in Gal(F(\varphi^{-})/F)$. By Kummer’s theory, non-zero elements in the right-hand-side of $(5.7)$ correspond, up to scalar multiples, bijectively to $p$-abelian extensions $L'$ of $F(\varphi^{-})[\mu_p]$ with $Gal(L'/F(\varphi^{-})[\mu_p]) \cong F$ such that $Gal(F(\varphi^{-})[\mu_p]/F)$ acts on $Gal(L'/F(\varphi^{-})[\mu_p])$ by $\pi \mathfrak{m}$ by conjugation. Let $EXT_{F(\varphi^{-})}$ be the set of $p$-abelian extensions $L$ inside $\overline{Q}$ of $F(\varphi^{-})$ (resp. $F(\varphi^{-})[\mu_p]$) with $Gal(L/F(\varphi^{-})) \cong F$ (resp. $Gal(L'/F(\varphi^{-})[\mu_p]) \cong F$). We will use $\pi \mathfrak{m}$ of the normal subgroup $Gal(L/F(\varphi^{-}))$ by $\pi \mathfrak{m}$ through conjugation. Non-zero elements in the extension group $H^1(F, \pi \mathfrak{m}) \cong Ext_{F[Gal(\overline{Q}/F)]}(F, \pi \mathfrak{m})$ correspond, up to scalar multiples, bijectively to $p$-abelian extensions $\pi \mathfrak{m} \hookrightarrow X \twoheadrightarrow F$. As an $F$-vector space, $X$ is two dimensional, and choosing a basis $x_1, x_2$ of $X$ over $\mathbb{F}$ so that on $\mathbb{F}x_1$, $Gal(\overline{Q}/F)$ acts by $\pi \mathfrak{m}$. For $\tau \in Gal(\overline{Q}/F)$, $(\tau x_1, \tau x_2) = (x_1, x_2)\rho(\tau)$ with $\rho = \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right)$ for a 1-cocycle $u$ representing $X$. Since $X$ is a non-trivial extension, the class $[u]$ of $u$ is non-trivial in $H^1(F, \pi \mathfrak{m})$. Then the splitting field $L$ of $X$ gives rise to an element in $EXT_{F(\varphi^{-})}$.

Since cohomological relation on cocycles $u$ corresponds equivalence relations on $\rho$ by conjugation inside the mirabolic subgroup $F$, we again conclude that non-zero elements in the left-hand-side of $(5.7)$ correspond, up to scalar multiples, one to one onto to elements in $EXT_{F(\varphi^{-})}$. Therefore $EXT_{F(\varphi^{-})} \ni L \mapsto L[\mu_p] \subseteq EXT_{F(\varphi^{-})}$ is a bijection.

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

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

$$\left( \mathcal{E}_+ / \mathcal{E}_+ \right) \otimes_{\mathbb{F}_p} \mathbb{F} \cong \bigoplus_{\tau} \left( \mathcal{E}_+ / \mathcal{E}_+ \otimes_{\mathbb{F}_p} \mathbb{F} \right)/(\mathfrak{m}^{-1}).$$

Similarly, for $X = F(\varphi^{-})^x / (F(\varphi^{-})^x)^p = F(\varphi^{-})^x \otimes_{\mathbb{F}} \mathbb{F}_p$, $Cl_F(\varphi^{-}) \otimes \mathbb{F}_p$ and $Cl^{\prime}_F(\varphi^{-}) \otimes \mathbb{F}_p$, we have

$$X = (X \otimes_{\mathbb{F}} \mathbb{F})/(\mathfrak{m}^{-1}).$$

A Kummer cocycle $[\xi] = \xi \otimes 1 \in F(\varphi^{-})^x \otimes_{\mathbb{F}} \mathbb{F}_p$ with $\xi \in F(\varphi^{-})^x$ is unramified outside $p$ if its image in $F(\varphi^{-})^x \otimes_{\mathbb{F}} \mathbb{F}_p$ vanishes at all finite places $v \mid p$ of $F(\varphi^{-})$. Thus the principal ideal $\mathfrak{A}_{F(\varphi^{-})^x}$ is a $p$-power $a^p$. Suppose that $[\xi] \in (F(\varphi^{-})^x \otimes_{\mathbb{F}} \mathbb{F}_p)(\Phi)$. Since $(Cl^{\prime}_F(\varphi^{-}) \otimes \mathbb{F}_p)(\mathfrak{m}^{-1}) = 0$ by our assumption $(Cl^{\prime}_F(\varphi^{-}) \otimes \mathbb{F}_p)(\mathfrak{m}^{-1}) = 0$, the projected image $[a]_{\Phi}$ in $Cl^{\prime}_F(\varphi^{-}) \otimes \mathbb{F}_p(\Phi)$ of the class $[a] \in Cl^{\prime}_F(\varphi^{-})$ is trivial. Thus replacing $a$ and $\Phi$-projection (in the fractional ideal group of $\mathfrak{A}_{F(\varphi^{-})^x}$) which is principal, we find that $\xi \equiv \varepsilon^p$ for $\varepsilon \in \mathfrak{A}_{F(\varphi^{-})^x}^{1/x}$. Then repeating the same argument in the case of $\mathbb{F} = \mathbb{F}_p$, we conclude $\varepsilon \in \mathcal{E}_+$ and $\text{Sel}_Q(\text{Ind}_F^\mathbb{Q}(\mathfrak{m}^{-1})) \cong (\mathcal{E}_+ / \mathcal{E}_+)(\mathcal{E}_+ \otimes_{\mathbb{F}_p} \mathbb{F})/(\mathfrak{m}^{-1})$, and thus $\text{Sel}_Q(\text{Ind}_F^\mathbb{Q}(\mathfrak{m}^{-1})) = 0$ as $(\varphi^{-})^{-1}$ does not appear in $\mathfrak{A}_{\bar{X}} \otimes_{\mathbb{Q}} \mathbb{Q}$ by Proposition 5.1.

6. Complete intersection property for $T_+$ and a proof of Theorem A

We give a proof of Theorem A under $p \nmid h_F(\varphi^{-})$ at the end of this section. We first claim to be able to add the compatibility (Q9) to the above list of the conditions (Q0–8):
(Q9) \( \pi^{n+1} \circ \sigma_{n+1} = \sigma_n \circ \pi^{n+1} \), and the set \( \{f_1^{(n)}, \ldots, f_r^{(n)}\} \) is made of eigenvectors of \( \sigma_n \) for all \( n \) (i.e., \( \sigma_n(f_j^{(n)}) = \pm f_j^{(n)} \)).

**Lemma 6.1.** We can find an infinite family \( Q = \{Q_m\}_m \) of \( r \)-sets of primes outside \( Np \) satisfying \( (Q0–9) \).

**Proof.** Pick an infinite family \( Q \) satisfying \( (Q0–8) \). We modify \( Q \) to have it satisfy (Q9). Since \( p > 2 \), plainly, \( R_n \) is generated over \( W \) by \( \sigma_n \)-eigenvectors \( \{\sigma_n(f_j^{(n)}) \pm f_j^{(n)}\}_{j=1,...,r} \). Since \( r \) is larger than or equal to the minimal number of generators \( \dim_{W} t_R^{n} \leq \dim_{W} D_{Q_m,K,v_{n}}(\mathbb{F}(\bar{c})) \) for the co-tangent space \( t_R^{n} := m_{R_n}/(m_{R_n}^2 + m_{W}) \), we can choose \( r \) generators among \( \{\sigma_n(f_j^{(n)}) \pm f_j^{(n)}\} \).

Once compatibility \( \pi_{n+1}^{r} \circ \sigma_{n+1} = \sigma_n \circ \pi_{n+1} \) is shown, we get

\[
\pi_{n+1}^{r}(\sigma_n(f_j^{(n+1)}) \pm f_j^{(n+1)}) = \sigma_n(f_j^{(n)}) + f_j^{(n)}
\]

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

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

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

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

\[
\{(\alpha(R_{m,n}, (f_1, \ldots, f_r)), \sigma_{m,n})\}_{m \geq n}
\]
satisfying \( (Q0–8) \) with \( m \) varying in the choosing process of \( Q \) (of Taylor–Wiles; see [HIM, page 191] or [MFG, §3.2.6]). Then \( m(n) \) is chosen to be minimal choice of \( m \) in the class \( \mathcal{I}_n^{TW} \); so, we can replace \( m(n) \) by a bigger one if we want (as \( \mathcal{I}_n^{TW} \) is an infinite set). In other words, choosing \( m \) appearing in \( \mathcal{I}_n^{TW} \) possibly bigger than \( m(n) \), we would like to show that we are able to add the datum of the involution \( \sigma \) induced by \( \pi_{m(n)}^{r} \). Therefore, we look into isomorphism classes in the infinite set of \( (\sigma\text{-added}) \) quadruples (varying \( m \))

\[
\{(\alpha(R_{m,n}, (f_1, \ldots, f_r)), \sigma_{m,n})\}_{m \geq n+1}
\]
of level \( n \) in place of triples \( \{(\alpha(R_{m,n}, (f_1, \ldots, f_r)), \sigma_{m,n})\}_{m \geq n+1} \) indicating the involution of \( R_{m,n} \) induced by \( \pi_{m,n}^{r} \) (which is compatible with the projection \( R_{m,n} \to \tilde{R}_{m,n} \)).

We start an induction on \( n \) to find the projective system satisfying \( \pi^{n+1} \circ \sigma_{n+1} = \sigma_n \circ \pi^{n+1} \). The projection \( \pi_{Q_m} : R_{Q_m} \to R_\emptyset \) (for any \( m \geq 1 \)) of forgetting ramification at \( Q_m \) is \( \sigma \)-compatible (by definition) for the involution \( \pi_{Q_m}^{r} \) and \( \sigma_{Q_m}^{r} \) coming from the \( \chi \)-twist, which induces a surjective \( W \)-algebra homomorphism \( \pi_{Q_m}^{r} : R_{Q_m} \to R_{\emptyset} \) satisfying \( \pi_{Q_m}^{r} \circ \sigma_{Q_m}^{r} = \pi_{Q_m}^{r} \circ \pi_{Q_m}^{r} \). Thus the initial step of the induction is verified. In the same way, the projection \( R_{m,n} \to R_{m,n} \) is compatible with the involution.

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

\[
((R_{m,n}, (f_1, \ldots, f_r)), \sigma_{m,n}) \in \mathcal{I}_n'
\]
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 \( R_{Q,n} \to R_{Q,n+1} \), and \( \tilde{R}_{Q,n+1} = R_{Q}/(p^{n+1}, \delta_q^{n+1} - 1)_{q \in Q} \to \tilde{R}_{Q,n} = R_{Q}/(p^n, \delta_q^{n} - 1)_{q \in Q} \), the projections

\[
R_{Q,n+1} \to R_{Q,n} \quad \text{and} \quad \tilde{R}_{Q,n+1} = R_{Q}/(p^{n+1}, \delta_q^{n+1} - 1)_{q \in Q} \to \tilde{R}_{Q,n} = R_{Q}/(p^n, \delta_q^{n} - 1)_{q \in Q}
\]
are compatible with the involutions induced by $\sigma_Q$, and hence for the same set of generators $\{f_j\}_j$, the two quadruples
\[
\{(R_{Q,j}, \alpha), (R_{Q,j}, (f_1, \ldots, f_r), \sigma_j)\}_j
\]
of level $j = n + 1$, $n$ are automatically $\sigma_j$-compatible.

Since the number of isomorphism classes of level $n+1$ in $T_n'$ is finite, we can choose an isomorphism class $I_{n+1}$ of level $n+1$ with $[I_{n+1}] = \infty$ inside $T_n'$ whose members are isomorphic each other (this is the pigeon-hole principle argument of Taylor–Wiles). Thus by induction on $n$, we get the desired compatibility $\pi_{n+1}^n \circ \sigma_{n+1} = \sigma_n \circ \pi_n^1$ for $I_{n+1}$; i.e., \( I_{n+1} \xrightarrow{\text{reduction}} I_n \rightarrow I_{n-1} \rightarrow \cdots \rightarrow I_1 \) with $[I_j] = \infty$ for all $j = 1, 2, \ldots, n + 1$. We hereafter write $m(n)$ for the minimal of $m$ with $(\{R_{n,m}, \alpha\}, R_{n,m}, (f_1, \ldots, f_r), \sigma_{n,m})$ appearing in $I_n$.\)

\[\square\]

**Lemma 6.2.** Suppose that the family $\mathcal{Q} = \{Q_m|m = 1, 2, \ldots\}$ satisfies (Q0–9). Define $Q^\pm_m = \{q \in Q_m | \chi(q) = \pm 1\}$. Then $|Q^\pm_m|$ (and hence $|Q^+_m|$) is independent of $m$ for $Q_m \in \mathcal{Q}$.\]

*Proof.* Since $|Q_m| = \dim_{\mathbb{F}} \text{Hom}_W[H](\mathcal{J}_{sp}(\varphi, \omega), \mathbb{F})$ by Proposition 4.5, it is independent of $m$.\)

By (Q9), we have the limit involution $\sigma_\infty$ acting on $R_\infty = \varprojlim_n R_{n,m(n)}$, and we may assume that the generators $(f_{j_1}^{(n)}, \ldots, f_{j_r}^{(n)})$ to satisfy $\sigma_n(f_{j_r}^{(n)}) = \pm f_{j_r}^{(n)}$. Therefore we may assume that $(f_{j_1}^{(n)}, \ldots, f_{j_r}^{(n)}) = (f_{j_1}^{(\infty)}, \ldots, f_{j_r}^{(\infty)}, f_{d_+}^{(n)}, \ldots, f_{d_-}^{(n)})$ with $\sigma_\infty(f_{j_1}^{(\infty)}) = \pm f_{j_1}^{(\infty)}$ for $r = d_+ + d_-$, and hence, we may assume that
\[
R_\infty \cong W[[T_{d_+, T_{d_+}, T_{d_-}, \ldots}]]
\]
with variables $T_{d_\pm}$ satisfying $\sigma_\infty(T_{d_\pm}) = \pm T_{d_\pm}$ for $r = d_+ + d_-$, and we have the following presentation for $\mathfrak{A}_Q := (\delta_{j_1} - 1)$:
\[
R_\infty/\mathfrak{A}_Q = W[[T_{d_+, T_{d_+}, T_{d_-}, \ldots}]]/\mathfrak{A}_Q \cong T_Q.
\]

Strictly speaking, we may have to modify slightly the isomorphism class $I_n$ of tuples for each $n$ to achieve this presentation (see the argument around (6.6) in the proof of the following Theorem 6.5).

Since $T^Q/(t - \gamma^h)T^Q \cong T_Q$, we can lift, as is well known, the above presentation over $W$ and the involution $\sigma_\infty$ to that of $T^Q$ over $A$ to obtain:
\[
(6.2) \quad \Lambda[[T_{d_+, T_{d_+}, T_{d_-}, \ldots}]]/\mathfrak{A}_Q \Lambda[[T_{d_+, T_{d_+}, T_{d_-}, \ldots}]] \cong T^Q,
\]
where $\sigma_\infty(T_{d_\pm}) = \pm T_{d_\pm}$ intact. We write simply $\mathcal{R} = \mathcal{R}_\infty := \Lambda[[T_{d_+, T_{d_+}, T_{d_-}, \ldots}]]$.

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 $\sigma_n$, $f_j^{(\infty)}$ is an eigenvector of $\sigma_\infty$. Let $\mathcal{R} := \Lambda[[T_{d_+, T_{d_+}, T_{d_-}, \ldots}]]$ and define an involution $\sigma$ on $\mathcal{R}$ by $\sigma(T_i) = \pm T_i \Rightarrow \sigma(\varphi_i^{(\infty)}) = \pm \varphi_i^{(\infty)}$. Choose $\varphi_i \in \mathcal{R}$ such that $f_j^{(\infty)} \bmod (t - \gamma^h) = f_j^{(\infty)}$ and $g_j \in T = T^\theta$ such that $g_j \bmod (t - \gamma^h)$ giving the image of $f_j^{(\infty)}$ in $T^\theta$. We impose that these $f_j$ and $g_j$ are made of eigenvectors of the involution. By sending $T_i = f_i$ to $g_i$, we have $\mathcal{R}/\mathfrak{A}_Q \mathcal{R} \cong T, \mathcal{R}^+/\mathfrak{A}_Q \mathcal{R} = T^\theta, \mathcal{R}/(t - \gamma^h) = R_\infty$ and $\mathcal{R}^+/\mathcal{R}/(t - \gamma^h) = R_\infty^+$.\]

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

Set
\[
(6.3) \quad S := W[[\Delta]] = \lim_n W[\Delta/\Delta^{p^n}] = \lim_n W[\Delta_n]
\]
for the $p$-profinite group $\Delta = \lim_\rightarrow \Delta_n \cong \mathbb{Z}_p^r$ with $\Delta = \Delta^+ \times \Delta^-$ and $A$ be a local $S$-algebra. Thus by identifying $\Delta/\Delta^{p^n}$ with $\Delta_n$, we have the identification $S = W[[S_1, \ldots, S_r]]$. The image $S_n := W_n[\Delta_n] (W_n = W/p^nW)$ of $S$ in $R_n$ is a local complete intersection and hence Gorenstein. Recall that the ordering of (Q3) is given as $Q^-_m := \{q_1, \ldots, q_r\}$ and $Q^+_m := \{q_{r+1} = q_1^+, \ldots, q_r = q_r^+\}$. We now write $s_j^{\pm}$ for the generator of $\Delta$ corresponding to $\delta_{j_1}^{\pm}$.\]
Definition 6.3. Write $s_{ij}^\pm$ for the generator of $\Delta_\pm$ corresponding to $\delta_{ij}^\pm$. Then define $S_j^+ = s_j^+ - 1$ and $S_j^- := s_j^- - (s_j^-)^{-1}$. Thus $\sigma_\infty(S_j^\pm) = \pm S_j^\pm$.

For the ideal $A_0 := \ker(W[\Delta_+] \to W_n[\Delta_+])$ for $W_n := W/p^n W$, we put

$$A_n = A_0 + ((s_1^\pm)^{p^n} - 1, \ldots, (s_r^\pm)^{p^n} - 1) \subset S$$

as an $S$-ideal. Then $A_n$ is stable under $\sigma$, and $A_n := \ker(S \to W_n[\Delta/p^n])$. Via the natural projection $\Delta \to \Delta_{Q_m}$ sending $s_j^\pm$ to $\delta_{ij}^\pm$, we get $A_{Q_m} = \ker(S \to W[\Delta_{Q_m}])$.

For $Q \in S$, recall $r_- = \lfloor Q^- \rfloor$ with

$$Q^- := \{ q \in Q \mid q \text{ is inert in } F/Q \} \quad \text{and} \quad Q^+ := \{ q \in Q \mid q \text{ is split in } F/Q \}.$$

Proposition 6.4. If $p \nmid h_F$, then $r_\pm = r_\mp + 1$, $d_+ = 0$ and $r_\mp = 1$. In particular $t_Q = \tilde{t}_Q$.

If further $p \nmid h_F h_{F(\varphi^-)}$, we have $r_- = 0$ (so, $d_\mp = 1$). Therefore we have a presentation $T = \Lambda[[T_\pm]]/(S_\pm)$ for $T_\pm = T_\pm^+$ and $S_\pm = S_\pm^+$ if $p \nmid h_F h_{F(\varphi^-)}$.

Proof. By construction, we have $R/(S_1^+, \ldots, S_r^+, S_1^-, \ldots, S_r^-) \cong T$, and $R/R(\sigma - 1)R$ has dimension $d_+ + \dim \Lambda = d_+ + 2$, since $R = \Lambda[T_1^+, \ldots, T_r^+, T_1^-, \ldots, T_r^-]$ and $R(\sigma - 1)R = (T_1^-, \ldots, T_r^-)$.

Suppose that $\sigma$ acts non-trivially on $S$; so, $r_- > 0$. Then $S/S(\sigma - 1)S \cong \Lambda[[S_1^+, \ldots, S_r^+]]$ has dimension $r_+ + 2$, since $S = \Lambda[[S_1^+, \ldots, S_r^+, S_1^-, \ldots, S_r^-]]$. The morphism $\text{Spec}(R) \to \text{Spec}(S)$ is finite flat; so, the induced morphism $\text{Spec}(R/R(\sigma - 1)R) = \text{Spec}(R)^{\sigma = 1} \to \text{Spec}(S)^{\sigma = 1} = \text{Spec}(S/S(\sigma - 1)S)$ is finite. Therefore

$$d_+ + 2 = \dim \text{Spec}(R/R(\sigma - 1)R) \leq \dim \text{Spec}(S/S(\sigma - 1)S) = r_\mp + 2.$$

Thus we have $d_+ \leq r_\mp$ and hence $d_\pm \geq r_\mp$ (because of $d_+ + d_- = d = r_\mp + r_\mp$).

Suppose $p \nmid h_F = [Cp]$, by Proposition 5.3, we have $r_\mp = \dim \text{Sel}_S^+(\chi \omega) = 1$. If $d_\mp > 0$, we have $0 < d_\mp \leq r_\pm = 1$, we have $d_\pm = r_\pm + 1$ and $d_\mp = r_\mp$. Then we get

$$T_\pm^+ \cap S = R(\sigma - 1)R \cap S \supset S(\sigma - 1)S = (S_1^+, \ldots, S_r^-).$$

This means $(T_1^+, \ldots, T_r^+, S_1^+) \supset (S_1^+, \ldots, S_r^-, S_1^+)$ and $T/T(\sigma - 1)T = R/(T_1^+, \ldots, T_r^+, S_1^+)$, and hence

$$2 > \dim T/T(\sigma - 1)T = \dim R/(T_1^+, \ldots, T_r^+, S_1^+) = \dim \Lambda[[T_1^+, \ldots, T_r^+]/(T_1^+, \ldots, T_r^+, S_1^+)] \geq r_\mp + 2 - (d_\mp + r_\pm) \geq 2.$$

The last inequality follows from the fact that the height of $(T_1^+, \ldots, T_r^+, S_1^+)$ is less than or equal to $d_\pm + 1 = r_\mp + r_\pm = r$ by [CRT, Theorem 13.5]. This is a contradiction. Therefore, we have $d_\pm = 0$, and from $d_\pm + d_- = r_\mp + r_\pm$, we get $d_- = 1 + r_\mp$. If further $p \nmid h_{F(\varphi^-)}$, by Proposition 5.4, we have $r_- = 0$.

Now we would like to prove

Theorem 6.5. Suppose (h1−6) and that the family $Q$ satisfies (Q0−9). Let $Q \in S$ or $Q = \emptyset$. Then the following two assertions holds.

1. the $T_\pm^+$-module $T_\pm^Q$ is generated by a single element over $T_\pm^Q$.

2. the rings $T_\pm$ and $T_\pm^Q$ are both local complete intersection over $\Lambda$ with presentation $T / \Lambda[[T_\mp]]/(S_\mp)$ and $T_\pm^Q / \Lambda[[T_\pm^Q]]/(S_\pm)$ such that $\sigma$ fixes $S_\pm$ and $\sigma(T_\pm) = -T_\mp$. More generally, for $Q \in S$, the rings $T_\pm^Q$ and $T_\mp^Q$ are local complete intersection.

Proof. By (Q9), $\sigma$ is compatible with the projective system of tuples

$$((R_n, \alpha), R_n, (f_1, \ldots, f_r), \sigma_n) \in \mathcal{I}_n.$$
Let \( I_\infty = R(\sigma - 1)R = RR_- \). Note that \( r_\pm := |Q_\pm| \) is independent of \( Q \) by Corollary 6.2.

Let \( S_\Lambda = S \otimes_W \Lambda = \Lambda[\Delta] \). Then plainly \( S_\Lambda \) is flat over \( S_\Lambda^1 := S_{\Lambda}^0 \), and \( R_- \) is generated over \( R_+ \) by a single element \( \delta \) with \( \sigma(\delta) = -\delta \). By Proposition 6.4, we have \( R = \Lambda[\langle T_- \rangle] \) and \( T^Q_\Lambda = \Lambda[\langle T_- \rangle]/(s_{\Lambda}^1 - 1) \). If a power series \( \Phi(T_-) \) is fixed by \( \sigma \), by equating the coefficients of the identity:

\[
\Phi(T_-) = \sigma(\Phi(T_-)) = \Phi(-T_-),
\]

we find that \( \Phi \) is actually a power series of \( (T_2) \). Thus the fixed part \( R_+ := R^G \) for \( G = \{\text{id}, \sigma_\infty\} \) is still a power series ring, and we have \( R_+ = \Lambda[\langle T_2 \rangle] \). Since \( T^Q_\Lambda = \Lambda[\langle T_2 \rangle]/(s_{\Lambda}^1 - 1) \) and \( T_- \) is the surjective image of \( R_- \). Since \( R_- \) is generated by one element \( \delta \) over \( R_+ \) (which can be given by \( T_- \)), its image \( T_- \) in \( T \) is generated by one element \( \theta \) over \( T_+ \). This proves the assertion (1) for \( Q = \emptyset \) and the assertion (2) for \( T \) and \( T_+ \).

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

\[
(6.6) \quad ((R_n, \alpha), R_{Q,n}, (f_1, \ldots, f_r), \sigma_n, \phi_n) \in \mathcal{I}_n
\]

for \( R_{Q,n} = R_n/(p^n + A_Q)R_n \). Then by the same argument, we get

\[
T^Q_\Lambda \cong \lim_{n \geq n_0} R_{Q,n} = R_\infty/A_Q.
\]

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

We now prove (2). Since \( d_- = 1 = r r_- = 0 \) and \( r_+ = 1 \) by Proposition 6.4, we can write \( Q^+ = Q_m^+ = \{q = q_1\} \) and \( Q^- = Q_m^- = \emptyset \). Recall \( \delta_\Lambda = S \otimes_W \Lambda = \Lambda[\Delta] \), and write \( s_{\Lambda}^1 = 1 + S_+ \) for the basis \( \Delta \) corresponding to \( \lim_{m} \delta_q \). Since \( d_- = 1, R_+ = \Lambda[\langle T_2 \rangle] \), and \( s_Q = A_Q \cap \Lambda \) is generated by \( s_{\Lambda}^1 \), \( T^Q_\Lambda = R_+/A_QR_+ \) is a local complete intersection (e.g., [CRT, Exercise 18.1]). Similarly, \( T^Q_\Lambda = \Lambda[\langle T_- \rangle]/(s_{\Lambda}^1 - 1) \) is a local complete intersection. \( \square 

Here is an example.

**Example 6.6.** We consider \( \Lambda[\langle T_- \rangle] \) and \( S_+ = T^2 - T \) for \( T = t - 1 \). Then if one specializes \( T \) to 0, we have

\[
W[[T_-]]/(1 + S_+)^{p^n} - 1) = W[[T_-]]/(1 + T^2)^{p^n} - 1) \mapsto W[[T_-]]/(T^2) \times \prod_{1 \neq \zeta \in \mu_{p^n}(\mathbb{Q}_p)} W[\zeta][\sqrt{\zeta} - 1]
\]

with

\[
W[[T_-]]/(1 + S_+)^{p^n} - 1, T_-) = W[[T_-]]/(1 + T^2)^{p^n} - 1, T_-) \cong W/((1 - \varpi)^{p^n} - 1).
\]

This tells us that \( T_Q/(T_Q(\sigma - 1)T_Q) = W \) for all \( Q \) even if \( Q^+_m \neq \emptyset \) consistent with Chevalley’s theorem.

If one specializes \( T \) to a non-zero non-unit \( \varpi \in W \), we have

\[
W[[T_-]]/(1 + S_+)^{p^n} - 1) = W[[T_-]]/(1 + T^2 - \varpi)^{p^n} - 1) \mapsto \prod_{\zeta \in \mu_{p^n}(\mathbb{Q}_p)} W[\zeta][\sqrt{\varpi + \zeta} - 1]
\]

with

\[
W[[T_-]]/(1 + S_+)^{p^n} - 1, T_-) = W[[T_-]]/(1 + T^2 - \varpi)^{p^n} - 1, T_-) \cong W/((1 - \varpi)^{p^n} - 1).
\]

Without specializing, we have

\[
\Lambda[[T_-]]/(1 + S_+)^{p^n} - 1) = \Lambda[[T_-]]/(1 + T^2 - T)^{p^n} - 1) \mapsto \prod_{\zeta \in \mu_{p^n}(\mathbb{Q}_p)} \Lambda[\zeta][\sqrt{T + \zeta} - 1]
\]

with

\[
\Lambda[[T_-]]/(1 + S_+)^{p^n} - 1, T_-) = \Lambda[[T_-]]/(1 + T^2 - T)^{p^n} - 1, T_-) \cong \Lambda/((1 - T)^{p^n} - 1).
\]
In this setting, for exterior derivative \( f \mapsto df \) having values in

\[
t_{\mathcal{R}/(1+S_+)^{p^n-1}/\Lambda} \cong t_{\mathcal{TQ}/\Lambda}^* = m_{\mathcal{TQ}}/(m_{\mathcal{TQ}}^2 + m_{\Lambda}) \cong m_{\mathcal{TQ}}/(m_{\mathcal{TQ}}^2 + m_{W}),
\]

we have

\[
d((1+S_+)^{p^n-1}) - 1 = d((1 + T_2^2 - T)p^{n-1}) = p^n(1 + T_2^2 - T)p^{n-1}(2T_-dT_2 - dT).
\]

Taking \( n = 0 \), this shows that \( T_-dT_2 \in m_{\Lambda} \) and hence \( dS_+ = 2T_-dT_2 = 0 \) in the cotangent space \( t_{\mathcal{TQ}/\Lambda}^* \). For \( Q \neq \emptyset \), we still have \( T_-dT_2 = 0 \) as \( T_- \in m_{\mathcal{TQ}} \) and \( m_{\mathcal{TQ}} \) kills \( t_{\mathcal{TQ}/\Lambda}^* \) and hence compatible with the vanishing \( \text{Sel}_0(\mathcal{T}) = 0 = \text{Sel}_Q(\mathcal{T}) \).

**Proof of Theorem A:** By Proposition 6.4, hereafter we write

\[
(6.7) \quad \mathcal{R} = \Lambda[[T_-]] \text{ and } \mathcal{S} = \Lambda[[S_+]].
\]

The primes giving rise to \( S_+ \) is made of \( Q_m^+ \); so, \( Q_m^+ = \{q_m^+\} \) is a singleton by Proposition 6.4. By Proposition 6.4, we find \( d_- = r_- + 1 = 1 \), which shows by Theorem 6.5 that \( \mathcal{R}_- \) is generated by \( T_- \) over \( \mathcal{R}_+ \) and hence \( \mathcal{R}_+ = \mathcal{T}_- \) is generated by its image \( \theta \). This proves the assertion (2). The assertion (1) follows directly from Theorem 6.5 as \( d_- = 1 \).

### 7. Proof of Corollary B

Throughout this section, we assume (h1–6). We now start the proof of Corollary B. In this proof, we give an argument which applies to \( T \) and \( T/(t - \gamma^k) \) at the same time. So we write for simplicity \( T \) for either \( T \) or \( T/(t - \gamma^k) \) (choosing \( k > 0 \)), and put

\[
B = \begin{cases} 
\Lambda/(t - \gamma^k) \cong W & \text{if } T = T/(t - \gamma^k) \quad (k > 0), \\
\Lambda & \text{if } T = T,
\end{cases}
\]

which is the base subalgebra of \( T \). Similarly, we write \( \mathcal{A} \) for \( \mathcal{R} \) or \( \mathcal{R}_\infty \) according as \( T = T \) or \( T = T/(t - \gamma^k) \). By Proposition 6.4, \( \mathcal{A}_+ := \mathcal{A}^\vartheta = B[[T_-]]^{p^k} = B[[T^2_-]] \). To make notation simple, we just write \( Y \) for \( T^2_- \); so, \( \mathcal{A}_+ = B[Y] \). We have a unique variable \( S_+ = S_+^1 \).

**Proposition 7.1.** Let \( \varepsilon \) be a generator of \( O^\times \) (a fundamental unit). Then we have

\[
S_+ = f(Y)
\]

with a power series \( 0 \neq f \in B[[Y]] \). Moreover, if \( B = \Lambda \), we have \( (f(0)) = ((\varepsilon) - 1) \) as principal ideals of \( \Lambda \), and hence

\[
\mathcal{T}ab := T/I = T_+/I_+ \cong \begin{cases} 
\Lambda/(\langle \varepsilon \rangle - 1) & \text{if } B = \Lambda, \\
W/(\gamma^k \log_{p}(\vartheta)/\log_{p}(1+p) - 1) & \text{if } B = \Lambda/(t - \gamma^k),
\end{cases}
\]

where \( I = T(\sigma - 1)T \) and \( X_+ = X^\vartheta \) for \( X = T, I \). In particular, \( f \) is a non-unit.

**Proof.** We have \( S_+ \in \mathcal{A}_+ \); so, \( S_+ = f \) in \( B[[Y]] \), and we find, if \( B = \Lambda \),

\[
\Lambda/(\langle \varepsilon \rangle - 1) = T/(T(\sigma - 1)T) = \mathcal{A}/((T_- + (f)) = \Lambda/(f(0)).
\]

This shows \( (f(0)) = ((\varepsilon) - 1) \).

**Proposition 7.2.** Let the notation be as above, and recall \( \mathcal{T}ab := T/I \) for \( I = T(\sigma - 1)T \). Then we have an isomorphism of \( \mathcal{T}ab \)-modules

\[
\Omega_{\mathcal{T}/B} \otimes_{\mathcal{T}} \mathcal{T}ab \cong I/I^2 \cong \begin{cases} 
\Lambda/(\langle \varepsilon \rangle - 1) & \text{if } B = \Lambda, \\
W/(\gamma^k \log_{p}(\vartheta)/\log_{p}(1+p) - 1) & \text{if } B = \Lambda.
\end{cases}
\]

**Proof.** By Proposition 7.1, \( f(0) = 0 \) if \( k = 0 \) and \( B = W \). First suppose either \( B = \Lambda \) or \( B = W \) with \( k > 0 \). Then the annihilator of \( I = T(\sigma - 1)T \) regarded as an ideal of \( T \) is the zero ideal (since \( T \otimes_B \text{Frac}(B) = I \otimes_B \text{Frac}(B) \)).

We have an exact sequence (e.g., [CRT, Theorem 25.2]):

\[
I/I^2 \xrightarrow{\sim} \Omega_{\mathcal{T}/B} \otimes_{\mathcal{T}} \mathcal{T}ab \to \Omega_{\mathcal{T}ab/B} \to 0.
\]
Since \( \Omega_{T^\Lambda/B} = 0 \) by Proposition 7.1, the map \( i \) is injective and \( \Omega_{T/B \otimes T} T_{\text{ab}} \cong I/I^2 \). From the exact sequence

\[
0 \to (S_+)/(S_+)^2 = T \cdot dS_+ \to T \cdot dT_- \to \Omega_{T/B} \to 0,
\]
tensoring with \( T_{\text{ab}} = T/I \) over \( T \), we get another exact sequence

\[
T_{\text{ab}} \cdot dS_+ \to T_{\text{ab}} \cdot dT_- \to (\Omega_{T/B \otimes T} T_{\text{ab}}) = (I/I^2) = 0.
\]

We may assume that \( f(T_-) = (\varepsilon - 1) + \sum_{a=1}^{\infty} a_a Y^a \). Since \( \frac{df(Y)}{dT_-} = 2a_j(T_-)^{2a - 1} \), we find

\[
df(Y)|_{T_- = 0} = (\frac{df(Y)}{dT_-})|_{T_- = 0} = T_{\text{ab}} \cdot dT_-
\]

This shows

\[
\Omega_{T/B \otimes T} T_{\text{ab}} \cong I/I^2 \cong \begin{cases} \Lambda/((\varepsilon) - 1) & \text{if } B = \Lambda, \\ W/(\gamma^k \log(\varepsilon)/\log_{p+1}(1+p) - 1) & \text{if } B = W, \end{cases}
\]
as desired. \( \square \)

Thus we have again proven Theorem A in a slightly different way:

**Corollary 7.3.** The ideal \( I = T(\sigma - 1)T \) is a principal ideal generated by an element \( \theta \in T^- \), and \( T^+ \) is a local complete intersection over \( B \).

**Proposition 7.4 (B. Mazur).** Assume (h1–6). We have a canonical identity \( \Omega_{T/\Lambda} \cong \text{Sel}_{Q}(\text{Ad}(\rho))^{\vee} \).

**Proof.** By Theorem 2.1, the couple \((\underline{T}, \rho)\) is the universal couple for the deformation functor \( D \). Thus we need to prove \( \Omega_{R/\Lambda} \cong \text{Sel}_{Q}(\text{Ad}(\rho)) \) for the universal couple \((R, \rho)\) of \( D \). For the Teichmüller lift \( \psi \) of \( \det(\overline{\mathbf{d}}) \) and \( \kappa : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \Lambda^\times \) given by \( \kappa(\sigma) = \psi(\sigma) \log_{p}(r_{\sigma}(\tau))/\log_{p}(1+p) \) for \( t = 1 + T \) and the \( p \)-adic cyclotomic character \( \nu_{p} \), the couple \((\Lambda, \kappa)\) is the universal couple of minimally ramified deformation outside \( p \). Since \( \det(\rho) \) for \( \rho \in D(A) \) is such a deformation, we have a unique \( W \)-algebra homomorphism \( \iota_{A} : \Lambda \to A \) such that \( \iota_{A} \circ \kappa = \det(\rho) \). In this way, \( R \) is a \( \Lambda \)-algebra by \( \iota_{R} \), and the unique \( W \)-algebra homomorphism \( \pi : R \to A \) with \( \pi \circ \rho \cong \rho \) becomes \( \Lambda \)-algebra homomorphism under the \( \Lambda \)-algebra structure induced by \( \iota_{A} \). Note also that the identification \( R \cong \mathbb{T} \) in Theorem 2.1 sends the \( \Lambda \)-algebra structure of \( R \) to the weight \( \Lambda \)-algebra structure of \( T \).

Let \( X \) be a finite \( R \)-module. Then \( R[X] \) is an object in \( CL_{W} \), and write \( \Phi(A) \) for \( A \in CL_{W} \), the set of deformations with values in \( GL_{2}(A) \) giving rise elements in \( D(A) \); so, \( D(A) = \Phi(A) \). For each \( \rho \in D(R[X]) \) with \( \rho \mod X = \rho_{R} \), we have \( \iota_{R}(X) : \Lambda \to R[X] \). Since \( \rho \mod X = \rho_{R} \), \( \iota_{R}(X) \mod X = \iota_{R} \) (so, the \( R \)-module structure combined with \( \iota_{R} \) induces the \( \Lambda \)-module structure on \( X \)), and the projection of \( \pi : R \to R[X] \) inducing \( \rho \) is a \( \Lambda \)-derivation of \( R \) with values in \( X \).

We consider the \( W \)-algebra homomorphism \( \xi : R \to R[X] \) with \( \xi \mod X = \text{id} \). Then we can write \( \xi(\rho) = \rho \otimes d_{\xi}(\rho) \) with \( d_{\xi}(\rho) \in X \). By the definition of the product, we get \( d_{\xi}(\rho_{R}) = rd_{\xi}(\rho_{R}) + r'd_{\xi}(\rho) \) and \( d_{\xi}(W) = 0 \). Thus \( d_{\xi} \) is an \( W \)-derivation, i.e., \( d_{\xi} \in \text{Der}_{W}(R, X) \). For any derivation \( d : R \to X \) over \( W \), \( r \mapsto r \otimes d(r) \) is obviously an \( W \)-algebra homomorphism, and we get

\[
\{ \pi \in \Phi(\{R[X]\}) | \pi \mod X = \rho \}/ \cong_X \equiv \{ \xi \in \text{Hom}_{\Lambda, \text{alg}}(R, R[X]) | \xi \mod X = \text{id} \}/ \cong_X \equiv \text{Der}_{\Lambda}(R, X) \equiv \text{Hom}_{R}(\Omega_{R/\Lambda}, X),
\]
where \( "\cong_X" \) is conjugation under \((1 \oplus M_{n}(X)) \cap GL_{2}(R[X])\).

Let \( \pi \) be the deformation in the left-hand-side of (7.4). Then we may write \( \pi(\sigma) = \rho(\sigma) \otimes u'_{\pi}(\sigma) \).
We see

\[
\rho(\sigma \tau) \otimes u'_{\pi}(\sigma \tau) = \rho(\sigma) \otimes u'_{\pi}(\sigma)(\rho(\tau) \otimes u'_{\pi}(\tau)) = \rho(\sigma \tau) \otimes (\rho(\sigma)u'_{\pi}(\tau) + u'_{\pi}(\sigma)\rho(\tau)),
\]
and we have

\[
u'_{\pi}(\sigma \tau) = \rho(\sigma)u'_{\pi}(\tau) + u'_{\pi}(\sigma)\rho(\tau).
\]
Since \(C, R, A, f \mid T \delta\) we have Corollary 7.5. as desired. □

Proof of Corollary B: Since the assertion (1) is already proven in Propositions 7.1 and 7.2, we prove the assertions (2) and (3). By the presentation \(\Lambda[[T_-]]/(S_+) = T\), we have an exact sequence

\[ 0 \to TdS_+ \to TdT_- \to \Omega_{T/\Lambda} \to 0.\]

We apply a theorem of Tate [MR70, A.3] for \((C, R, A, f_1, g_1) = (T, \Lambda, \Lambda[[T_-]] = R, S_+, T_- - \theta)\) under the notation there. Define \(\delta \in R \otimes_{\Lambda} T = T[[T_-]]\) by \(S_+ = \delta(T_- - \theta)\), and write \(\beta : R \otimes_{\Lambda} T = T[[T_-]] \to T\) for the projection; so, \(\beta(T_-) = \theta\). Then we have \(dS_+ = \delta dT_- + (T_- - \theta) d\delta\). This shows \(\Omega_{T/\Lambda} = T/\beta(\delta))\). Thus by Proposition 7.4, \(\text{Sel}_Q(Ad(\rho))^\vee \cong \mathbb{T}/L\) with \(L := \beta(\delta)\) is cyclic over \(T\). Since \(\delta_{T/\Lambda} = (L)\) for the different \(\delta_{T/\Lambda}\) by [MR70, Appendix], \(L\) is a non-zero divisor as \(T\) is reduced.

\[
\Lambda = \prod_{v \mid \infty} \mathbb{Q}_v = \mathbb{Q}_\infty, \quad R = \prod_{v \mid \infty} \mathbb{Z}_v = \mathbb{Z}_\infty.
\]

Then we obtain this result replacing the \(R\)-module \(X\) in the above proof of Mazur’s theorem by a \(T/I\)-module \(X\). The last assertion is the restatement of (7.3) and Corollary 7.3. □
and free of finite rank over $\Lambda$. Then $\Omega_{T/A} \otimes_T \langle \theta \rangle$ is in turn isomorphic to $I/I^2 \cong \langle \theta \rangle$ by Corollary 7.3 and Proposition 7.2. Thus $\langle \beta(\delta) \rangle \otimes_T \langle \theta \rangle \cong \Omega_{T/A} \otimes_T \langle \theta \rangle \cong \langle \theta \rangle$; so, $(\beta(\delta)) \subset \langle \theta \rangle$. Indeed, evaluating $S_+ = \delta(T_+ - \theta)$ at $T_+ = 0$, we get $\langle \theta \rangle - 1 = -\delta(0)\theta$. By Corollary 7.5, we have $\Omega_{T/A} \otimes_T \langle \theta \rangle \cong \text{Sel}_Q(\text{Ad}(\text{Ind}^G_\mathfrak{L} \Phi))^\vee$.

References

Books


Articles


Preprints/reprints authored by Hida cited above are available at www.math.ucla.edu/~hida.