Advanced Studies in Pure Mathematics *99*, *20XX*
Title
pp. 1–61

Cyclicity of adjoint Selmer groups and fundamental units

Haruzo Hida

Abstract.

We study the universal minimal ordinary Galois deformation $\rho_{\mathbb{T}}$ of an induced representation $\mathrm{Ind}_F^{\mathbb{Q}}\varphi$ from a real quadratic field F with values in $\mathrm{GL}_2(\mathbb{T})$. By Taylor–Wiles, the universal ring $\mathbb{T}$ is isomorphic to a local ring of a Hecke algebra. Combining an idea of Vatsal–Cho [CV03] with a modified Taylor–Wiles patching argument in [H17], under mild assumptions, we show that the Pontryagin dual of the adjoint Selmer group of $\rho_{\mathbb{T}}$ is canonically isomorphic to $\mathbb{T}/(L)$ for a non-zero divisor $L \in \mathbb{T}$ which is a generator of the different $\mathfrak{d}_{\mathbb{T}/\Lambda}$ of $\mathbb{T}$ over the weight Iwasawa algebra $\Lambda = W[[T]]$ inside $\mathbb{T}$. Moreover, defining $\langle\varepsilon\rangle := (1+T)^{\log_p(\varepsilon)/\log_p(1+p)}$ for a fundamental unit ε of the real quadratic field F, we show that the adjoint Selmer group of $\mathrm{Ind}_F^{\mathbb{Q}}\Phi$ for the (minimal) universal character Φ deforming φ is isomorphic to $\Lambda/(\langle\varepsilon\rangle - 1)$ as Λ-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 $(p) = \mathfrak{p}\mathfrak{p}'$ in O with $\mathfrak{p} \neq \mathfrak{p}'$. In our article [H17], we have studied the cyclicity question 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. Though the fundamental idea of applying the patching method of Taylor–Wiles to the cyclicity problem is similar to [H17], the execution is different, and we show that the annihilator L of the adjoint Selmer group is always non-trivial having the factor $\langle\varepsilon\rangle - 1$ as it covers $\Lambda/(\langle\varepsilon\rangle - 1) \neq 0$ ($\Leftarrow T|(\langle\varepsilon\rangle - 1)$). We discuss this point more after stating Theorem A.

Let ς be the generator of $\mathrm{Gal}(F/\mathbb{Q})$. Take an anticyclotomic branch character $\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \overline{\mathbb{Q}}^\times$. Here ϕ "anti-cyclotomic" means that for

1991 *Mathematics Subject Classification.* primary 11R23, 11F25, 11F33, 11F80; secondary 11F11, 11G18, 11F27.

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

any lift $\widetilde{\varsigma} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with $\widetilde{\varsigma}|_F = \varsigma$, we have $\phi(\widetilde{\varsigma}\tau\widetilde{\varsigma}^{-1}) = \phi(\tau)^{-1}$ for all $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/F)$. Regard it as a finite order idele character $\phi : F_{\mathbb{A}}^\times/F^\times \to \overline{\mathbb{Q}}^\times$ such that $\phi(x^\varsigma) = \phi^{-1}(x)$. Often we find a finite order character φ of $F_{\mathbb{A}}^\times/F^\times$ such that $\phi = \varphi^-$, where $\varphi^-(x) = \varphi(x)\varphi(x^\varsigma)^{-1}$. Note that $\phi = \varphi^- \Leftrightarrow \phi|_{\mathbb{A}^\times} = 1$. Suppose

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

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

1. $\mathbf{h}$ is a reduced algebra flat over Λ interpolating p-ordinary Hecke algebras of varying level Np^{r+1}, weight $k+1 \geq 2$ and Neben characters;
2. Each prime $P \in \mathrm{Spec}(\mathbf{h})$ has a unique (continuous) Galois representation $\rho_P : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\kappa(P))$ for the residue field $\kappa(P)$ of P;
3. ρ_P restricted to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ (the p-decomposition group) is isomorphic to an upper triangular representation whose quotient character is unramified.

By (2), each localization $\mathbb{T}$ of $\mathbf{h}$ has a mod p representation $\overline{\rho} = \rho_{\mathfrak{m}_\mathbb{T}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F})$ for the residue field $\mathbb{F} = \mathbb{T}/\mathfrak{m}_\mathbb{T}$. If $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}$ for the reduction $\overline{\varphi}$ modulo p of φ, we have an involution $\sigma \in \mathrm{Aut}(\mathbb{T}/\Lambda)$ such that $\sigma \circ \rho_P \cong \rho_P \otimes \chi$ for $\chi := \left(\frac{F/\mathbb{Q}}{}\right)$. For a subscheme $\mathrm{Spec}(A) \subset$

$\mathrm{Spec}(\mathbb{T})$ stable under σ, we put $A_\pm := \{x \in A | \sigma(x) = \pm x\}$. Then $A_+ \subset A$ is a subring and A_- is an A_+-module.

We prove

Theorem A: *Let* $\mathrm{Spec}(\mathbb{T})$ *be a connected component of* $\mathrm{Spec}(\mathbf{h})$ *associated to the induced Galois representation* $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$ *for the reduction* $\overline{\varphi}$ *of* φ *modulo* $\mathfrak{m}_W$ *for the maximal ideal* $\mathfrak{m}_W$ *of* W*. Suppose* (h1–6)*. Then the following two equivalent assertions hold:*

(1) *The rings* $\mathbb{T}$ *and* $\mathbb{T}_+$ *are both local complete intersections free of finite rank over* Λ*.*
(2) *The* $\mathbb{T}$*-ideal* $I = \mathbb{T}(\sigma - 1)\mathbb{T} \subset \mathbb{T}$ *is principal and is generated by a non-zero-divisor* $\theta \in \mathbb{T}_- = \mathbb{T}_-$ *with* $\theta^2 \in \mathbb{T}_+$*. The element* θ *generates the* $\mathbb{T}_+$*-module* $\mathbb{T}_-$ *which is free over* $\mathbb{T}_+$*, and* $\mathbb{T} = \mathbb{T}_+[\theta]$ *is free of rank* 2 *over* $\mathbb{T}_+$*.*

The relative different $\mathfrak{d}_{\mathbb{T}/\mathbb{T}_+}$ for $\mathbb{T}$ over $\mathbb{T}_+$ (defined by Tate in [MR70, Appendix]) is generated by θ as a $\mathbb{T}$-ideal.

The implication (1) $\Rightarrow$ (2) follows from a ring theoretic lemma [H17, Lemma 10.4], and the converse is a consequence of [H17, Lemma 5.5] because $\mathbb{T}/(\theta) \cong \mathbb{T}_+/(\theta^2)$ 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 than Theorem A is given in [CV03, Theprem 2.1 (2)] in the case where $\mathfrak{f} = 1$.

The condition (h4) combined with $(p) = \mathfrak{p}\mathfrak{p}^\varsigma$ implies an assumption for "$R = \mathbb{T}$" theorems of Wiles and Taylor et al [Wi95] and [TW95]:

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

and the main reason for us to assume (h4) is the use of the "$R = \mathbb{T}$" theorem for the minimal universal deformation ring R of $\overline{\rho}$ (see Theorem 2.1). The universal representation $\rho_{\mathbb{T}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(R) = \mathrm{GL}_2(\mathbb{T})$ is obtained patching together the representations ρ_P associated to arithmetic primes $P \in \mathrm{Spec}(\mathbb{T})$. The condition (W) is equivalent to the condition that the representation $\overline{\rho}$ is not of the form $\mathrm{Ind}_M^{\mathbb{Q}} \xi$ for a quadratic field $M \neq F$ and a character $\xi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \mathbb{F}^\times$ by Frobenius reciprocity. Then the implication: (h4) $\Rightarrow$ (W) follows from [H15, Proposition 5.2]. For a deformation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(A)$ of $\overline{\rho}$, we let $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ act on $\mathfrak{sl}_2(A)$ by $x \mapsto \rho(\tau)x\rho(\tau)^{-1}$ and write this 3-dimensional representation as $Ad(\rho)$.

We actually prove a stronger fact than (1) which asserts that $\mathbb{T} \cong \Lambda[[T_-]]/(S_+)$ and $\mathbb{T}_+ \cong \Lambda[[T_-^2]]/(S_+)$ for a one variable power series ring $\Lambda[[T_-]]$ over Λ with $S_+ \in \Lambda[[T_-^2]]$ and θ is given by the image of T_- in

$\mathbb{T}$. Here the variables satisfy $\sigma(T_-) = -T_-$ and $\sigma(S_+) = S_+$. This switching of the sign $\sigma(T_-)/T_- = -\sigma(S_+)/S_+$ (see Proposition 6.4) appears innocuous but has a substantial effect (of forcing non-trivial ramification of $\mathbb{T}$ over $\mathbb{T}_+$) resulting the infinity of the Selmer group $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))$ without exception. This is something like the exceptional zero phenomenon observed in [MTT] as the divisibility of the standard p-adic L-function of GL(2) by the cyclotomic variable but in our case, the weight variable T always divides the characteristic ideal of the Pontryagin dual of the Selmer group (as described in Corollary B below).

In [H17] dealing with the anticyclotomic Iwasawa module over an imaginary quadratic field, we studied the universal deformation ring of an induced representation of the imaginary quadratic field. Writing $(\mathcal{R}, \mathcal{T}, \tau \in \mathrm{Aut}(\mathcal{T}/\Lambda))$ in the imaginary case for the objects corresponding to $(R, \mathbb{T}, \sigma)$ in the real case as above, we have two significant differences in the situation:

(1) $\mathrm{Spec}(\mathcal{T})$ has a big component $\mathrm{Spec}(\mathcal{T}_{cm})$ with $\dim \mathcal{T}_{cm} = \dim \Lambda$ fixed by the involution τ corresponding to σ (existence of large CM components);
(2) Under an appropriate hypothesis similar to (h1–6), we proved in the imaginary case that $\mathbb{T} \cong \Lambda[[T_-]]/(S_-)$ with $\tau(T_-) = -T_-$ and $\tau(S_-) = -S_-$ (so, no switching of the sign).

The fact (1) asserting to have a big closed subscheme $\mathrm{Spec}(\mathcal{T}_{cm})$ fixed by τ forces $\tau(S_-) = -S_-$ (see [H17, Example 4.9 and Theorem 4.10]), and the non-triviality of the Selmer group is equivalent to $(T_-) \supsetneq (S_-)$ (i.e., non-triviality of the Selmer group would be rare when we vary the prime p in the imaginary case). Write $\overline{\chi}$ for the mod p quadratic character corresponding to F and $\overline{\omega}$ for the mod p Teichmüller character. A technical reason for the switch of sign in the real case is a consequence of the fact (by Kummer theory) that the dual Selmer group $\mathrm{Sel}^{\perp}(\overline{\chi\omega})$ is one dimensional when F is real, while $\mathrm{Sel}^{\perp}(\overline{\chi\omega})$ vanishes for imaginary F (see Proposition 6.4 and its proof), as long as the class number of F is prime to p.

Though the use of the patching argument to study cyclicity was first done in [H17] and again in this paper, to pin down the subtle difference of the two cases described above, we go through each step of the argument in detail. There is one more case of expected cyclicity where the residual representation is a modulo p reduction of an exceptional Artin representation (of tetrahedral, octahedral and icosahedral type). In this case, we do not have the involution (stemming from reducibility of $Ad(\overline{\rho})$ in the dihedral case), and the setting is again different.

Under (h5), the universal deformation of the character $\overline{\varphi}$ for deformations with prime-to-p-conductor $\mathfrak{c}$ is isomorphic to $\Lambda/(\langle\varepsilon\rangle - 1)$ for a fundamental unit $\varepsilon \in O^\times$ (see [CV03] and Corollary 2.3 in the text). We write $\Phi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to (\Lambda/(\langle\varepsilon\rangle - 1))^\times$ for the universal character.

By a theorem of Mazur (Theorem 7.4), the differential module $\Omega_{\mathbb{T}/\Lambda}$ has a description as (the Pontryagin dual of) an adjoint Selmer group, and by Theorem A, one can prove cyclicity of $\Omega_{\mathbb{T}/\Lambda}$ as $\mathbb{T}$-module. After stating a cyclicity result on our Selmer group (and $\Omega_{\mathbb{T}/\Lambda}$), we recall our definition of the Selmer group which could be slightly smaller than the usual Greenberg's Selmer groups when either φ^- is unramified at p or $\varphi^-|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ has order 2. Sine $\mathbb{T}$ is shown to be a quotient of $\Lambda[[T_-]]$ 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*

$$\langle\varepsilon\rangle - 1 := t^{\log_p(\varepsilon)/\log_p(1+p)} - 1 \ (t = 1 + T \in \Lambda)$$

for a fundamental unit ε of F. Then we have

1. *a canonical isomorphism $(\theta)/(\theta)^2 \cong \mathbb{T}/(\theta) \cong \Lambda/(\langle\varepsilon\rangle - 1)$ for $\theta \in \mathbb{T}$ in* Theorem A (2),
2. *the Pontryagin dual module $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))^\vee$ of the adjoint Selmer group $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))$ is cyclic isomorphic to $\mathbb{T}/(L)$ as $\mathbb{T}$-modules for a non-zero divisor L with $(\theta) \supset (L)$,*
3. *The Selmer group $\mathrm{Sel}_{\mathbb{Q}}(Ad(\mathrm{Ind}_F^{\mathbb{Q}}\Phi))^\vee \cong \Lambda/(\langle\varepsilon\rangle - 1) \cong \mathbb{T}/(\theta)$ which has natural surjection of $\mathbb{T}$-modules from $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))$.*

Moreover we have $\mathfrak{d}_{\mathbb{T}/\Lambda} = (L)$ for the different $\mathfrak{d}_{\mathbb{T}/\Lambda}$ relative to the extension $\mathbb{T}/\Lambda$, and the above surjection comes from the natural surjection $\mathbb{T}/\mathfrak{d}_{\mathbb{T}/\Lambda} \to \mathbb{T}/\mathfrak{d}_{\mathbb{T}/\mathbb{T}_+}$ by the transition formula $\mathfrak{d}_{\mathbb{T}/\Lambda} = \mathfrak{d}_{\mathbb{T}/\mathbb{T}_+}\mathfrak{d}_{\mathbb{T}_+/\Lambda}$ of different with $\mathbb{T}/\mathfrak{d}_{\mathbb{T}/\mathbb{T}_+} = \mathbb{T}/(\theta) \cong \Lambda/(\langle\varepsilon\rangle - 1)$.

By Corollary B, the p-adic L-function L always has zero at $t = 1 \Leftrightarrow T = 0$, and if $L = \langle\varepsilon\rangle - 1$ up to units, the derivative $\frac{dL}{dt}|_{t=1}$ is equal to $\log_p(\varepsilon)/\log_p(1+p)$ up to units (which plays the role of the $\mathcal{L}$-invariant in the cyclotomic theory of Mazur–Tate–Teitelbaum). In any case, $\log_p(\varepsilon)/\log_p(1+p)$ is a factor of $\frac{dL}{dt}|_{t=1}$.

By the "$R = T$" theorem, $\mathbb{T}$ is the minimal universal deformation ring for $\mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}$, and this implies

$$\begin{aligned}\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))^\vee \otimes_{\mathbb{T}} \mathbb{T}/(\theta) &\cong \mathrm{Sel}_{\mathbb{Q}}(Ad(\mathrm{Ind}_F^{\mathbb{Q}}\Phi)) \\ &\cong (\theta)/(\theta^2) \cong \mathbb{T}/(\theta) \cong \Lambda/(\langle\varepsilon\rangle - 1),\end{aligned}$$

which means $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))^\vee \cong \mathbb{T}/\mathfrak{a}$ by Nakayama's lemma. To show that the annihilator $\mathfrak{a}$ in $\mathbb{T}$ is principal and is equal to the different $\mathfrak{d}_{\mathbb{T}/\Lambda}$, the theory of dualizing modules of complete intersection rings given by Tate in the appendix to [MR70] plays an important role (see Section 7). Plainly for each irreducible component $\mathrm{Spec}(\mathbb{I})$ of $\mathrm{Spec}(\mathbb{T})$, the adjoint Selmer group $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{I}}))^\vee$ (which is equal to $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))^\vee \otimes_{\mathbb{T}} \mathbb{I}$) is again cyclic isomorphic to $\mathbb{I}/(L_p(Ad(\rho_p))$ for $L_p(Ad(\rho_p)) \in \mathbb{I}$ interpolating the adjoint L-values (see [H16, §6.4.4 and 6.5.3]). Thus by Corollary B, the projection of L to $\mathbb{I}$ coincides with $L_p(Ad(\rho_{\mathbb{I}}))$ up to units in $\mathbb{I}$.

We could speculate whether cyclicity of the Selmer group remains true under some milder ramification assumption (i.e., studying non-minimal deformations). For example, we could ask what happens if we allow ramification at a single prime l outside Np. If $l \not\equiv 1 \mod p$, even if we allow ramification at l, the p-ordinary deformation ring of prime-to-p level Nl and the minimal deformation ring of level N are equal; so, there is no difference of the corresponding Selmer groups. Therefore we can assume that $l \equiv 1 \mod p$. Writing $\mathrm{Sel}^{(l)}_{\mathbb{Q}}(Ad(\mathrm{Ind}^{\mathbb{Q}}_F \Phi))$ for the new Selmer group with l-ramification allowed, we would have factorization $\mathrm{Sel}^{(l)}_{\mathbb{Q}}(Ad(\mathrm{Ind}^{\mathbb{Q}}_F \Phi)) = \mathrm{Sel}^{(l)}_{\mathbb{Q}}(\chi) \oplus \mathrm{Sel}^{(l)}_{\mathbb{Q}}(\mathrm{Ind}^{\mathbb{Q}}_F \Phi^-)$, where (Λ_l, Φ) is the universal pair deforming $\overline{\varphi}$ unramified outside $l\mathfrak{cp}\infty$ and the Selmer group $\mathrm{Sel}^{(l)}_{\mathbb{Q}}(\chi)$ is isomorphic to $Cl_F(l) \otimes_{\mathbb{Z}} \Lambda_l^\vee$ for the ray class group $Cl_F(l)$ modulo l and the Pontryagin dual $\Lambda_l^\vee$ of Λ_l. It is likely that, under suitable adjustments of our assumptions, the induced part $\mathrm{Sel}^{(l)}_{\mathbb{Q}}(\mathrm{Ind}^{\mathbb{Q}}_F \Phi^-)$ would remain cyclic (non-trivial). If l is a Taylor–Wiles prime of our choice, one can prove that $Cl_F(l)$ is trivial if $p \nmid h_F$, and hence one expects the cyclicity of the entire adjoint Selmer group to be true under suitable assumptions. If $Cl_F(l) \otimes_{\mathbb{Z}} \mathbb{Z}_p \neq 1$, plainly the cyclicity for $\mathrm{Sel}^{(l)}_{\mathbb{Q}}(Ad(\mathrm{Ind}^{\mathbb{Q}}_F \Phi))$ fails (and hence also for the adjoint Selmer group l-ramification allowed). Since the structure of $Cl_F(l)$ depends highly on ε under the assumption of $p \nmid h_F$, the problem of cyclicity would be subtler if one allows extra ramification (and hence we do not touch upon this question in the present paper).

As a historical note, an intricate relation between the fundamental unit and the congruence between Hecke eigenforms with real Neben type was first noticed by Shimura in [Sh72]. A close relation of $\mathbb{T}$ and ε is then conjectured in [H98] predicting that $\theta = \sqrt{\langle \epsilon \rangle - 1}$, and by Corollary B, we come close to the conjecture under (h1–6). Just before the theory of $\mathbf{h}$ was established in [H86a] and [H86b], we had given an example of a geometrically irreducible quadratic extension of Λ appearing as a quotient of $\mathbf{h}$ (see [H85, (10a,b)]). The fact $2 | \dim_{\mathbb{K}} \mathrm{Frac}(\mathbb{I})$ ($\mathbb{K} = \mathrm{Frac}(\Lambda)$)

for each irreducible component $\mathrm{Spec}(\mathbb{I})$ of $\mathrm{Spec}(\mathbb{T})$ is proven in [BD15], and there is another series of examples of different nature in [Ra14] and [KR15] with degree arbitrarily large over Λ. Assuming $N = D$ for the discriminant D of the real quadratic field F and the Gorenstein property for the subring $\mathbb{T}_+$ of $\mathbb{T}$, Cho and Vatsal [CV03] proved $2|\dim_{\mathbb{K}} \mathrm{Frac}(\mathbb{I})$ essentially, after some work by the author [H85] and [H98], though in [CV03], the phenomenon: $\mathbb{I} \neq \Lambda$ is not much emphasized.

Keeping in mind the fact that the Galois representation $\rho_{\mathbb{T}}$ is the universal minimal ordinary deformation of $\overline{\rho}$ (by the "$R = T$" theorem of Taylor–Wiles), here we define the adjoint Selmer groups for a minimal ordinary deformation ρ in the following way (assuming (h1) and (h3)). For such a deformation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}) \to \mathrm{GL}_2(A)$ of $\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$ with $\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} = \left(\begin{smallmatrix} \epsilon & * \\ 0 & \delta \end{smallmatrix}\right)$ and $(\epsilon \bmod \mathfrak{m}_A) = \overline{\varphi}$, regarding $Ad(\rho)$ as a subspace of trace zero A-linear endomorphisms $\mathrm{End}_A(\rho)$ which contains $\mathrm{Hom}_A(\delta, \epsilon) = \{T \in Ad(\rho) | T(\epsilon) = 0\} \subset \mathrm{End}_A(\rho)$ canonically. Put $F_+(\rho) := \mathrm{Hom}_A(\delta, \epsilon)$. Then $F_+(\rho)$ is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ which acts on it by the character ϵ/δ. Then we have a filtration $F_+(\rho) \subset F_-(\rho) \subset Ad(\rho)$ so that the Galois action on $F_-(\rho)/F_+(\rho)$ is trivial. Thus $F_+(\rho)$ (resp. $F_-(\rho)$) is made of upper nilpotent (resp. upper triangular) matrices under a choice of the basis of $Ad(\rho)$ so that ρ is upper triangular over $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ with quotient character is given by δ. 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

$$\begin{aligned} &\mathrm{Sel}(Ad(\rho)) \\ &= \mathrm{Ker}(H^1(\mathbb{Q}, Ad(\rho)^*) \to \frac{H^1(\mathbb{Q}_p, Ad(\rho)^*)}{F_+^- H^1(\mathbb{Q}_p, Ad(\rho)^*)} \times \prod_{l \nmid p} H^1(I_l, Ad(\rho)^*), \end{aligned}$$

where $F_+^- H^1(\mathbb{Q}_p, Ad(\rho)^*)$ is defined as follows. The classes in the submodule $F_+^- H^1(\mathbb{Q}_p, Ad(\rho)^*)$ come from local cocycles with values in $F_-(\rho)^*$ whose restriction to I_p have values in $F_+(\rho)^*$. Thus we have

$$F_+^- H^1(\mathbb{Q}_p, Ad(\rho)^*) = \mathrm{Res}^{-1}_{D_p/I_p}(H^1(I_p, F_+(\rho)^*)) \subset H^1(\mathbb{Q}_p, F_-(\rho)^*).$$

From the cohomology sequence attached to the exact sequence $F_+(\rho^*) \hookrightarrow Ad(\rho)^* \twoheadrightarrow Ad(\rho)^*/F_+(\rho)^*$, we can replace $\frac{H^1(\mathbb{Q}_p, Ad(\rho)^*)}{F_+^- H^1(\mathbb{Q}_p, Ad(\rho)^*)}$ 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 $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ as $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ normalizes

I_p; so, we have
(0.1)
$$\mathrm{Sel}(Ad(\rho)) = \mathrm{Ker}(H^1(\mathbb{Q}, Ad(\rho)^*) \to H^1(I_p, \frac{Ad(\rho)^*)}{F_+(\rho)^*}) \times \prod_{l \nmid p} H^1(I_l, Ad(\rho)^*).$$

Contents

§1. Big Hecke algebra

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

We consider the following traditional congruence subgroups

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

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

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

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

Let $\Gamma_Q^{(p)}$ 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

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

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

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

which is canonically isomorphic to the maximal p-abelian quotient of $\Gamma_0(Q)/\Gamma_1(Q)$ independent of the exponent r. If $Q = \emptyset$, we have $\Gamma_{Q,r} = \Gamma_0(Np^r)$, and if $q \not\equiv 1 \mod p$ for all $q \in Q$, we have $\Gamma_1(N_Q p^r) \subset \Gamma_{Q,r} = \Gamma_0(N_Q p^r)$ for $N_Q := N\prod_{q\in Q} q$.

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

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

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

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

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

We write the image $M^{\mathrm{ord}} := e(M)$ of the idempotent attaching the superscript "ord" (e.g., S_{k+1}^{ord}).

Fix a character ψ_0 modulo Np, and assume now $\psi_0(-1) = -1$. Let ω be the modulo p Teichmüller character. Recall the multiplicative group $\Gamma := 1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ and its topological generator $\gamma = 1 + p$. Then the Iwasawa algebra $\Lambda = W[[\Gamma]] = \varprojlim_n W[\Gamma/\Gamma^{p^n}]$ is identified with the power series ring $W[[T]]$ by a W-algebra isomorphism sending $\gamma \in \Gamma$ to $t := 1 + T$. As constructed in [H86a], [H86b] and [GME], we have a unique 'big' ordinary Hecke algebra $\mathbf{h}^Q$ (of level $\Gamma_{Q,\infty}$). We write $\mathbf{h}$ for $\mathbf{h}^\emptyset$.

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

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

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

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

sending $T(n)$ to $T(n)$ (and $U(l)$ to $U(l)$ for $l|Np$).

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

Lemma 1.1. *The Hecke algebra $\mathbf{h}^Q$ is flat over $\Lambda[\Delta_Q]$ with a canonical isomorphism: $\mathbf{h}^Q/\mathfrak{A}_{\Delta_Q}\mathbf{h}^Q \cong \mathbf{h}^\emptyset$ for the augmentation ideal $\mathfrak{A}_{\Delta_Q} \subset \Lambda[\Delta_Q]$.*

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

Since N_Q is cube-free, by [H13, Corollary 1.3], $\mathbf{h}^Q$ is reduced. Let $\mathrm{Spec}(\mathbb{I})$ be an irreducible component of $\mathrm{Spec}(\mathbf{h}^Q)$. Write $a(n)$ for the image of $T(n)$ in $\mathbb{I}$ (so, $a(p)$ is the image of $U(p)$). If a point P of $\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ kills $(t - \epsilon(\gamma)\gamma^k)$ with $1 \leq k \in \mathbb{Z}$ (i.e., $P((t - \epsilon(\gamma)\gamma^k)) = 0$), we call P an *arithmetic* point, and we write $\epsilon_P := \epsilon$, $k(P) := k \geq 1$ and $p^{r(P)}$ for the order of ϵ_P. If P is arithmetic, by (C2), we have a Hecke eigenform $f_P \in S_{k+1}(\Gamma_{Q,r(P)+1}, \epsilon\psi_k)$ such that its eigenvalue for $T(n)$ is given by $a_P(n) := P(a(n)) \in \overline{\mathbb{Q}}$ for all n. Thus $\mathbb{I}$ gives rise to a family $\mathcal{F} = \{f_P | \text{arithmetic } P \in \mathrm{Spec}(\mathbb{I})\}$ of Hecke eigenforms. We define a *p-adic analytic family of slope* 0 (with coefficients in $\mathbb{I}$) to be

the family as above of Hecke eigenforms associated to an irreducible component $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbf{h}^Q)$. We call this family slope 0 because $|a_P(p)|_p = 1$ for the p-adic absolute value $|\cdot|_p$ of $\overline{\mathbb{Q}}_p$ (it is also often called an ordinary family). This family is said to be analytic because the Hecke eigenvalue $a_P(n)$ for $T(n)$ is given by an analytic function $a(n)$ on (the rigid analytic space associated to) the p-profinite formal spectrum $\mathrm{Spf}(\mathbb{I})$. Identify $\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ with $\mathrm{Hom}_{W\text{-alg}}(\mathbb{I}, \overline{\mathbb{Q}}_p)$ so that each element $a \in \mathbb{I}$ gives rise to a "function" $a : \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p) \to \overline{\mathbb{Q}}_p$ whose value at $(P : \mathbb{I} \to \overline{\mathbb{Q}}_p) \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ is $a_P := P(a) \in \overline{\mathbb{Q}}_p$. Then a is an analytic function of the rigid analytic space associated to $\mathrm{Spf}(\mathbb{I})$. Taking a finite covering $\mathrm{Spec}(\widetilde{\mathbb{I}})$ of $\mathrm{Spec}(\mathbb{I})$ with surjection $\mathrm{Spec}(\widetilde{\mathbb{I}})(\overline{\mathbb{Q}}_p) \twoheadrightarrow \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$, abusing slightly the definition, we may regard the family $\mathcal{F}$ as being indexed by arithmetic points of $\mathrm{Spec}(\widetilde{\mathbb{I}})(\overline{\mathbb{Q}}_p)$, where arithmetic points of $\mathrm{Spec}(\widetilde{\mathbb{I}})(\overline{\mathbb{Q}}_p)$ are made up of the points above arithmetic points of $\mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$. The choice of $\widetilde{\mathbb{I}}$ is often the normalization of $\mathbb{I}$ or the integral closure of $\mathbb{I}$ in a finite extension of the quotient field of $\mathbb{I}$.

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

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

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

$$\text{(Gal}_q\text{)} \qquad \rho_{\mathbb{I}}([z, \mathbb{Q}_q]) \sim \begin{pmatrix} \alpha_q(z) & 0 \\ 0 & \beta_q(z) \end{pmatrix}$$

with characters α_q and β_q of $\mathbb{Q}_q^\times$ for $z \in \mathbb{Q}_q^\times$, where one of α_q and β_q is unramified (e.g., [MFG, Theorem 3.32 (2)] or [HMI, Theorem 3.75]). For each prime ideal P of $\mathrm{Spec}(\mathbb{I})$, writing $\kappa(P)$ for the residue field of P, we also have a semi-simple Galois representation $\rho_P : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\kappa(P))$ unramified outside $N_Q p$ such that $\mathrm{Tr}(\rho_P(\mathrm{Frob}_l))$ is given by $a(l)_P$ for all primes $l \nmid N_Q p$. If P is the maximal ideal $\mathfrak{m}_{\mathbb{I}}$, we write $\overline{\rho}$ for ρ_P which is called the residual representation of $\rho_{\mathbb{I}}$. The

residual representation $\overline{\rho}$ is independent of $\mathbb{I}$ as long as $\mathrm{Spec}(\mathbb{I})$ belongs to a given connected component $\mathrm{Spec}(\mathbb{T})$ of $\mathrm{Spec}(\mathbf{h}^Q)$. Indeed, $\mathrm{Tr}(\rho_P)$ mod $\mathfrak{m}_{\mathbb{I}} = \mathrm{Tr}(\overline{\rho})$ for any $P \in \mathrm{Spec}(\mathbb{T})$. If P is an arithmetic prime, we have $\det(\rho_P) = \epsilon_P \psi_k \nu_p^k$ for the p-adic cyclotomic character ν_p (regarding ϵ_P and ψ_k as Galois characters by class field theory). This is the Galois representation associated to the Hecke eigenform f_P (constructed earlier by Shimura and Deligne) if P is arithmetic (e.g., [GME, §4.2]).

We describe how to construct residue rings of $\mathbf{h}^Q$ whose Galois representation is induced from a quadratic field F (see [LFE, §7.6] and [HMI, §2.5.4]). Here we allow F to be imaginary also. We write ς for the generator of $\mathrm{Gal}(F/\mathbb{Q})$ as before. Let $\mathfrak{c}$ be the prime-to-p conductor of a character $\overline{\varphi}$ as in (h1–2). Put $\mathfrak{C} = \mathfrak{c} \cap \mathfrak{c}^\varsigma$. Assume that $\mathfrak{c}$ is a square free integral ideal of F with $\mathfrak{c} + \mathfrak{c}^\varsigma = O$ (i.e., (h2)). Since Q is outside N, Q is a finite set of rational primes unramified in $F/\mathbb{Q}$ prime to $\mathfrak{C}p$. Let Q^+ be the subset in Q made up of primes split in F. We choose a prime factor $\mathfrak{q}$ of q for each $q \in Q^+$ (once and for all), and put $\mathfrak{Q}^+ := \prod_{q \in Q^+} \mathfrak{q}$. We put $\mathfrak{C}_{Q^+} := \mathfrak{C} \prod_{q \in Q^+} q$. We simply write $\mathfrak{C}$ for $\mathfrak{C}_\emptyset$. Consider the ray class group $Cl(\mathfrak{a})$ (of F) modulo $\mathfrak{a}$ for an integral ideal $\mathfrak{a}$ of O, and put

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

On $Cl(\mathfrak{C}_{Q^+}p^\infty)$, the automorphism ς acts as an involution.

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

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

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

which c acts by -1). We have the projections

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

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

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

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

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

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

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

Theorem 1.3. *Suppose that* $\overline{\varphi}(\mathrm{Frob}_\mathfrak{q}) \neq \overline{\varphi}(\mathrm{Frob}_{\mathfrak{q}^\varsigma})$ *for all* $\mathfrak{q}|\mathfrak{Q}^+$. *Then we have a surjective* Λ*-algebra homomorphism* $\mathbf{h}^{Q^+} \twoheadrightarrow W[Z_{Q^+}]$ *such that*

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

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

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

Hereafter, we assume that F is a real quadratic extension over $\mathbb{Q}$ and that the residue field of W is given by $\mathbb{F} = \mathbb{T}/\mathfrak{m}_\mathbb{T}$. Let $\mathbb{T}$ be as in

Theorem A. We fix a weight $k \geq 0$. Let $\theta(\varphi) \in S_1(\Gamma_0(Np), \psi)$ for the corresponding theta series (see [HMI, Theorem 2.71]). Then $\psi = \psi_0$, where we define ψ_k to be given by $\psi_k = \chi\varphi|_{\mathbb{A}^\times}\omega^{-k}$ for the Teichmüller character. Recall the identity $\psi_k\nu_p^k \mod \mathfrak{m}_W = \det(\overline{\rho})$ for the p-adic cyclotomic character ν_p; so, ψ_0 is the Teichmüller lift of $\det(\overline{\rho})$. By the existence of a lift of Hasse invariant, we can find a Hecke eigenform $f \in S_{k+1}(\Gamma_0(Np), \psi_k)$ congruent to $\theta(\varphi)$ modulo p, and hence the Hecke algebra $\mathbb{T}_\emptyset = \mathbb{T}/(t-\gamma^k)\mathbb{T}$ (resp. $\mathbb{T}^Q/(t-\gamma^k)\mathbb{T}^Q$) is a local ring of $\mathbf{h}_{\emptyset,k,\psi_k}$ (resp. $\mathbf{h}_{Q,k,\psi_k}$).

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

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

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

Here are the conditions (D1–4):

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

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

$$\delta([p, \mathbb{Q}_p]) \equiv \varphi^\varsigma([p, \mathbb{Q}_p]) \mod \mathfrak{m}_A,$$

where we define $\varphi^\varsigma(\tau) := \varphi(\widetilde{\varsigma}\tau\widetilde{\varsigma}^{-1})$ for $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/F)$.

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

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

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

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

where

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

We may also impose another condition if necessary:

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

and consider the functor

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

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

By our choice of $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}$, we have $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q})} \cong \begin{pmatrix} \overline{\epsilon}_q & 0 \\ 0 & \overline{\delta}_q \end{pmatrix}$ for two local characters $\overline{\epsilon}_q, \overline{\delta}_q$ for all primes $q|N_Q p$. If $\overline{\delta}_p \neq \overline{\epsilon}_p$ and $\overline{\epsilon}_q(\mathrm{Frob}_q) \neq \overline{\delta}_q(\mathrm{Frob}_q)$ for all $q \in Q$, the functors $\mathcal{D}$, $\mathcal{D}^Q$, $\mathcal{D}_{k,\psi_k}$ and $\mathcal{D}_{Q,k,\psi_k}$ are representable by universal objects $(R, \boldsymbol{\rho}) = (R^\emptyset, \boldsymbol{\rho}^\emptyset)$, $(R^Q, \boldsymbol{\rho}^Q)$, $(R_\emptyset, \boldsymbol{\rho}_\emptyset)$ and $(R_Q, \boldsymbol{\rho}_Q)$, respectively (see [MFG, Proposition 3.30] or [HMI, Theorem 1.46 and page 186]).

Here is a brief outline of how to show the representability of $\mathcal{D}$. It is easy to check the deformation functor $\mathcal{D}^{\mathrm{ord}}$ only imposing (D1–2) is representable by a W-algebra R^{ord} . The condition (D4) is actually redundant as it follows from the universality of the Teichmüller lift and the conditions (D1–2). Since N is the prime-to-p conductor of $\det\overline{\rho}$ (h1–2) and p is unramified in $F/\mathbb{Q}$, if l is a prime factor of N, writing $\rho|_{I_l}^{ss}$ for its semi-simplification of ρ over I_l, we see from (h3) that $(\rho|_{I_l})^{ss} = \epsilon_l \oplus \delta_l$ for two characters ϵ_l and δ_l (of order prime to p) with δ_l unramified and $\epsilon_l \equiv \psi|_{I_l} \mod \mathfrak{m}_A$. Thus by the character $\epsilon_N := \prod_{l|N}\epsilon_l$ of $I_N = \prod_{l|N} I_l$, A is canonically an algebra over the group algebra $W[I_N]$. Then R is given by the maximal residue ring of R^{ord} on which I_N acts by

$\psi_{1,N} = \prod_{l|N} \psi|_{I_l}$; so, $R = R^{\mathrm{ord}} \otimes_{W[I_N],\psi_{1,N}} W$, where the tensor product is taken over the algebra homomorphism $W[I_N] \to W$ induced by the character $\psi_{1,N}$. Since $\overline{\rho}$ is an induced representation, $\overline{\rho}|_{I_l}$ is semi-simple and $\overline{\rho}|_{I_l} = \overline{\epsilon}_l \oplus \overline{\delta}_l$. Similarly one can show the representability of $\mathcal{D}^Q$ and $\mathcal{D}_{Q,k,\psi_k}$.

Let $\mathbb{T}$ be the local ring of $\mathbf{h} = \mathbf{h}^\emptyset$ as in Theorem B whose residual representation is $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$. The ring $\mathbb{T}$ 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 $\mathbb{T}$, we need to specify in the deformation problem the unramified quotient character and for $\mathbb{T}$, the residue class of $U(p)$-eigenvalue given by $\overline{\varphi}(\mathfrak{p}^\varsigma)$. The unramified quotient is unique if φ ramifies at $\mathfrak{p}$. However if φ is unramified at p, we need to fix the resideu 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

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

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

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

See [Wi95, Theorem 3.3] and [DFG04] for a proof (see also [HMI, §3.2] or [MFG, Theorem 3.31] for details of how to lift the results in [Wi95] to the (bigger) ordinary deformation ring with varying determinant character). These references require the assumption (W) which is absolute irreducibility of $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/M)}$ for $M = \mathbb{Q}[\sqrt{p^*}]$ with $p^* := (-1)^{(p-1)/2}p$.

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

automorphisms σ_Q of R_Q and R^Q. We identify R and $\mathbb{T}$ now by Theorem 2.1; in particular, we have an automorphism $\sigma = \sigma_\emptyset \in \mathrm{Aut}(\mathbb{T})$ as above.

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

$$\mathbb{T}_\pm := \{x \in \mathbb{T} | x^\sigma = \pm x\}.$$

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

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

and

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

Let $F_{\mathfrak{cp}}$ be the maximal abelian p-extension of F inside the ray class field of conductor $\mathfrak{cp}$. Put $C = C_\emptyset := \mathrm{Gal}(F_{\mathfrak{cp}}/F)$. Similarly, write $F_{\mathfrak{cp}^\infty}$ for the maximal p-abelian extension inside the ray class field over F of conductor $\mathfrak{cp}^\infty$. Put $H := \mathrm{Gal}(F_{\mathfrak{cp}^\infty}/F)$. Note that $F_{\mathfrak{cp}^\infty}/F$ is a finite extension as F is real. Then $\mathcal{D}_F$ is represented by $(W[C], \Phi)$ where $\Phi(x) = \varphi(x)x$ for $x \in C$, where φ is the Teichmüller lift of $\overline{\varphi}$ with values in $W^\times$. Similarly $\mathcal{D}_F^\infty$ is represented by $W[H]$.

In Definition 1.2, we defined H as the anticyclotomic p-primary part $\mathrm{Gal}(K^-/F)$ of the Galois group of the ray class field K of conductor $(\mathfrak{c} \cap \mathfrak{c}^\varsigma)p^\infty$. The present definition is a bit different from the one given there. However, the present H is isomorphic to the earlier $\mathrm{Gal}(K^-/F)$ by sending τ to $\tau^{(1-\varsigma)/2} = \sqrt{\tau c \tau^{-1} c^{-1}}$ (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* $\lambda \mapsto \mathrm{Ind}_F^{\mathbb{Q}} \lambda$ *induces an isomorphism* $\mathcal{D}_F \cong \mathcal{D}_T^{\mathcal{G}}$ *and* $\mathcal{D}_F^\infty \cong \mathcal{D}^{\mathcal{G}}$, *where*

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

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

Proof. Since the proof is essentially the same for the two cases, we only deal with $\mathcal{D}_F^\infty \cong \mathcal{D}^{\mathcal{G}}$. By [DHI98, Lemma 3.2], we have $\rho\otimes\chi\cong\rho$ for $\rho\in\mathcal{D}(A)$ is equivalent to having $\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/F)\to A^\times$ such that $\rho\cong \mathrm{Ind}_F^{\mathbb{Q}}\lambda$. We can choose λ so that λ has conductor a factor of $\mathfrak{cp}^\infty$ by (D4) and $C(\det(\rho))|Np^\infty$. Then λ is unique by (D2–3) and (h3). Thus we get the desired isomorphism. Q.E.D.

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

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

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

$$\boldsymbol{\rho}^Q|_{I_q}=\left(\begin{smallmatrix}\boldsymbol{\delta}_q & 0\\ 0 & \boldsymbol{\delta}'_q\end{smallmatrix}\right) \tag{2.1}$$

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

We can choose infinitely many distinct Qs with $\overline{\rho}(\mathrm{Frob}_q)$ for $q\in Q$ having two distinct eigenvalues. We split $Q=Q^+\sqcup Q^-$ so that $Q^\pm=\{q\in Q|\chi(q)=\pm1\}$. By choosing an eigenvalue $\overline{\alpha}_q$ of $\overline{\rho}(\mathrm{Frob}_q)$ for each $q\in Q$, we have a unique Hecke algebra local factor $\mathbb{T}_Q$ of the Hecke algebra $\mathbf{h}_{Q,k,\psi_k}$, whose residual representation is isomorphic to $\overline{\rho}$ and $U(q) \mod \mathfrak{m}_{\mathbb{T}^Q}$ is the chosen eigenvalue $\overline{\alpha}_q$. This follows in the following way: We choose $\overline{\alpha}_q$ for $q\in Q^-$. For $q\in Q^+$, we choose a unique prime factor $\mathfrak{q}|q$ so that $\overline{\varphi}(\mathrm{Frob}_{\mathfrak{q}^c})=\overline{\alpha}_q$. In this way, we get a local factor $\mathbb{T}^Q$ of h^Q which covers the local ring $W[Z_Q]$ as in [H17, Corollary 1.3]. Define

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

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

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

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

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

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

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

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

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

$CL_W \to SETS$ by

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

Hereafter we simply write Z_Q for Z_{Q^+}. Then plainly $\mathcal{D}^\infty_{F,Q}$ is representable by $W[Z_Q] \cong W[H_Q]$. 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*

$$R^Q/I^Q \cong W[H_Q] \quad \textit{and} \quad R^Q/I^Q \otimes_\Lambda \Lambda/(T) \cong W[C_Q]$$

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

§3. The Taylor–Wiles system

In their proof of Theorem 2.1, Taylor and Wiles used an infinite family $\mathcal{Q}$ of finite sets Q made of primes $q \equiv 1 \mod p$ outside N. We can choose infinitely many distinct Qs with $\overline{\rho}(\mathrm{Frob}_q)$ for $q \in Q$ having two distinct eigenvalues. Recall $\chi = \left(\frac{F/\mathbb{Q}}{\ }\right)$ and $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$ for real quadratic F as in Theorem A. We split $Q = Q^+ \sqcup Q^-$ so that $Q^\pm = \{q \in Q | \chi(q) = \pm 1\}$. By fixing a weight $k \geq 0$ and choosing an eigenvalue

$\overline{\alpha}_q$ of $\overline{\rho}(\mathrm{Frob}_q)$ for each $q \in Q$, we have a unique local factor $\mathbb{T}^Q$ (resp. $\mathbb{T}_Q$) of the Hecke algebra $\mathbf{h}^Q$ (resp. $\mathbf{h}_{Q,k,\psi_k}$) as in [H17, (1.7)], whose residual representation is isomorphic to $\overline{\rho}$ and $U(q) \mod \mathfrak{m}_{\mathbb{T}_Q}$ is the chosen eigenvalue $\overline{\alpha}_q$.

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

The Hecke algebra $h_k(\Gamma_Q, \psi; W)$ has an involution coming from the action of the normalizer of Γ_Q. Taking $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma \equiv \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \mod D^2$ and $\gamma \equiv 1 \mod (N_Q/D)^2$, put $\eta := \gamma \left(\begin{smallmatrix} D & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then η normalizes Γ_Q, and the action of η satisfies $\eta^2 = 1$, $\eta U(l)\eta^{-1} = \chi(l)U(l)$ for each prime $l | N_Q/D$ and $\eta T(l)\eta^{-1} = \chi(l)T(l)$ for each prime $l \nmid N_Q$ (see [MFM, (4.6.22), page 168]). Thus the conjugation of η induces on $\mathbb{T}_Q$ an involution compatible with σ_Q under the canonical surjection $R_Q \twoheadrightarrow \mathbb{T}_Q$. Note that $\sigma_Q(U(q)) = -U(q)$ for $q \in Q^-$; so, the role of $\overline{\alpha}_q$ will be played by $-\overline{\alpha}_q = \overline{\beta}_q$. This affects on the inertia action of Δ_q at q by $\delta_q \mapsto \delta_q^{-1}$ for $q \in Q^-$, because the action is normalized by the choice of $\overline{\alpha}_q$ with $\overline{\alpha}_q \equiv U(q) \mod \mathfrak{m}_{\mathbb{T}_Q}$ (see Lemma 3.1 and [HMI, Theorem 3.74]). Since $\mathbb{T}^Q$ is the local component of the big Hecke algebra of tame level Γ_Q whose reduction modulo $t - \gamma^k$ is $\mathbb{T}_Q$, again $\mathbb{T}^Q$ has involution σ_Q induced from η. We write $\mathbb{T}^Q_+$ (resp. $\mathbb{T}^+_Q$) for the fixed subring of $\mathbb{T}^Q$ (resp. $\mathbb{T}_Q$) under the involution.

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

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

made of the following objects:

(1) $R_{n,m} := \mathbb{T}_{Q_m}/(p^n, \delta_q^{p^n}-1)_{q\in Q_m}\mathbb{T}_{Q_m}$ for each $0 < n \le m$. Since the integer m in the system (3.1) is determined by n, we have written it as $m(n)$. In [HMI, page 191], $R_{n,m}$ is defined to be the image of $\mathbb{T}_{Q_m}$ in $\mathrm{End}_{W[\Delta_n]}(M_{n,m})$ for $M_{n,m} := M_{Q_m}/(p^n, \delta_q^{p^n}-1)_{q\in Q_m}M_{Q_m}$, but by our choice $M_Q = \mathbb{T}_Q$, the image is identical to $\mathbb{T}_{Q_m}/(p^n, \delta_q^{p^n}-1)_{q\in Q_m}\mathbb{T}_{Q_m}$. An important point is that $R_{n,m}$ is a finite ring whose order is bounded independent of m (by (Q0) below).
(2) $\widetilde{R}_{n,m} := R_{n,m}/(\delta_q - 1)_{q\in Q_m}$,
(3) $\alpha_n : W_n[\Delta_n] \to R_{n,m}$ for $W_n := W/p^nW$ is a $W[\Delta_n]$-algebra homomorphism for $\Delta_n = \Delta_{n,Q_m}$ induced by the $W[\Delta_{Q_m}]$-algebra structure of $\mathbb{T}_{Q_m}$ (making $R_{n,m}$ finite $W[\Delta_n]$-algebras).
(4) $(f_1 = f_1^{(n)}, \dots, f_r = f_r^{(n)})$ is an ordered subset of the maximal ideal of $R_{n,m}$.

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

(Q0) $M_{Q_m} = \mathbb{T}_{Q_m}$ is free of finite rank d over $W[\Delta_{Q_m}]$ with d independent of m (see Lemma 1.1 and the remark after the lemma and [HMI, (tw3), pages 190 and 199] taking $M_{Q_m} := \mathbb{T}_{Q_m}$).
(Q1) $|Q_m| = r \ge \dim_{\mathbb{F}} \mathcal{D}_{Q_m,k,\psi_k}(\mathbb{F}[\epsilon])$ for r independent of m [HMI, Propositions 3.29 and 3.33], where ϵ is the dual number with $\epsilon^2 = 0$. (Note that $\dim_{\mathbb{F}} \mathcal{D}_{Q_m,k,\psi_k}(\mathbb{F}[\epsilon])$ is the minimal number of generators of R_{Q_m} over W.)
(Q2) $q \equiv 1 \mod p^m$ and $\overline{\rho}(\mathrm{Frob}_q) \sim \begin{pmatrix} \overline{\alpha}_q & 0 \\ 0 & \overline{\beta}_q \end{pmatrix}$ with $\overline{\alpha}_q \ne \overline{\beta}_q \in \mathbb{F}$ if $q \in Q_m$ (so, $|\Delta_q| =: p^{e_q} \ge p^m$). Actually as we will see later in Lemma 4.1, we can impose a slightly stronger condition: $q \equiv 1 \mod Cp^m$ for $C = N_{F/\mathbb{Q}}(\mathfrak{c})$.
(Q3) The set $Q_m = \{q_1, \dots, q_r\}$ is ordered so that
- $\Delta_{q_j} \subset \Delta_{Q_m}$ is identified with $\mathbb{Z}/p^{e_{q_j}}\mathbb{Z}$ by $\delta_{q_j} \mapsto 1$; so, $\Delta_n = \Delta_{n,Q_{m(n)}} = (\mathbb{Z}/p^n\mathbb{Z})^{Q_{m(n)}}$,
- $\Delta_n = (\mathbb{Z}/p^n\mathbb{Z})^{Q_{m(n)}}$ is identified with $\Delta_{n+1}/\Delta_{n+1}^{p^n}$ which is $((\mathbb{Z}/p^{n+1}\mathbb{Z})/p^n(\mathbb{Z}/p^{n+1}\mathbb{Z}))^{Q_{m(n)}}$,

- the diagram

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

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

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

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

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

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

(Q8) We have $R_{Q_m} \cong \mathbb{T}_{Q_m}$ by the canonical morphism, and $R_{Q_m} \cong R_\infty/\mathfrak{A}_{Q_m} R_\infty$ for the ideal $\mathfrak{A}_{Q_m} := ((1 + S_j)^{|\Delta_{q_j}|} - 1)_{j=1,2,\dots r}$ of $W[[S_1, \dots, S_r]]$ 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 $\{S_1, \dots, S_r\}$ in (Q6) corresponding to q.

Lemma 3.1. *Let $\chi := \left(\frac{F/\mathbb{Q}}{\ }\right)$ as before. Then the involution σ_{Q_m} on $\mathbb{T}_{Q_m}$ acts on $\delta_q|_{I_q}$ (the image of $s_q = 1 + S_q$) for $q \in Q_m$ by $\sigma_{Q_m}(\delta_q|_{I_q}) = (\delta_q|_{I_q})^{\chi(q)}$. In particular, the ideal $(p^n, \delta_q^{p^n} - 1)_{q \in Q_m}$ of $\mathbb{T}_{Q_m}$ is stable under σ_{Q_m}, and the involution σ_{Q_m} induces an involution $\sigma = \sigma_n$ of $R_n = R_{n,m}$.*

Proof. For each $q \in Q$, by (2.1), the restriction of $\boldsymbol{\rho}^Q$ to the inertia group $I_q \subset \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ has the form $\begin{pmatrix} \boldsymbol{\delta}_q & 0 \\ 0 & \boldsymbol{\delta}_q^{-1} \end{pmatrix}$ and the choice of the eigenvalue $\overline{\alpha}_q$ determines the character $\boldsymbol{\delta}_q$ (i.e., $\overline{\alpha}_q$-eigenspace of $\overline{\rho}(\mathrm{Frob}_q)$ is the image of $\boldsymbol{\delta}_q^{-1}$-eigenspace in $\overline{\rho}$ by (2.3); see also [MFG,

Theorem 3.32 and its proof] or [HMI, Theorem 3.75]). By tensoring χ, $\overline{\alpha}_q$ is transformed to $\chi(q)\overline{\alpha}_q = \overline{\beta}_q$, and hence $\boldsymbol{\delta}_q$ will be transformed to $\boldsymbol{\delta}_q^{\chi(q)}$ under σ_{Q_m}. Thus, we get the desired result as the canonical morphism $R_{Q_m} \to \mathbb{T}_{Q_m}$ is $W[\Delta_{Q_m}]$-linear.

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

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

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

Set

$$\mathcal{S} := \Lambda[[\boldsymbol{\Delta}]] = \varprojlim_n W[\boldsymbol{\Delta}/\boldsymbol{\Delta}^{p^n}] = \varprojlim_n W[\Delta_n] \tag{3.2}$$

for the p-profinite group $\boldsymbol{\Delta} = \varprojlim_n \Delta_n \cong \mathbb{Z}_p^r$ with $\boldsymbol{\Delta} = \boldsymbol{\Delta}_+ \times \boldsymbol{\Delta}_-$ and A be a local $\mathcal{S}$-algebra. By identifying $\boldsymbol{\Delta}/\boldsymbol{\Delta}^{p^n}$ with Δ_n, we get an identification $\mathcal{S} = W[[S_1, \dots, S_r]]$. The image $\mathcal{S}_n := W_n[\Delta_n]$ ($W_n = W/p^nW$) of $\mathcal{S}$ in R_n is a local complete intersection and hence Gorenstein. We assume that the ordering of (Q3) is given as $Q_m^- := \{q_1, \dots, q_{r_-}\}$ and $Q_m^+ := \{q_{r_-+1} =: q_1^+, \dots, q_{r_+}^+ = q_r\}$.

§4. Taylor–Wiles primes

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

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

Here is a lemma due to A. Wiles [Wi95, Lemma 1.12] 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 $K_1 = \overline{\mathbb{Q}}^{\mathrm{Ker}\, Ad}$ (the splitting field of $Ad = Ad(\overline{\rho})$). Since $Ad \cong \overline{\chi} \oplus \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$, we have $K_1 = F(\varphi^-)$.

Lemma 4.1. *Assume* (W). *Pick* $0 \neq x \in \mathrm{Ker}(\beta_Q)$, *and write*

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

as an element of $\mathrm{Hom}_{\mathrm{Gal}(K_1(\mu_p)/\mathbb{Q})}(\mathrm{Gal}(\mathbb{Q}^{(QNp)}/K_1(\mu_p)), Ad^*(1))$ *for the restriction of the cocycle representing* x *to* $\mathrm{Gal}(\mathbb{Q}^{(QNp)}/K_1(\mu_p))$. *Let* $\widetilde{\rho}$ *be the composite of* $\overline{\rho}$ *with the projection* $\mathrm{GL}_2(\mathbb{F}) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F})$, *and pick a positive integer* C *which is a product of primes* $l \neq p$ *split in* $F/\mathbb{Q}$. *Then,* f_x *factors through* $\mathrm{Gal}(\mathbb{Q}^{(Np)}/K_1(\mu_p))$, *and there exists* $\sigma_x \in \mathrm{Gal}(\mathbb{Q}^{(Np)}/\mathbb{Q})$ *such that*

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

Strictly speaking, [Wi95, Lemma 1.12] gives the above statement replacing K_1 by the splitting field K_0 of $\overline{\rho}$. Since the statement is about the cohomology group of $Ad^*(1)$, we can replace K_0 in his argument by K_1. We note also $\mathrm{Ker}(Ad(\overline{\rho})) = \mathrm{Ker}(\widetilde{\rho})$ as the kernel of the adjoint representation: $\mathrm{GL}(2) \to \mathrm{GL}(3)$ is the center of GL_2 (so it factors through PGL_2).

Proof. Since $x \in \mathrm{Ker}(\beta_Q)$, f_x is unramified at $q \in Q$; so, f_x factors through $\mathrm{Gal}(\mathbb{Q}^{(Np)}/K_1(\mu_p))$. We have two possibilities of the field $F' := K_1 \cap \mathbb{Q}(\mu_{Cp^m})$; i.e., $F' = \mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$ disjoint from F. Indeed, the maximal abelian extension of $\mathbb{Q}$ inside K_1 is either F (when $\mathrm{ord}(\overline{\varphi}^-)$ is odd > 1) or a composite FF' of the quadratic extensions F and F' over $\mathbb{Q}$ (if $\mathrm{ord}(\overline{\varphi}^-)$ is even $2n > 2$). If $\overline{\varphi}^-$ has odd order, $F' = \mathbb{Q}(\mu_{Cp^m}) \cap K^1 = \mathbb{Q}$ as it is a subfield of F and $\mathbb{Q}(\mu_{Cp^m})$ (because $(C, D) = 1$ and $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$).

Assume that $\mathrm{ord}(\overline{\varphi}^-) = 2n > 2$. Let $\mathcal{D} := \mathrm{Gal}(K_1/\mathbb{Q})$ and $\mathcal{C} := \mathrm{Gal}(K_1/F)$. Then $\mathcal{C}$ is a cyclic group of order $2n$. Pick a generator $g \in \mathcal{C}$. Then $\mathcal{D} = \mathcal{C} \sqcup \mathcal{C}\widetilde{\varsigma}$ for a lift $\widetilde{\varsigma}$ of ς, and we have a characterization $\mathcal{C}\varsigma = \{\tau \in \mathcal{D} | \tau g \tau^{-1} = g^{-1}, \tau^2 = 1\}$. For the derived group $\mathcal{D}'$ of $\mathcal{D}$, we have $\mathcal{D}^{ab} := \mathcal{D}/\mathcal{D}' \cong (\mathbb{Z}/2\mathbb{Z})^2$. We have $K_1^{\mathcal{D}'} = FF'$, and $\mathrm{Gal}(K_1/F')$ is equal to $\mathcal{C}^2 \rtimes \langle \varsigma \rangle$ (a dihedral group of order $2n$). If $n > 2$ (so, $2n > 4$), $\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$ restricted to $\mathrm{Gal}(K_1/F')$ is still irreducible isomorphic to $\mathrm{Ind}_{F'F}^{F'} \overline{\varphi}^-$. If $n = 2$, F' is a unique quadratic extension in $K_1^{\mathcal{D}'}$ unramified at D. In

any case, $F' \neq F$ which is quadratic over $\mathbb{Q}$. Since $F' = \mathbb{Q}(\mu_{Cp^m}) \cap K_1$ is at most quadratic disjoint from F, we can achieve (1)-(2) by picking up suitable σ_x in $\mathcal{C}^2 \rtimes \langle\varsigma\rangle$ because $Ad = \overline{\chi} \oplus \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$.

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

If $f_x(Y) \supset X$, we claim to find σ satisfying (1) and (2) and having eigenvalue 1 in X. If $X = \overline{\chi\omega}$, the splitting field of X is $F(\mu_p)$. Note that $F(\mu_{Cp^m})$ is abelian over $\mathbb{Q}$. Thus choosing σ fixing $F(\mu_{Cp^m})$ with $\sigma \in \mathcal{C}^2|_{K_1}$ and having $\mathrm{ord}(\overline{\varphi}^-(\sigma)) \geq \mathrm{ord}((\overline{\varphi}^-)^2) = |\mathcal{C}^2| \geq 2$, we have σ having eigenvalue 1 on $X = \overline{\chi\omega}$.

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

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

Let $Q = \emptyset$ and choose a basis $\{x\}_x$ over $\mathbb{F}$ of the "dual" Selmer group $\mathrm{Sel}_{\emptyset}^{\perp}(Ad^*(1))$ inside $H^1(\mathbb{Q}^{(Np)}/\mathbb{Q}, Ad^*(1))$ (see (4.1) below for the definition of the Selmer group). Then Wiles' choice of Q_m is a set of primes q so that $\mathrm{Frob}_q = \sigma_x$ on M_x as in the above lemma. By Chebotarev density, we have infinitely many sets Q_m with this property.

Corollary 4.2. *Let the notation be as in* Lemma 4.1 *and its proof. If* $0 \neq f_x(Y) \subset \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-\overline{\omega}$, *the field automorphism* σ *in* Lemma 4.1 *satisfies* $\left(\frac{F/\mathbb{Q}}{\sigma}\right) = -1$. *Otherwise, we can choose* σ *so that* $\left(\frac{F/\mathbb{Q}}{\sigma}\right) = 1$.

Proof. In this case, we can have $X[1] \subset \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-\overline{\omega} \neq 0$; so, $Ad(\sigma)(1) = Ad(\sigma)$ (as $\omega(\sigma) = 1$) must have two distinct eigenvalues $\{1, -1\}$ on

$\mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}^-$, which implies $\left(\frac{F/\mathbb{Q}}{\sigma}\right) = -1$ as σ has to have eigenvalues -1 with multiplicity 2. Q.E.D.

Definition 4.3. Recall K^- defined in Definition 1.2. Let $\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to W^\times$ be a character of order prime to p whose image generates $\mathbb{Z}_p[\phi] \subset W$. Let $\mathcal{Y}^-$ (resp. $\mathcal{Y}^-_{sp}$) be the Galois group over $K^-F(\phi)$ of the maximal p-abelian extension of $K^-F(\phi)$ unramified outside $\mathfrak{p}$ and totally split at $\mathfrak{p}^\varsigma$ (resp. totally splits at all prime factors of $\mathfrak{p}^\varsigma N$). Regarding $\mathrm{Gal}(F(\phi)/F)$ as a subgroup of $\mathrm{Gal}(K^-F(\phi)/F) \cong \mathrm{Gal}(F(\phi)/F) \times \mathrm{Gal}(K^-/F)$, define

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

Here $\mathbb{Z}_p(\phi)$ is the $\mathbb{Z}_p(\phi)$-module free of rank 1 on which $\mathrm{Gal}(F(\phi)/F)$ acts by ϕ. More generally write $\mathcal{Y}^-_Q$ for the Galois group over $K^-_QF(\phi)$ of the maximal p-abelian extension L_Q of $K^-_QF(\phi)$ unramified outside $\mathfrak{p}$ and Q and totally splitting at $\mathfrak{p}^\varsigma$. Then define

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

Hereafter, more generally for a $\mathbb{Z}_p[\mathrm{Gal}(F(\phi)/F)]$-module X, we write $X[\phi] := X \otimes_{\mathbb{Z}_p[\mathrm{Gal}(F(\phi)/F)],\phi} W$ (the maximal quotient on which the Galois group acts by ϕ after extending scalar to W containing the values of ϕ). The base ring W will be clear in the context.

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

(4.1)

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

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

Since $Ad = \overline{\chi} \oplus \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$ for $\overline{\chi} := (\chi \mod p)$, the Selmer groups $\mathrm{Sel}_Q(Ad)$ (resp. $\mathrm{Sel}_Q^\perp(Ad^*(1))$) is the direct sum of the Selmer groups $\mathrm{Sel}_Q(\overline{\chi})$ (resp. $\mathrm{Sel}_Q^\perp(\overline{\chi\omega})$) and $\mathrm{Sel}_Q(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-)$ (resp. $\mathrm{Sel}_Q^\perp(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-\overline{\omega})$). To give a sketch of this direct sum decomposition (first noticed in [CV03, Theorem 3.1]), consider $\mathrm{Sel}_\emptyset^\perp(Ad^*(1))$ (whose decomposition as above is equivalent to (4.2) below). Then $\mathcal{D}_Q^p(\mathbb{F}[\epsilon])$ is made of classes of cocycles such that $u_\rho|_{I_p}$ is upper nilpotent with values in $F_+(\rho)$ in the introduction and $u_p|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q})}$ is upper triangular. Thus we confirm for $l = p$ that

(4.2)
$$\mathcal{D}_Q^l(\mathbb{F}[\epsilon])^\perp = (\mathcal{D}_Q^l(\mathbb{F}[\epsilon])^\perp \cap H^1(\mathbb{Q}_l, \overline{\chi\omega})) \oplus (\mathcal{D}_Q^l(\mathbb{F}[\epsilon])^\perp \cap H^1(\mathbb{Q}_l, \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-\overline{\omega})),$$

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

- (D_p) the Selmer cocycle u for $\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-\overline{\omega}$ is possibly ramified at $\mathfrak{p}$ with $u(\phi\tau\phi^{-1}) = \overline{\varphi}^-\overline{\omega}(\phi)u(\tau)$ for $\tau \in I_\mathfrak{p}^w$ but trivial over the decomposition group at $\mathfrak{p}^\varsigma$, where $\phi \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/F_\mathfrak{p})$ and $I_\mathfrak{p}^w \subset I_\mathfrak{p}$ is the wild inertia subgroup.

If φ^- is non-trivial over $I_\mathfrak{p}$, $\overline{\epsilon} \neq \overline{\delta}$, and the given filtration $\overline{\epsilon} \hookrightarrow \overline{\rho} \twoheadrightarrow \overline{\delta}$ determines $F_+(\overline{\rho})$. Thus the triviality at $\mathfrak{p}^\varsigma$ of the Selmer cocycle is automatic as $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ leaves stable $F_+(\overline{\rho})$, and hence any deformation local at p of $\overline{\rho}$ having values in $F_+(\overline{\rho})$ over I_p has values in $F_-(\overline{\rho})$ over the entire decomposition group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Note here that $I_\mathfrak{p}^w$ fixes $F(\varphi^-\omega)$ by (h1), and hence $u_\rho|_{I_\mathfrak{p}^w} : I_\mathfrak{p}^w \to \overline{\varphi}^-$ is a homomorphism, and the decomposition group acts by such a homomorphism by inner conjugation. Thus the condition (D_p) requires in particular that $u_\rho|_{I_\mathfrak{p}^w}$ is a $\mathbb{F}[\mathrm{Gal}(\overline{\mathbb{Q}}_p/F_\mathfrak{p})]$-homomorphism (where we regard $u_\rho|_{I_\mathfrak{p}^w}$ as having values in the subspace $F_+(\overline{\rho})$ which is isomorphic to the $\mathrm{Gal}(F(\varphi^-\omega/F)$-module $\overline{\varphi}^-$). If $\overline{\varphi}^-$ is ramified at $\mathfrak{p}$, the conjugation action of the $\mathfrak{p}$-inertia subgroup $I_{\mathfrak{P}/\mathfrak{p}}$ of $\mathrm{Gal}(L_\emptyset/F)$ on its wild inertia subgroup $I_{\mathfrak{P}/\mathfrak{p}}^w$ determines the action of the decomposition subgroup $D_{\mathfrak{P}/\mathfrak{p}}$ at $\mathfrak{p}$ as the inertia eigenspace of $\mathrm{Hom}(I_{\mathfrak{P}/\mathfrak{p}}^w, \overline{\varphi}^-)$ is automatically an eigenspace under the decomposition group, and the specification of the filtration $\overline{\epsilon} \hookrightarrow \overline{\rho} \twoheadrightarrow \overline{\delta}$ is automatic so that $\overline{\epsilon}$ is ramified. In any case, $\mathcal{D}_Q^p(\mathbb{F}[\epsilon])^\perp \cap H^1(\mathbb{Q}_p, \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-\overline{\omega})$ is the direct factor $H^1(F_\mathfrak{p}, \overline{\varphi}^-\overline{\omega})$ of

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

since $\overline{\varphi}_\varsigma^-(\tau) = \overline{\varphi}^-(\varsigma\tau\varsigma^{-1}) = (\overline{\varphi}^-)^{-1}(\tau)$.

Since $\overline{\chi}$ is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, we have

$$H^1(\mathbb{Q}_p, \overline{\chi\omega}) = H^1(\mathbb{Q}_p, \mu_p) \cong \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p$$

by Kummer theory. Since $\overline{\omega}$ ramifies at p, we have $H^0(I_p, \overline{\chi\omega}) = 0$, and by inflation and restriction sequence, we have an exact sequence:

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

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

$$\begin{array}{ccccc} H^1(\mathrm{Frob}_p^{\widehat{\mathbb{Z}}}, \overline{\chi}) & \xrightarrow{\hookrightarrow} & H^1(\mathbb{Q}_p, \overline{\chi}) & \xrightarrow{\twoheadrightarrow} & H^1(I_p, \overline{\chi})^{\mathrm{Frob}_p=1} \\ \wr\downarrow & & \wr\downarrow & & \wr\downarrow \\ \mathrm{Hom}(\mathrm{Frob}_p^{\widehat{\mathbb{Z}}}, \mathbb{F}) & \xrightarrow[\hookrightarrow]{} & \mathrm{Hom}(\mathbb{Q}_p^\times, \mathbb{F}) & \xrightarrow[\twoheadrightarrow]{} & \mathrm{Hom}(\mathbb{Z}_p^\times, \mathbb{F})^{\mathrm{Frob}_p=1}. \end{array}$$

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

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

So, it is ramified, and hence

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

For a prime $l | N_{F/\mathbb{Q}}(\mathfrak{c})$, $Ad \cong \overline{\chi} \oplus \overline{\varphi}^- \oplus (\overline{\varphi}^-)^{-1}$ and $Ad^*(1) \cong \overline{\chi\omega} \oplus \overline{\varphi}^-\overline{\omega} \oplus (\overline{\varphi}^-)^{-1}\overline{\omega}$ over $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ (as $F_l = \mathbb{Q}_l \oplus \mathbb{Q}_l$). Write $\overline{\varphi}'$ (resp. $\overline{\chi}'$) for $\overline{\varphi}^-$ and $\overline{\varphi}^-\overline{\omega}$ (resp. for $\overline{\chi}$ and $\overline{\chi\omega}$) in order to treat the two cases at the same time. We normalize Ad so that the character $\overline{\chi}$ is realized on $\mathbb{F}\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $\overline{\varphi}^-$ appears on the upper nilpotent matrices and $(\overline{\varphi}^-)^{-1}$ acts on lower nilpotent matrices, and we also normalize $Ad^*(1)$ accordingly.

Since $H^0(I_l,\overline{\varphi}')=0$, we have $H^1(\mathbb{Q}_l,\overline{\varphi}')\cong H^1(I_l,\overline{\varphi}')^{\mathrm{Frob}_l=1}$ by the restriction map. Since $\overline{\omega}$ is unramified at l, we have $\overline{\varphi}^-\overline{\omega}|_{I_l}=\overline{\varphi}^-|_{I_l}$. We have the following exact sequence

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

Since $\overline{\varphi}'(I_l)$ has order prime to p, we have $H^j(\overline{\varphi}'(I_l),\overline{\varphi}')=0$ for all $j>0$. Thus $H^1(I_l,\overline{\varphi}')\cong\mathrm{Hom}_{\overline{\varphi}'(I_l)}(\mathrm{Ker}(\overline{\varphi}'|_{I_l}),\overline{\varphi}')$. Since any elements in $\mathrm{Hom}_{\overline{\varphi}'(I_l)}(\mathrm{Ker}(\overline{\varphi}'|_{I_l}),\overline{\varphi}')$ factors through the tame quotient of I_l which is abelian, the conjugation action of $\overline{\varphi}'(I_l)$ on $\mathrm{Ker}(\overline{\varphi}'|_{I_l})$ is trivial, while φ' is non-trivial; so, we conclude $H^1(I_l,\overline{\varphi}')\cong\mathrm{Hom}_{\overline{\varphi}'(I_l)}(\mathrm{Ker}(\overline{\varphi}'|_{I_l}),\overline{\varphi}')$ vanishes. Thus we get $H^1(\mathbb{Q}_l,Ad)=\mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l),\mathbb{F}\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right))\cong\mathbb{F}$ and $H^1(\mathbb{Q}_l,Ad^*(1))=H^1(\mathbb{Q}_l,\mathbb{F}\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)\otimes\overline{\omega})=H^1(\mathrm{Frob}_l^{\widehat{\mathbb{Z}}},\mathbb{F}\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)\otimes\overline{\omega})\cong\mathbb{F}$, which is the Tate dual of $H^1(\mathbb{Q}_l,Ad)$. This tell us that the Selmer cocycle u_ρ giving a class in $\mathcal{D}_Q^l(\mathbb{F}[\epsilon])$ for Ad has values in $\mathbb{F}\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$ over $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ and is unramified. In other words, we have $\mathcal{D}_Q^l(\mathbb{F}[\epsilon])=H^1(\mathbb{Q}_l,Ad)$; so, again the direct sum decomposition (4.2) holds, and we find $\mathcal{D}_Q^l(\mathbb{F}[\epsilon])^\perp=H^1(\mathbb{Q}_l,Ad)^\perp=0$.

At $l|D$, $\overline{\varphi}^-|_{\mathrm{Gal}(\overline{\mathbb{Q}}_l/F_l)}$ is trivial. Thus we have $Ad\cong\overline{\chi}\oplus\mathrm{Ind}_F^{\mathbb{Q}}\overline{\mathbf{1}}\cong\overline{\chi}\oplus\mathbf{1}\oplus\overline{\chi}$ over $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$. The first factor $\overline{\chi}$ is realized in $\mathbb{F}\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$, the last factor $\overline{\chi}$ is realized on $\mathbb{F}\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$ and the middle factor $\mathbf{1}$ is realized on $Ad^{I_l}=\mathbb{F}\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$. Arguing in the same way as we showed $H^1(\mathbb{Q}_l,\overline{\varphi}^-)=0$, replacing $\overline{\varphi}^-$ by $\overline{\chi}$, we find that $H^1(\mathbb{Q}_l,\overline{\chi})=0$. By Shapiro's lemma, we have $H^1(\mathbb{Q}_l,\mathrm{Ind}_F^{\mathbb{Q}}\mathbf{1})=H^1(F_l,\mathbb{F})=\mathrm{Hom}(F_l^\times,\mathbb{F})\cong\mathbb{F}$ by (h3). Thus the cohomology classes in $H^1(\mathbb{Q}_l,Ad)$ is represented by cocycles with values in $\mathbb{F}\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$. Therefore we get $H^1(\mathbb{Q}_l,Ad)=\mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l),\mathbb{F}\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right))$, and $\rho\in\mathcal{D}_Q^l(\mathbb{F}[\epsilon])$ if and only if u_ρ has image in $Ad(\mathbb{F})^{I_l}=\mathbb{F}\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ and is unramified. In particular, $\mathcal{D}_Q^l(\mathbb{F}[\epsilon])=H^1(\mathbb{Q}_l,Ad)\cong\mathbb{F}$ and $\mathcal{D}_Q^l(\mathbb{F}[\epsilon])^\perp=0$. Thus we get

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

By the same argument applied to $Ad^*(1)|_{\mathrm{Gal}(\mathbb{Q}_l/\mathbb{Q}_l)}=\overline{\chi\omega}\oplus\overline{\omega}\oplus\overline{\chi\omega}$ with $H^1(\mathbb{Q}_l,\overline{\chi\omega})=0$, Kummer's theory tells us that $H^1(\mathbb{Q}_l,Ad^*(1))=\mathbb{Q}_l^\times/(\mathbb{Q}_l^\times)^p\otimes_{\mathbb{F}_p}\mathbb{F}\cong\mathbb{F}$, which is represented by cocycle with values in $\mathbb{F}\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ on which $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ acts by $\overline{\omega}$ as a factor of $Ad^*(1)$. Therefore the direct sum decomposition (4.2) holds, and

$$\mathcal{D}_Q^l(\mathbb{F}[\epsilon])^\perp=H^1(\mathbb{Q}_l,Ad)^\perp=0.$$

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

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

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

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

$$\begin{aligned}\mathrm{Sel}_\emptyset^\perp(\mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}^-\overline{\omega}) &\cong \mathrm{Sel}_\emptyset^\perp(\overline{\varphi}^-\overline{\omega})\\ &= \mathrm{Hom}_{\mathrm{Gal}(F(\varphi^-\omega)/F)}(\mathrm{Gal}(L_\emptyset^{sp}/F(\varphi^-\omega)), \overline{\varphi}^-\overline{\omega})^{[p,F_\mathfrak{p}]=\overline{\varphi}^-([p,F_\mathfrak{p}])}.\end{aligned}$$

Here the condition $[p, F_\mathfrak{p}] = \overline{\varphi}^-([p, F_\mathfrak{p}]) = \overline{\varphi}^-\overline{\omega}([p, F_\mathfrak{p}])$ is automatic if φ^- ramifies at $\mathfrak{p}$ as already explained. Since $p \nmid h_F$, the extension K^-/F (in Definition 1.2) is fully wild $\mathfrak{p}^\varsigma$-ramified, while $F(\varphi^-\omega)$ is at most tamely $\mathfrak{p}^\varsigma$-ramified. Therefore the inertia subgroup of $\mathfrak{p}^\varsigma$ for the extension $K^-F(\varphi^-\omega)/F(\varphi^-\omega)$ is the whole group $\mathrm{Gal}(K^-F(\varphi^-\omega)/F(\varphi^-\omega))$. This tells us that $L_\emptyset^{sp} \cap K^-F(\varphi^-\omega) = F(\varphi^-\omega)$. Thus, we have the vanishing of the $\varphi^-\omega$-eigenspace

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

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

$$\begin{aligned}&\mathrm{Hom}_{\mathrm{Gal}(F(\varphi^-\omega)/F)}(\mathrm{Gal}(L_\emptyset^{sp}/F(\varphi^-\omega)), \overline{\varphi}^-\overline{\omega})\\ &\qquad = \mathrm{Hom}(\mathcal{Y}_{sp}^-(\varphi^-\omega)_H, \mathbb{F}) = \mathrm{Hom}_{W[H]}(\mathcal{Y}_{sp}^-(\varphi^-\omega), \mathbb{F}).\end{aligned}$$

Proposition 4.4. *Let $Cl_{Q^+}^- = \{x \in Cl_{Q^+} | \varsigma(x) = x^{-1}\}$, and write $Cl_{\mathbb{Q}(\chi\omega)}(p^\infty)$ for the class group of the splitting field of $\chi\omega$. Then, under*

(h1–4), *we have* $\mathcal{Y}^-_Q(\varphi^-) = \mathcal{Y}^-(\varphi^-)$ *for* $Q \in \mathcal{Q}$,

(4.3)
$$\mathrm{Sel}_Q(Ad) \cong \mathrm{Hom}(Cl^-_{Q^+}, \mathbb{F}) \oplus \mathrm{Hom}_{W[H]}(\mathcal{Y}^-(\varphi^-), \mathbb{F}) \text{ including } Q = \emptyset,$$
$$\mathrm{Sel}^\perp_\emptyset(Ad^*(1)) \cong \mathrm{Sel}^\perp_\emptyset(\overline{\chi\omega}) \oplus \mathrm{Hom}_{W[H]}(\mathcal{Y}^-_{sp}(\varphi^-\omega), \mathbb{F}),$$

and

$$\begin{aligned} \mathrm{Sel}_Q(\overline{\chi}) &\cong \mathrm{Hom}(Cl^-_{Q^+}, \mathbb{F}) \text{ including } Q = \emptyset, \\ \mathrm{Sel}_Q(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) &\cong \mathrm{Hom}_{W[H]}(\mathcal{Y}^-(\varphi^-), \mathbb{F}) \text{ including } Q = \emptyset, \\ \mathrm{Sel}^\perp_\emptyset(\overline{\chi\omega}) &\hookrightarrow \mathrm{Hom}(Cl_{\mathbb{Q}(\chi\omega)}(p^\infty), \mathbb{F})[\overline{\chi\omega}] \\ \mathrm{Sel}^\perp_\emptyset(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-\overline{\omega}) &\cong \mathrm{Hom}_{W[H]}(\mathcal{Y}^-_{sp}(\varphi^-\omega), \mathbb{F}), \end{aligned} \tag{4.4}$$

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

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 $\mathcal{D}^p_Q(\mathbb{F}[\epsilon])$ is made of classes of cocycles with values in $Ad = \mathfrak{sl}_2(\mathbb{F})$ such that $u_\rho|_{I_p}$ is upper nilpotent with values in $F_+(\rho)$ in the introduction and $u_\rho|_{D_p}$ ($D_p := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$) is upper triangular. Similarly $\mathcal{D}^l(\mathbb{F}[\epsilon])$ for $l|N$ is made of classes of unramified cocycles u_ρ with values in diagonal matrices over D_l. Then by the same argument proving (4.2) (or by the dual statement of (4.2)), we note that

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

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

$$\begin{aligned} &\mathrm{Sel}_Q(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) \\ &= \mathrm{Ker}(H^1(\mathbb{Q}^{(QNp)}/\mathbb{Q}, \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) \xrightarrow{\mathrm{Res}} \prod_{l|Np} \frac{H^1(\mathbb{Q}_l, \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-)}{\mathcal{D}^l(\mathbb{F}[\epsilon])}) \\ &= \mathrm{Ker}(H^1(\mathbb{Q}^{(QNp)}/\mathbb{Q}, \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) \xrightarrow{\mathrm{Res}} H^1(F_{\mathfrak{p}^\varsigma}, \overline{\varphi}^-) \times \prod_{l|N} H^1(I_l, \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-). \end{aligned} \tag{4.5}$$

By the inflation restriction sequence,

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

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

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

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

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

If φ^- is ramified at $\mathfrak{p}^\varsigma$, $H^0(I_{\mathfrak{p}^\varsigma},\overline{\varphi}^-)=0$ and $H^1(\mathrm{Frob}_p^{\widehat{\mathbb{Z}}}, H^0(I_{\mathfrak{p}^\varsigma},\overline{\varphi}^-))=0$. If φ^- is unramified at $\mathfrak{p}^\varsigma$, we have

$$H^1(\mathrm{Frob}_p^{\widehat{\mathbb{Z}}}, H^0(I_{\mathfrak{p}^\varsigma},\overline{\varphi}^-)) = \mathbb{F}/(\overline{\varphi}^-(\mathrm{Frob}_p)-1)\mathbb{F} = 0$$

as $\overline{\varphi}^-(Frob_p) \neq 1$. Triviality over $\mathrm{Gal}(\overline{\mathbb{Q}}_p/F_{\mathfrak{p}^\varsigma})$ (total splitting condition at $\mathfrak{p}^\varsigma$ for $\mathcal{Y}_{sp}(\varphi^-)$) is equivalent to unramifiedness at $\mathfrak{p}^\varsigma$. Thus we conclude $\mathrm{Ker}(H^1(F_{\mathfrak{p}^\varsigma},\overline{\varphi}^-) \xrightarrow{\mathrm{Res}} H^1(I_{\mathfrak{p}^\varsigma},\overline{\varphi}^-)) = 0$, and $\mathrm{Sel}_Q(\mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}^-)$ is actually given (by replacing $H^1(F_{\mathfrak{p}^\varsigma},\overline{\varphi}^-)$ by $H^1(I_{\mathfrak{p}^\varsigma},\overline{\varphi}^-)$ in (4.5))

(4.6)
$$\mathrm{Ker}(H^1(\mathbb{Q}^{(QNp)}/\mathbb{Q}, \mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}^-) \xrightarrow{\mathrm{Res}} H^1(I_{\mathfrak{p}^\varsigma},\overline{\varphi}^-) \times \prod_{l|N} H^1(I_l, \mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}^-)$$

if φ^- is ramified at $\mathfrak{p}$. By the inflation-restriction sequence, we have an exact sequence $H^1(\mathrm{Frob}_l^{\widehat{\mathbb{Z}}}, (\overline{\varphi}^-)^{I_l}) \hookrightarrow H^1(D_l,\overline{\varphi}^-) \to H^1(I_l,\overline{\varphi}^-)$ with $(\overline{\varphi}^-)^{I_l}=0$ for $l|N$, and hence by Shapiro's lemma (and (h3), we can rewrite, recalling $G_Q := \mathrm{Gal}(\mathbb{Q}^{(QNp)}/\mathbb{Q})$,

$$\mathrm{Sel}_Q(\mathrm{Ind}_F^{\mathbb{Q}}\overline{\varphi}^-) =$$
$$\begin{cases} \mathrm{Ker}(H^1(G_Q,\varphi^-) \to H^1(I_{\mathfrak{p}^\varsigma},\overline{\varphi}^-) \times \prod_{\mathfrak{l}|N} H^1(I_{\mathfrak{l}},\overline{\varphi}^-)) & \text{if } \varphi^-|_{I_{\mathfrak{p}}} \neq 1, \\ \mathrm{Ker}(H^1(G_Q,\varphi^-) \to H^1(F_{\mathfrak{p}^\varsigma},\overline{\varphi}^-) \times \prod_{\mathfrak{l}|N} H^1(I_{\mathfrak{l}},\overline{\varphi}^-)) & \text{if } \varphi^-|_{I_{\mathfrak{p}}} = 1, \end{cases}$$

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

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

Similarly, $\mathrm{Sel}_Q(\overline{\chi}) \cong \mathrm{Hom}_{\mathrm{Gal}(F/\mathbb{Q})}(\mathrm{Gal}(\mathbb{Q}^{(QNp)}/F), \overline{\chi}) = \mathrm{Hom}(Cl_Q^-, \mathbb{F})$. Therefore the first identity of (4.3) follows if we prove

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

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

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

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

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

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

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

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

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

group of $\mathfrak{Q}$, we have

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

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

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

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

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

as desired. Q.E.D.

The primes $q_x \in Q_m$ is indexed by a basis $\{x\}_x$ of the Selmer group $\mathrm{Sel}_{\emptyset}^{\perp}(Ad^*(1))$ so that f_x as in Lemma 4.1 has non-trivial value at Frob_{q_x}. Thus writing $Q_m^{\pm} := \{q \in Q_m | \chi(q) = \pm 1\}$, we get from our choice in Corollary 4.2

(4.7)
$$|Q_m^-| = \dim_{\mathbb{F}} \mathrm{Hom}_{W[H]}(\mathcal{Y}_{sp}^-(\varphi^-\omega), \mathbb{F}) \quad \text{and} \quad |Q_m^+| = \dim_{\mathbb{F}} \mathrm{Sel}_{\emptyset}^{\perp}(\overline{\chi\omega}).$$

§5. Galois action on unit groups

We use notation introduced in Definition 1.2 for abelian extensions of the real quadratic field F. As before, for any $W[\mathrm{Gal}(F(\varphi^-)/F)]$-module X, we write $X[\varphi^-]$ for the φ^--eigenspace:

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

Proposition 5.1. *Recall that F is real quadratic over $\mathbb{Q}$. Let $\mathfrak{R}$ be the integer ring of $F(\varphi^-)$. Write a for the order of φ^-. Then a is even with $a = 2b$ for $0 < b \in \mathbb{Z}$, and we have $\mathfrak{R}^\times \otimes_{\mathbb{Z}} \overline{\mathbb{Q}} \cong \chi \oplus \bigoplus_{j=1}^{b-1} \mathrm{Ind}_F^{\mathbb{Q}}(\varphi^-)^{2j}$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.*

Proof. Since $\det(\mathrm{Ind}_F^{\mathbb{Q}}\varphi)(c) = -1$ for complex conjugation, φ ramifies at only one infinite place. Therefore φ^- 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 $\mathrm{Gal}(F(\varphi^-)/F)$ has order 2 and is in the center of the dihedral group $\mathrm{Gal}(F(\varphi^-)/\mathbb{Q})$. Thus $F(\varphi^-)$ is a CM field with maximal totally real field $F((\varphi^-)^2)$ [IAT, Proposition 5.11]; so, c acts trivially on $\mathfrak{R}^\times \otimes_{\mathbb{Z}} \mathbb{Q}$ and as Galois modules, we have $\mathbf{1} \oplus (\mathfrak{R}^\times \otimes_{\mathbb{Z}} \mathbb{Q}) \cong \mathrm{Ind}_{F((\varphi^-)^2)}^{\mathbb{Q}} \mathbf{1}$ for the identity character $\mathbf{1}$. Then the assertion is clear from this expression. Q.E.D.

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

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

and $E_- = E \cap (1 + \mathfrak{p}^\varsigma O_{\mathfrak{p}^\varsigma})^p = E(\mathfrak{p}^{2\varsigma}) = E(p^2)$.

Proposition 5.2. *Let the notation be as above, and assume that $p \geq 3$. Then we have*

$$\dim_{\mathbb{F}} \mathrm{Hom}(Cl_{\mathbb{Q}(\chi\omega)}, \mathbb{F})[\overline{\chi\omega}] \geq \dim_{\mathbb{F}_p} E(p^2)/E(p)^p$$

with equality if the class number h_F is prime to p, and $E(p^2)/E(p)^p$ is canonically embedded into $\mathrm{Hom}(Cl_{\mathbb{Q}(\chi\omega)}, \mathbb{F}_p)[\overline{\chi\omega}]$. Similarly, assuming further (h3)*,*

$$\dim_{\mathbb{F}} \mathrm{Sel}_\emptyset^\perp(\overline{\chi\omega}) \geq 1$$

with equality if the class number h_F is prime to p, and $E \otimes_{\mathbb{Z}} \mathbb{F} = E/E^p$ is canonically embedded into $\mathrm{Sel}_\emptyset^\perp(\overline{\chi\omega})$.

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 $F/\mathbb{Q}$, $F_{\mathfrak{p}} = \mathbb{Q}_p$ for each prime factor $\mathfrak{p}|p$ in F, and hence $1+p^2O_p = (1+pO_p)^p$. By (h3), $E_+ \subset (O_{\mathfrak{l}}^\times)^p$ for all prime factors $\mathfrak{l}|N$; so, $F_{\mathfrak{l}}[\mu_p][\sqrt[p]{\varepsilon}] = F_{\mathfrak{l}}[\mu_p]$ for all $\varepsilon \in E_+$ at all $\mathfrak{l}|N$ (i.e., total splitting at $l|N$).

Take $\varepsilon \in E_+$. If ε represents a non-trivial element in $E_+(p^2)/E_+^p$, $\varepsilon \in E_+ \setminus E_+^p$ and $\varepsilon \in E_+(p^2) = E_+ \cap (1 + p^2O_p)$. Consider a Kummer extension $F(\mu_p)[\sqrt[p]{\varepsilon}]/F(\mu_p)$. In this proof, we let the Galois group act on field elements from the left (in order to get left modules under Galois action). Pick a p-th root $\epsilon := \sqrt[p]{\varepsilon}$. Then $u = u_\epsilon : \sigma \mapsto {}^{\sigma-1}\epsilon = {}^\sigma\epsilon/\epsilon \in \mu_p$ is a cocycle of $\mathrm{Gal}(F(\mu_p)[\sqrt[p]{\varepsilon}]/F)$ representing the cohomology class of $\varepsilon \in F^\times/(F^\times)^p \cong H^1(F, \mu_p)$. First of all, $({}^\sigma\epsilon)^p = {}^\sigma\varepsilon = \varepsilon$; so, ${}^{\sigma-1}\epsilon \in$

μ_p. Indeed, for $\sigma, \tau \in \mathrm{Gal}(F(\mu_p)[\sqrt[p]{\varepsilon}]/F)$, we have $u(\sigma\tau) = {}^{\sigma\tau-1}\epsilon = {}^{\sigma\tau-\sigma+\sigma-1}\epsilon = {}^{\sigma}u(\tau)u(\sigma)$.

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

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

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

The set of conjugates of ϵ over $\mathbb{Q}$ is given by $\{\zeta\epsilon, \zeta'\epsilon^{-1}\}_{\zeta,\zeta' \in \mu_p(\overline{\mathbb{Q}})}$ as $c(\varepsilon) = \varepsilon^{-1}$. Thus $L := F(\mu_p)[\epsilon]$ is a Galois extension over $\mathbb{Q}$ and $\mathrm{Gal}(L/F) \lhd \mathrm{Gal}(L/\mathbb{Q})$. Thus for any lift $\gamma \in \mathrm{Gal}(L/\mathbb{Q})$ of the generator ς of $\mathrm{Gal}(F/\mathbb{Q})$, we can think of $\eta'(\sigma) := \eta(\gamma\sigma\gamma^{-1})$ which is a representation of $\mathrm{Gal}(L/\mathbb{Q})$ into $\mathrm{GL}_2(\mathbb{F}_p)$ with values in the mirabolic subgroup

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

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

Thus we may lift the generator ς of $\mathrm{Gal}(F/\mathbb{Q})$ uniquely to a central element $\gamma \in \mathrm{Gal}(L/\mathbb{Q})$. Then ${}^{\gamma}\epsilon = \zeta\epsilon^{-1}$ for some $\zeta \in \mu_p(L)$ as ${}^{\varsigma}\varepsilon = \varepsilon^{-1}$, which implies ${}^{\gamma}\epsilon^{-1} = \zeta^{-1}\epsilon$. Then ${}^{\gamma+1}\epsilon = \zeta$. Since γ^2 is the identity, we

find that ${}^{\gamma}\zeta = {}^{\gamma(\gamma+1)}\epsilon = {}^{\gamma+1}\epsilon = \zeta$. We honestly compute

$$\begin{aligned}{}^{\gamma}u_\epsilon(\sigma) &= {}^{\gamma(\sigma-1)}\epsilon = {}^{(\sigma-1)\gamma}\epsilon \\ &= {}^{\sigma-1}(\zeta\epsilon^{-1}) = \zeta^{\omega(\sigma)-1}({}^{1-\sigma}\epsilon) = \zeta^{\omega(\sigma)-1}u_\epsilon(\sigma)^{-1}.\end{aligned}$$

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

$$^{\gamma}\zeta_p = \zeta_p^{-1}.$$

Thus γ acts on $\mathbb{Q}(\mu_p)$ as complex conjugation and on F by ς. Therefore

$$F(\mu_p)^Z := H^0(Z, F(\mu_p)) = \mathbb{Q}(\chi\omega). \tag{5.1}$$

Hence we have a cyclic extension $\mathbb{Q}_\varepsilon/\mathbb{Q}(\chi\omega)$ which is the subfield of L fixed by γ. Since ε is a unit, only possible ramification of L over $F(\mu_p)$ at finite places is at a prime over p. Since $\varepsilon \in 1 + p^2O_p$, ε is a p-power at all place $\mathfrak{P}|p$ of F, and L is a p-cyclic extension unramified everywhere over $F(\mu_p)$. Since $p > 2$, $\mathbb{Q}_\varepsilon/\mathbb{Q}(\chi\omega)$ is a p-cyclic extension unramified everywhere, as $\mathbb{Q}_\varepsilon$ at each real place of $\mathbb{Q}(\chi\omega)$ has a real embedding. By the above construction, for $E_+(p^2) = E_+ \cap (1 + pO_p)^p$, We get $E(p^2)/E^p \cong E_+(p^2)/E_+^p$ and injective homomorphisms

(1) $E(p^2)/E^p \hookrightarrow \mathrm{Hom}(Cl_{\mathbb{Q}(\chi\omega)}, \mathbb{F}_p)[\overline{\chi\omega}]$,
(2) $E/E^p \cong E_+/E_+^p \hookrightarrow \mathrm{Hom}(Cl_{\mathbb{Q}(\chi\omega)}(p^\infty), \mathbb{F}_p)[\overline{\chi\omega}]$

by sending ε to $U_\epsilon|_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\chi\omega))}$ which in Case (1) factors through the Galois group $Cl_{\mathbb{Q}(\chi\omega)} = \mathrm{Gal}(H(\chi\omega)/\mathbb{Q}(\chi\omega))$ 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 $L/F(\mu_p)$ be a p-abelian extension unramified everywhere. Then we can choose $\xi \in F(\mu_p)^\times$ so that $L = F(\mu_p)[\sqrt[p]{\xi}]$ by Kummer's theory (i.e., $F[\mu_p]^\times/(F[\mu_p]^\times)^p \cong H^1(F, \mu_p)$). Suppose that $L/\mathbb{Q}$ is a Galois extension such that the conjugation action of $\mathrm{Gal}(F[\mu_p]/\mathbb{Q})$ on $\mathrm{Gal}(L/F[\mu_p]) \cong \mathbb{F}_p$ is given by $\overline{\chi\omega}$. Then we have $F[\mu_p]^\times/(F[\mu_p]^\times)^p[\omega] \cong H^1(F[\mu_p], \mu_p)[\omega]$. The action of $\tau \in \mathrm{Gal}(F[\mu_p]/F)$ on a cocycle $u : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mu_p$ is ${}^{\tau}u : \sigma \mapsto \tau(u(\widetilde{\tau}^{-1}\sigma\tau))$ for a lift $\widetilde{\tau} \in \mathrm{Gal}(L/F)$ of $\tau \in \mathrm{Gal}(F[\mu_p]/F)$. Thus we have

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

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

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

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

$$1 \to H^0(F[\mu_p]/F, F[\mu_p]^\times/\mu_p) \xrightarrow{x\mapsto x^p} H^0(F[\mu_p]/F, F[\mu_p]^\times)$$
$$\to H^0(F[\mu_p]/F, F[\mu_p]^\times/(F[\mu_p]^\times)^p) \to H^1(F[\mu_p]/F, F[\mu_p]^\times/\mu_p)$$

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

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

Thus we can choose $\xi \in F^\times$.

Suppose that $L/F[\mu_p]$ is everywhere unramified. Then (ξ) 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, (ξ) is a p-power as an ideal of F, write $(\xi) = \prod_{\mathfrak{l}} \mathfrak{l}^{pe(\mathfrak{l})}$ for prime ideals $\mathfrak{l}$ of F. Since $\mathrm{Gal}(F[\mu_p]/\mathbb{Q})$ acts on $\mathrm{Gal}(L/F[\mu_p])$ by $\overline{\chi\omega}$, we have $(\sqrt[p]{\tau\xi}) = (\sqrt[p]{\xi})^{\chi(\tau)}$ modulo p-power ideals. Thus $e(\mathfrak{l}) \equiv -e(\mathfrak{l}^\varsigma) \mod p$ for the generator ς of $\mathrm{Gal}(F/\mathbb{Q})$. In particular, $\mathfrak{l}$ is split in $F/\mathbb{Q}$ if $e(\mathfrak{l}) \neq 0$. This implies for $h = h_F$, $(\mathfrak{l}^{e(\mathfrak{l})}\mathfrak{l}^{ce(\mathfrak{l}^\varsigma)})^h = (\varpi_{\mathfrak{l}})$ for $\varpi_{\mathfrak{l}} \in F^\times$. If $p \nmid h_F$, we can replace ξ by ξ^h without changing L. Thus we may assume that $(\xi) = (\xi')^p$ for $\xi' := \prod_{\{\mathfrak{l}|(\xi)\}/\mathrm{Gal}(F/\mathbb{Q})}(\varpi_{\mathfrak{l}})$ with $\varpi_{\mathfrak{l}} \in F$ as above. Write $\xi = \varepsilon\xi'^p$. Then $\varepsilon \in O^\times$. Since $L/F[\mu_p]$ and $F/\mathbb{Q}$ are unramified at p, we find $\varepsilon \equiv 1 \mod p^2$. Regard $\tau \mapsto {}^{\tau-1}\varepsilon$ be a cocycle with values in $O^\times$. The exact sequence

$$1 \to H^0(F/\mathbb{Q}, O^\times \otimes \chi) \xrightarrow{x\mapsto x^p} H^0(F/\mathbb{Q}, O^\times \otimes \chi)$$
$$\to H^0(F/\mathbb{Q}, (O^\times/(O^\times)^p) \otimes \chi) \to H^1(F/\mathbb{Q}, O^\times \otimes \chi),$$

combined with the fact that $H^1(F/\mathbb{Q}, O^\times \otimes \chi)$ is killed by $[F : \mathbb{Q}] = 2$ prime to p, we find that $H^0(F/\mathbb{Q}, (O^\times/(O^\times)^p) \otimes \chi) = O^\times/(O^\times)^p = E/E^p$. Thus we may assume that $\varepsilon^\varsigma = \varepsilon^{-1}$ in F; so, $\varepsilon \in E$, and $\sqrt[p]{\varepsilon}$ generates L over $\mathbb{Q}$. Since a is prime to p, we may assume that $\varepsilon \in E_+$. Since $\varepsilon \equiv 1 \mod p^2$, we find that ε gives rise to a non-trivial class of $E_+(p^2)/E_+^p \supset \mathcal{E} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$. Thus we conclude $\dim \mathrm{Hom}(Cl_{\mathbb{Q}(\overline{\chi\omega})}, \mathbb{F}_p)[\overline{\chi\omega}] = \dim_{\mathbb{F}_p} E_+(p^2)/E_+^p$, 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 ε has to be in $O[\frac{1}{p}]^\times$, by (Km) (i.e., locally at p, $L'_p = \mathbb{Q}_p(\mu_p)[\sqrt[p]{\varepsilon}]$ with $\varepsilon \in \mathbb{Z}_p^\times$), we find $\varepsilon \in O^\times$, and we get the result as $\mathrm{Ker}(Cl_F(p) \to Cl_F)$ has order prime to p. Q.E.D.

Consider $\mathfrak{E} := \mathrm{Ker}(N_{F(\varphi^-)/F} : \mathfrak{R}^\times \to O^\times)$ to study $\mathrm{Sel}_\emptyset^\perp(\overline{\varphi}^-\overline{\omega}) \cong \mathrm{Hom}_{W[H]}(\mathcal{Y}^-(\varphi^-\omega), \mathbb{F})$ for H as in Definition 1.2. Define

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

for an ideal $\mathfrak{a}$ of $F(\varphi^-)$ over $\mathfrak{p}$.

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

$$\mathrm{Sel}_\emptyset^\perp(\overline{\varphi}^-\overline{\omega}) = \mathrm{Hom}_{W[H]}(\mathcal{Y}_{sp}^-(\varphi^-\omega), \mathbb{F}) = 0$$

if $(Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F})[\overline{\varphi}^-] = 0$.

The action of $\gamma \in \mathrm{Gal}(F(\varphi^-)/F)$ on $\phi \in \mathrm{Hom}_{W[H]}(\mathcal{Y}_{sp}^-(\varphi^-\omega), \mathbb{F})$ is given by $\gamma\phi(x) = \phi(\gamma^{-1}x) = (\overline{\varphi}^-)^{-1}(\gamma)\phi(x)$. We also note that $\varphi^-(\widetilde{\varsigma}\gamma\widetilde{\varsigma}^{-1}) = (\varphi^-)^{-1}(\gamma)$; so, by applying ς, we have $(Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F})[\overline{\varphi}^-] = 0 \Leftrightarrow (Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F})[(\overline{\varphi}^-)^{-1}] = 0$.

In the following proof, we write a for the exponent of $\mathfrak{E}$ modulo the radical $\mathfrak{r}^\varsigma$ of $\mathfrak{p}^\varsigma$ in $\mathfrak{R}$ (i.e., a is the minimal positive integer so that $\varepsilon^a \equiv 1 \mod \mathfrak{r}^\varsigma$ for all $\varepsilon \in \mathfrak{E}$). Since $-1 \in \mathfrak{E}$ (and $p > 2$), a is even, and plainly a is prime to p. Let $\mathfrak{E}_- := \{\varepsilon^a | \varepsilon \in \mathfrak{E}\}$. Note that all $\varepsilon \in \mathfrak{E}_-$ is positive at each real places of F, and $\mathfrak{E}_- \subset \mathfrak{E}(\mathfrak{r}^\varsigma)$. For each prime factor $\mathfrak{P}|\mathfrak{p}^\varsigma$ in $\mathfrak{R}$, we consider its $\mathfrak{P}$-adic completion $\mathfrak{R}_\mathfrak{P}$. Then we define $\mathfrak{E}_+ := \mathfrak{E}_- \cap (\prod_{\mathfrak{P}|\mathfrak{p}^\varsigma}(1 + \mathfrak{P}\mathfrak{R}_\mathfrak{P})^p \times \prod_{\mathfrak{L}|N}(\mathfrak{R}_\mathfrak{L}^\times)^p$ inside $\prod_{\mathfrak{L}|\mathfrak{p}^\varsigma N} R_\mathfrak{P}^\times$. By definition $\mathfrak{E}_+ \supset (\mathfrak{E}_-)^p$.

First Proof: We first give a proof very similar to the one for Proposition 5.2 assuming that $\overline{\varphi}^-$ has values in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and after doing this we shall give a shorter cohomological proof for general φ^-. We record here the longer proof as it is somehow more constructive; so, if the reader prefers the short-cut, she or he can ignore this first proof. Thus we only deal with the case where $\overline{\varphi}^-$ has values in $\mathbb{F}_p$. Take $\varepsilon \in \mathfrak{E}_+$. Suppose that $\varepsilon \in \mathfrak{E}_+$ represents a non-trivial element in $(\mathfrak{E}_+/\mathfrak{E}_-^p)[(\overline{\varphi}^-)^{-1}]$. Consider a Kummer extension $F(\varphi^-)(\mu_p)[\sqrt[p]{\varepsilon}]/F(\varphi^-)(\mu_p)$. Again, we let the Galois group acts on field elements from the left. Pick a p-th root $\epsilon := \sqrt[p]{\varepsilon}$. Since $({}^\sigma\epsilon)^p = {}^\sigma\varepsilon = \varepsilon$, we have ${}^{\sigma-1}\epsilon \in \mu_p(\overline{\mathbb{Q}})$. Then $u = u_\epsilon : \sigma \mapsto {}^{\sigma-1}\epsilon = {}^\sigma\epsilon/\epsilon \in \mu_p$ is a cocycle with values in $\mu_p(\overline{\mathbb{Q}})$ of $\mathrm{Gal}(F(\varphi^-)(\mu_p)[\sqrt[p]{\varepsilon}]/F(\varphi^-))$ representing the cohomology class of $\varepsilon \in F(\varphi^-)^\times/(F(\varphi^-)^\times)^p \cong H^1(F(\varphi^-), \mu_p)$. Indeed, for $\sigma, \tau \in \mathrm{Gal}(F(\varphi^-)(\mu_p)[\sqrt[p]{\varepsilon}]/F(\varphi^-))$, we have $u(\sigma\tau) = {}^{\sigma\tau-1}\epsilon = {}^{\sigma\tau-\sigma+\sigma-1}\epsilon = {}^\sigma u(\tau)u(\sigma)$.

Fix a p-th primitive root ζ_p of unity, and identify μ_p with $\mathbb{F}_p$ by $\zeta_p^m \mapsto m \in \mathbb{F}_p$. In this way, we regard u_ϵ as a cocycle $U = U_\epsilon$ with values

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

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

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

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

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

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

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

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

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

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

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

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

Thus γ acts on $F(\mu_p)$ as $\omega(\varphi^-(\gamma))^{-1}$. Therefore

$$F(\varphi^-)(\mu_p)^Z := H^0(Z, F(\varphi^-)(\mu_p)) = F(\varphi^-\omega). \tag{5.2}$$

Hence we have a cyclic extension $F_\varepsilon/F(\varphi^-\omega)$ which is the fixed subfield of L by γ. Since ε is a unit, only possible ramification of L over $F(\varphi^-)(\mu_p)$ at finite places is at a prime over p. Thus we get an injective homomorphism

$$(\mathfrak{E}_+/\mathfrak{E}_-^p)[(\overline{\varphi}^-)^{-1}] \hookrightarrow \mathrm{Hom}(C(\varphi^-\omega)(p^\infty), \mathbb{F}_p)[\overline{\varphi}^-\overline{\omega}] \tag{5.3}$$

sending ε to $U_\epsilon|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F(\varphi^-\omega))}$ which factors through factors through $C(\varphi^-\omega)(p^\infty)$. The ray class group $C(\varphi^-\omega)(p^\infty)$ is the Galois group of the maximal abelian extension of $F(\varphi^-\omega)$ unramified outside p and ∞. Since $\varepsilon \in \mathfrak{E}_+$ is locally a p-power at $\mathfrak{P}|\mathfrak{p}^\varsigma N$ by the definition of $\mathfrak{E}_+$, the corresponding Kummer cocycle is trivial at $\mathfrak{p}^\varsigma N$. Therefore, by (D_p) and (D_N), the image of $(\mathfrak{E}_+/\mathfrak{E}_-^p)[(\overline{\varphi}^-)^{-1}]$ lands in the image of $\mathrm{Sel}_\emptyset^\perp(\overline{\varphi}^-\overline{\omega})$ in $\mathrm{Hom}(C(\varphi^-\omega)(p^\infty), \mathbb{F}_p)[\overline{\varphi}^-\overline{\omega}]$.

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

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

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

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

The action of $\tau \in \mathrm{Gal}(F(\varphi^-)[\mu_p]/F(\varphi^-))$ on a cocycle u of $\mathrm{Gal}(\overline{\mathbb{Q}}/F(\varphi^-))$ with values in μ_p is ${}^\tau u : \sigma \mapsto \tau(u(\widetilde{\tau}^{-1}\sigma\widetilde{\tau}))$ for a lift $\widetilde{\tau} \in \mathrm{Gal}(L/F(\varphi^-))$ of

$\tau \in \mathrm{Gal}(F(\varphi^-)[\mu_p]/F(\varphi^-))$. For the Kummer cocycle $u_\xi(\tau) = {}^{\tau-1}\sqrt[p]{\xi}$ giving rise to an $\overline{\omega}$-eigen class in $H^1(F(\varphi^-)[\mu_p], \mu_p)[\overline{\omega}]$, we have

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

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

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

Thus we get $\tau({}^{(\sigma-1)}(\sqrt[p]{{}^\tau\xi})) = {}^{\overline{\omega}(\tau)(\sigma-1)}(\sqrt[p]{{}^\tau\xi})$. This shows

$$\xi^\tau \equiv \xi \mod (F(\varphi^-)[\mu_p]^\times)^p,$$

and $\tau \mapsto {}^{\tau-1}\xi$ is a cocycle with values in $(F(\varphi^-)[\mu_p]^\times)^p$. The exact sequence

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

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

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

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

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

$$\begin{aligned}(5.4)\quad H^1(F, \overline{\varphi^-}\overline{\omega}) &\cong H^0(F(\varphi^-)/F, H^1(F(\varphi^-), \overline{\omega})) \\ &\cong H^0(F(\varphi^-)/F, F(\varphi^-)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p) \cong (F(\varphi^-)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)[(\overline{\varphi^-})^{-1}],\end{aligned}$$

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

Suppose that $L/F(\varphi^-)[\mu_p]$ is trivial at prime factors in N and unramified outside p. Then $\xi\mathfrak{R}[\frac{1}{p}]$ is a p-power as a fractional $\mathfrak{R}[\frac{1}{p}]$-ideal in $F(\varphi^-)[\mu_p]$. Since $F(\varphi^-)[\mu_p]$ only ramifies at p with ramification index prime to p, (ξ) is a p-power as a fractional $\mathfrak{R}[\frac{1}{p}]$-ideal of $F(\varphi^-)$. Write $(\xi) = \prod_{\mathfrak{l}} \mathfrak{l}^{pe(\mathfrak{l})}$ for prime ideals $\mathfrak{l}$ of $\mathfrak{R}[\frac{1}{p}]$. If $h = h_{F(\varphi^-)}$ is prime to p, we may replace ξ by ξ^h without changing $F(\varphi^-)[\mu_p][\sqrt[p]{\xi}]$, and then $\prod_{\mathfrak{l}} \mathfrak{l}^{pe(\mathfrak{l})}$ becomes a p-power of a principal ideal (ξ'); i.e., $\xi = \varepsilon\xi'^p$ for $\varepsilon \in \mathfrak{R}[\frac{1}{p}]^\times$. Thus we may replace ξ by $\varepsilon \in \mathfrak{R}[\frac{1}{p}]^\times$.

We now show that we can replace ξ by $\varepsilon \in \mathfrak{R}[\frac{1}{p}]^\times$ under the assumption: $(Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F}_p)[\overline{\varphi}^-] = 0$ milder than $p \nmid h_{F(\varphi^-)}$. Since $\mathrm{Gal}(F(\varphi^-)[\mu_p]/F)$ acts on $\mathrm{Gal}(L/F(\varphi^-)[\mu_p])$ by $\overline{\varphi}^-\overline{\omega}$, we have

$$\prod_{\mathfrak{l}} \mathfrak{l}^{\tau e(\mathfrak{l})} \equiv (\sqrt[p]{\tau\xi}) \equiv (\sqrt[p]{\xi})^{[\varphi^-(\tau)^{-1}]} \equiv \prod_{\mathfrak{l}} \mathfrak{l}^{[\varphi^-(\tau)^{-1}]e(\mathfrak{l})}$$

modulo p-power of fractional $\mathfrak{R}[\frac{1}{p}]$-ideals. Thus we conclude $e(\mathfrak{l}) \equiv [\varphi^-(\gamma)^{-1}]e(\mathfrak{l}^\gamma) \mod p$ for the generator $\gamma \neq 1$ of $\mathrm{Gal}(F(\varphi^-)/F)$. In particular, $\mathfrak{l}$ is completely split in $F(\varphi^-)/F$ if $e(\mathfrak{l}) \neq 0$, since $\overline{\varphi}^-(\gamma) \neq 1$. Write Cl'_X for the ideal class group of $O_X[\frac{1}{p}]$ for a number field X with integer ring O_X. Note that $Cl'_{F(\varphi^-)}$ is the surjective image of $Cl_{F(\varphi^-)}$. If

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

$(Cl'_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{Z}_p)[\overline{\varphi}^-]) = 0$ by Nakayama's lemma, and $\prod_{j=1}^a {\gamma^j}\mathfrak{a}^{[\varphi^-(\gamma^j)]}$ for $\mathfrak{a} = \prod_{\mathfrak{l}} \mathfrak{l}^{e(\mathfrak{l})}$ is principal generated by ξ'. Replacing ξ by the $(\varphi^-)^{-1}$-projection $\prod_{j=1}^a {\gamma^j}\xi^{[\varphi^-(\gamma^j)]}$ with no effect on the corresponding Kummer extension, we may assume that $\xi = \varepsilon\xi'^p$. Then $\varepsilon \in \mathfrak{R}[\frac{1}{p}]^\times$.

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

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

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

$$H^0(F(\varphi^-)/F, (\mathfrak{R}[\frac{1}{p}]^\times/(\mathfrak{R}[\frac{1}{p}]^\times)^p) \otimes \varphi^-) = (\mathfrak{R}[\frac{1}{p}]^\times/(\mathfrak{R}[\frac{1}{p}]^\times)^p)[(\overline{\varphi}^-)^{-1}].$$

Therefore the class of ε in $\mathfrak{R}[\frac{1}{p}]^\times \otimes_{\mathbb{Z}} \mathbb{F}$ is in the $(\overline{\varphi}^-)^{-1}$-eigenspace.

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

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

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

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

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

$$\begin{aligned} 0 \to (\mathfrak{R}^\times \otimes_{\mathbb{Z}} \mathbb{F})[(\overline{\varphi}^-)^{-1}] &\to (\mathfrak{R}[\frac{1}{p}]^\times \otimes_{\mathbb{Z}} \mathbb{F})[(\overline{\varphi}^-)^{-1}] \\ &\to (\mathrm{Ind}_F^{\mathbb{Q}} \mathbb{Z}[\mathrm{Gal}(F(\varphi^-)/F)/D] \otimes_{\mathbb{Z}} \mathbb{F})[(\overline{\varphi}^-)^{-1}] \to 0. \end{aligned}$$

Note that $\overline{\mathbb{Q}}[\mathrm{Gal}(F(\varphi^-)/F)/D]$ contain only characters trivial over D as a sub-quotient. Since $D \cong \varphi^-(\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p))$ is non-trivial by (h1), $\mathbb{Z}[\mathrm{Gal}(F(\varphi^-)/D][\overline{\varphi}^-] = 0$ as $\mathrm{Gal}(F(\varphi^-)/F) \cong \mathrm{Im}(\varphi^-)$ by φ^-. Thus we may assume that $\varepsilon \in \mathfrak{E}_+$ by (D_p) and (D_N). By Proposition 5.1 (1), we have $\mathfrak{R}^\times[(\varphi^-)^{-1}] = 0$, and hence $\mathfrak{R}^\times \otimes_{\mathbb{Z}} \mathbb{F}[(\overline{\varphi}^-)^{-1}] = 0$. This shows that $\mathrm{Hom}_{W[H]}(\mathcal{Y}_{sp}^-(\varphi^-\omega), \mathbb{F}) = 0$, which conclude the proof when $\mathbb{F} = \mathbb{F}_p$.

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

$$\begin{aligned} (5.5)\quad H^1(F, \overline{\varphi}^-\overline{\omega}) &\cong H^0(F(\varphi^-)/F, H^1(F(\varphi^-), \overline{\omega} \otimes_{\mathbb{F}_p} \mathbb{F})) \\ &\cong H^0(F(\varphi^-)/F, F(\varphi^-)^\times \otimes_{\mathbb{Z}} \mathbb{F}) \cong (F(\varphi^-)^\times \otimes_{\mathbb{Z}} \mathbb{F})[(\overline{\varphi}^-)^{-1}], \end{aligned}$$

as $H^1(F(\varphi^-)/F, H^0(F(\varphi^-), M)) = 0$ for any $\mathbb{F}[\mathrm{Gal}(\overline{\mathbb{Q}}/F(\varphi^-))$-module M because of $p \nmid [F(\varphi^-) : F]$. The last identity follows from the fact that ${}^\tau u(g) = \tau u(\tau^{-1}g\tau) = \varphi^-(\tau)u(\tau^{-1}g\tau)$ for cocycle u giving rise to a class $H^1(F, \overline{\varphi}^-\overline{\omega})$ for $\tau \in \mathrm{Gal}(F(\varphi^-)/F)$. By Kummer's theory, non-zero elements in the right-hand-side of (5.5) correspond, up to scalar multiples, bijectively to p-abelian extensions L' of $F(\varphi^-\omega)[\mu_p]$ with $\mathrm{Gal}(L'/F(\varphi^-)[\mu_p]) \cong \mathbb{F}$ such that $\mathrm{Gal}(F(\varphi^-\omega)[\mu_p]/F)$ acts on $\mathrm{Gal}(L'/F(\varphi^-\omega)[\mu_p])$ by $\overline{\varphi}^-\overline{\omega}$ by conjugation. Let $EXT_{/F(\varphi^-\omega)}$ (resp. $EXT_{/F(\varphi^-)[\mu_p]}$) be the set of p-abelian extensions L ($\subset \overline{\mathbb{Q}}$) of $F(\varphi^-\omega)$ (resp. $F(\varphi^-)[\mu_p]$) with $\mathrm{Gal}(L/F(\varphi^-\omega)) \cong \mathbb{F}$ (resp. $\mathrm{Gal}(L'/F(\varphi^-)[\mu_p]) \cong \mathbb{F}$) such that $\mathrm{Gal}(F(\varphi^-\omega)/F)$ (resp. $\mathrm{Gal}(F(\varphi^-)[\mu_p]/F)$) acts on the normal subgroup $\mathrm{Gal}(L/F(\varphi^-\omega))$ via $\overline{\varphi}^-\overline{\omega}$ by conjugation. Non-zero elements in the extension group $H^1(F, \overline{\varphi}^-\overline{\omega}) \cong \mathrm{Ext}_{\mathbb{F}_p[\mathrm{Gal}(\overline{\mathbb{Q}}/F)]}(\mathbb{F}, \overline{\varphi}^-\overline{\omega})$ correspond, up to scalar multiples, bijectively to extensions $\overline{\varphi}^-\overline{\omega} \hookrightarrow X \twoheadrightarrow \mathbb{F}$. As an $\mathbb{F}$-vector space, X is two dimensional, and choosing a basis x_1, x_2 of X over $\mathbb{F}$ so that on $\mathbb{F}x_1$, $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ acts by $\overline{\varphi}^-\overline{\omega}$. For $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/F)$, $(\tau(x_1), \tau(x_2)) = (x_1, x_2)\rho(\tau)$ with $\rho = \begin{pmatrix} \overline{\varphi}^-\overline{\omega} & u \\ 0 & 1 \end{pmatrix}$ for a 1-cocycle u representing X. Since X is a non-trivial extension, the class $[u]$ of u is non-trivial in $H^1(F, \overline{\varphi}^-\overline{\omega})$. Then the splitting field L of X gives rise to an element in $EXT_{/F(\varphi^-\omega)}$. Since cohomologous relation on cocycles u corresponds equivalence relations on ρ by conjugation inside the mirabolic subgroup P, we again conclude that non-zero elements in the left-hand-side of (5.5) correspond, up to scalar multiples, one to one onto to elememnts in $EXT_{/F(\varphi^-\omega)}$. Therefore $EXT_{/F(\varphi^-\omega)} \ni L \mapsto L[\mu_p] \in EXT_{/F(\varphi^-\omega)[\mu_p]}$ is a bijection.

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

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

which is isomorphic to $(\mathfrak{E}_+/\mathfrak{E}_-^p \otimes_{\mathbb{F}_p} \mathbb{F})[(\overline{\varphi}^-)^{-1}]$ as $\mathbb{F}_p$-vector spaces by projecting down to $(\overline{\varphi}^-)^{-1}$-eigenspace in $(\mathfrak{E}_+/\mathfrak{E}_-^p)[\Phi] \otimes_{\mathbb{F}_p} \mathbb{F}$ as

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

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

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

A Kummer cocycle $[\xi] = \xi \otimes 1 \in F(\varphi^-)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ with $\xi \in F(\varphi^-)^\times$ is unramified outside p if its image in $F(\varphi^-)_v^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ vanishes at all finite places $v \nmid p$ of $F(\varphi^-)$. Thus the principal ideal $\xi\mathfrak{R}[\frac{1}{p}]$ is a p-power $\mathfrak{a}^p$. Suppose $[\xi] \in (F(\varphi^-)^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)[\Phi]$. Since $(Cl'_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{Z}_p)[\Phi] = 0$ by our assumption $(Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F})[\overline{\varphi}^-] = 0$, the projected image $[\mathfrak{a}]_\Phi$ in $Cl'_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F}_p[\Phi]$ of the class $[\mathfrak{a}] \in Cl'_{F(\varphi^-)}$ is trivial. Thus replacing $\mathfrak{a}$ and ξ by its Φ-projection (in the fractional ideal group of $\mathfrak{R}[\frac{1}{p}]$) which is principal, we find that $\xi = \varepsilon\xi'^p$ for $\varepsilon \in \mathfrak{R}[\frac{1}{p}]^\times$. Then repeating the same argument in the case of $\mathbb{F} = \mathbb{F}_p$, we conclude $\varepsilon \in \mathfrak{E}_-$ and $\mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) \cong (\mathfrak{E}_+/\mathfrak{E}_-^p)[\Phi]$ as $\mathbb{F}_p$-vector space. Then we have $\mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) \cong (\mathfrak{E}_+/\mathfrak{E}_-^p \otimes_{\mathbb{F}_p} \mathbb{F})[(\overline{\varphi}^-)^{-1}]$, and thus $\mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) = 0$ as $(\varphi^-)^{-1}$ does not appear in $\mathfrak{R}^\times \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}$ by Proposition 5.1. Q.E.D.

§6. Proof of Theorem A

We give a proof of Theorem A uner $p \nmid h_{F(\varphi^-)}$ at the end of this section. We first show that we can add the compatibility (Q9) to the list of the conditions (Q0–8) in Section 3:

(Q9) $\pi_n^{n+1} \circ \sigma_{n+1} = \sigma_n \circ \pi_n^{n+1}$, and the set $\{f_1^{(n)}, \dots, f_r^{(n)}\}$ is made of eigenvectors of σ_n for all n (i.e., $\sigma_n(f_j^{(n)}) = \pm f_j^{(n)}$).

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

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

$\sigma_n \circ \pi_n^{n+1}$ is shown, we get

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

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

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

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

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

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

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

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

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

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

Now suppose that we find an isomorphism class $\mathcal{I}_n$ of the (σ-added) quadruples (indexed by r-sets $Q_m \in \mathcal{Q}$ satisfying (Q0–9) varying m with $m \ge n$) containing infinitely many quadruples of level n whose reduction modulo $(p^{n-1}, \delta_q^{p^{n-1}} - 1)_{q \in Q}$ is in the unique isomorphism

class $\mathcal{I}_{n-1}$ (already specified in the induction process). Since the subset of such $Q \in \mathcal{Q}$ of level $m \geq n+1$ (so $q \equiv 1 \mod p^{n+1}$ for all $q \in Q$) whose reduction modulo $(p^n, \delta_q^{p^n} - 1)_{q \in Q}$ falls in the isomorphism class $\mathcal{I}_n$ is infinite, we may replace $\mathcal{I}_n$ by an infinite subset $\mathcal{I}'_n \subset \mathcal{I}_n$ coming with this property (i.e., $m > n$), and we find an infinite set $\mathcal{I}'_{n+1}$ of $\{((R_{n,m+1}, \alpha), \widetilde{R}_{n,m+1}, (f_1, \dots, f_r), \sigma_{n,m+1})\}_{m \geq n+1}$ which surjects down modulo $(p^n, \delta_q^{p^n} - 1)_{q \in Q}$ isomorphically to a choice

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

at the level n. Indeed if all $q \in Q$ satisfies $q \equiv 1 \mod p^{n+1}$, as we now vary m so that $m > n$ (rather than $m \geq n$), we can use the same $Q = Q_m$ to choose the isomorphism class of level $n+1$. Therefore, for $R_{Q,j} = \mathbb{T}_Q/(p^j, \delta_q^{p^j} - 1)_{q \in Q}$, the projections $R_{Q,n+1} \twoheadrightarrow R_{Q,n}$ and $\widetilde{R}_{Q,n+1} = R_Q/(p^{n+1}, \delta_q^{p^{n+1}} - 1)_{q \in Q} \twoheadrightarrow \widetilde{R}_{Q,n} = R_Q/(p^n, \delta_q^{p^n} - 1)_{q \in Q}$ are compatible with the involutions induced by σ_Q, and hence for the same set of generators $\{f_j\}_j$, the two quadruples

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

of level $j = n+1, n$ are automatically σ_j-compatible.

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

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

Proof. By Proposition 4.4 $|Q_m^-| = \dim_{\mathbb{F}} \mathrm{Hom}_{W[H]}(\mathcal{Y}_{sp}^-(\varphi^- \omega), \mathbb{F})$, and therefore it is independent of m. Q.E.D.

By (Q9), we have the limit involution σ_∞ on $R_\infty = \varprojlim_n R_{n,m(n)}$. We may assume that the generators $(f_1^{(n)}, \dots, f_r^{(n)})$ to satisfy $\sigma_n(f_j^{(n)}) = \pm f_j^{(n)}$. Therefore we may assume that

$$(f_1^{(n)}, \dots, f_r^{(n)}) = (f_{1,+}^{(n)}, \dots, f_{d_+,+}^{(n)}, f_{1,-}^{(n)}, \dots, f_{d_-,-}^{(n)})$$

with $\sigma_\infty(f^{(n)}_{j,\pm}) = \pm f^{(n)}_{j,\pm}$ for $r = d_+ + d_-$, and hence, we may assume that

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

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

$$R_\infty/\mathfrak{A}_Q = W[[T_{1,+}, \dots, T_{d_+,+}, T_{1,-}, \dots, T_{d_-,-}]]/\mathfrak{A}_Q \cong \mathbb{T}_Q. \tag{6.1}$$

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

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

$$\frac{\Lambda[[T_{1,+}, \dots, T_{d_+,+}, T_{1,-}, \dots, T_{d_-,-}]]}{\mathfrak{A}_Q \Lambda[[T_{1,+}, \dots, T_{d_+,+}, T_{1,-}, \dots, T_{d_-,-}]]} \cong \mathbb{T}^Q, \tag{6.2}$$

where $\sigma_\infty(T_{j,\pm}) = \pm T_{j,\pm}$ intact. We write simply

$$\mathcal{R} = \mathcal{R}_\infty := \Lambda[[T_{1,+}, \dots, T_{d_+,+}, T_{1,-}, \dots, T_{d_-,-}]].$$

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

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

Set

$$\mathcal{S} := W[[\mathbf{\Delta}]] = \varprojlim_n W[\mathbf{\Delta}/\mathbf{\Delta}^{p^n}] = \varprojlim_n W[\Delta_n] \tag{6.3}$$

for the p-profinite group $\mathbf{\Delta} = \varprojlim_n \Delta_n \cong \mathbb{Z}_p^r$ with $\mathbf{\Delta} = \mathbf{\Delta}_+ \times \mathbf{\Delta}_-$ and A be a local $\mathcal{S}$-algebra. Thus by identifying $\mathbf{\Delta}/\mathbf{\Delta}^{p^n}$ with Δ_n, we have

the identification $\mathcal{S} = W[[S_1, \dots, S_r]]$. The image $\mathcal{S}_n := W_n[\Delta_n]$ ($W_n = W/p^nW$) of $\mathcal{S}$ in R_n is a local complete intersection and hence Gorenstein. Recall that the ordering of (Q3) is given as $Q_m^- := \{q_1, \dots, q_{r_-}\}$ and $Q_m^+ := \{q_{r_-+1} =: q_1^+, \dots, q_r = q_{r_+}^+\}$. We now write $s_j^\pm$ for the generator of $\mathbf{\Delta}$ corresponding to $\delta_{q_j^\pm}$.

Definition 6.3. *Write $s_j^\pm$ for the generator of $\mathbf{\Delta}_\pm$ corresponding to $\delta_{q_j^\pm}$. Then define $S_j^+ = s_j^+ - 1$ and $S_j^- := s_j^- - (s_j^-)^{-1}$. Thus $\sigma_\infty(S_j^\pm) = \pm S_j^\pm$.*

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

$$\mathfrak{A}_n = \mathfrak{a}_n + ((s_1^-)^{p^n} - 1, \dots, (s_{r_-}^-)^{p^n} - 1) = \mathrm{Ker}(\mathcal{S} \to W_n[\mathbf{\Delta}/\mathbf{\Delta}^{p^n}]) \subset \mathcal{S}$$

as an $\mathcal{S}$-ideal. Then $\mathfrak{A}_n$ is stable under σ. Via the natural projection $\mathbf{\Delta} \twoheadrightarrow \Delta_{Q_m}$ sending $s_j^\pm$ to $\delta_{q_j^\pm}$, we get $\mathfrak{A}_{Q_m} = \mathrm{Ker}(\mathcal{S} \to W[\Delta_{Q_m}])$.

For $Q \in \mathcal{Q}$, recall $r_- = |Q^-|$ with

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

Proposition 6.4. *If $p \nmid h_F$, then $r = d_- = r_- + 1$, $d_+ = 0$ and $r_+ = 1$. In particular $t_Q = t_{\overline{Q}}^-$. If further $p \nmid h_F h_{F(\varphi^-)}$, we have $r_- = 0$ (so, $d_- = 1$). Therefore we have a presentation $\mathbb{T} = \Lambda[[T_-]]/(S_+)$ for $T_- = T_1^-$ and $S_+ = S_1^+$ if $p \nmid h_F h_{F(\varphi^-)}$.*

Proof. By construction, we have $\mathcal{R}/(S_1^+, \dots, S_{r_+}^+, S_1^-, \dots, S_{r_-}^-) \cong \mathbb{T}$, and $\mathcal{R}/\mathcal{R}(\sigma - 1)\mathcal{R}$ has dimension $d_+ + \dim \Lambda = d_+ + 2$, since $\mathcal{R} = \Lambda[T_1^+, \dots, T_{d_+}^+, T_1^-, \dots, T_{d_-}^-]]$ and $\mathcal{R}(\sigma - 1)\mathcal{R} = (T_1^-, \dots, T_{d_-}^-)$.

Suppose $p \nmid h_F = |Cl_F|$, by Proposition 5.2, we have

$$r_+ = \dim_{\mathbb{F}} \mathrm{Sel}_\emptyset^\perp(\overline{\chi\omega}) = 1.$$

If $d_+ > 0$, we have $0 < d_+ \le r_+ = 1$, we have $d_+ = r_+ = 1$ and $d_- = r_-$. Then we get

$$(6.4)\quad (T_1^-, \dots, T_{d_-}^-) \cap \mathcal{S} = \mathcal{R}(\sigma - 1)\mathcal{R} \cap \mathcal{S} \supset \mathcal{S}(\sigma - 1)\mathcal{S} = (S_1^-, \dots, S_{r_-}^-).$$

This means $(T_1^-, \dots, T_{d_-}^-, S_1^+) \supset (S_1^-, \dots, S_{r_-}^-, S_1^+)$ and $\mathbb{T}/\mathbb{T}(\sigma - 1)\mathbb{T} = \mathcal{R}/(T_1^-, \dots, T_{d_-}^-, S_1^+)$, and hence

$$\begin{aligned} 2 > \dim \mathbb{T}/\mathbb{T}(\sigma - 1)\mathbb{T} &= \dim \mathcal{R}/(T_1^-, \dots, T_{d_-}^-, S_1^+) \\ &= \dim \frac{\Lambda[[T_1^-, \dots, T_{d_-}^-, T_1^+]]}{(T_1^-, \dots, T_{d_-}^-, S_1^+)} \ge r + 2 - (d_- + r_+) \ge 2. \end{aligned}$$

The last inequality follows from the fact that the height of the ideal $(T_1^-, \dots, T_{d_-}^-, S_1^+)$ is less than or equal to $d_- + 1 = r_- + r_+ = r$ by [CRT, Theorem 13.5]. This is a contradiction. Therefore, we have $d_+ = 0$, and from $d_+ + d_- = r = r_+ + r_-$, we get $d_- = 1 + r_-$. If further $p \nmid h_{F(\varphi^-)}$, by Proposition 5.3, we have $r_- = 0$. Q.E.D.

Now we would like to prove

Theorem 6.5. *Suppose* (h1–6). *Let $\mathcal{Q}$ be the family satisfies* (Q0–9). *Let $Q \in \mathcal{Q}$ or $Q = \emptyset$. Then the following two assertions holds.*

(1) *The $\mathbb{T}_+^Q$-module $\mathbb{T}_-^Q$ is generated by a single element over $\mathbb{T}_+^Q$.*
(2) *The rings $\mathbb{T}_+ = \mathbb{T}_+^\emptyset$ and $\mathbb{T}^\emptyset$ are both local complete intersection over Λ with presentation $\mathbb{T} \cong \Lambda[[T_-]]/(S_+)$ and $\mathbb{T}_+ \cong \Lambda[[T_-^2]]/(S_+)$ such that σ fixes S_+ and $\sigma(T_-) = -T_-$. More generally, for $Q \in \mathcal{Q}$, the rings $\mathbb{T}_+^Q$ and $\mathbb{T}^Q$ are local complete intersection.*

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

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

We have the limit involution σ_∞ acting on R_∞ which is uniquely lifted to an involution $\sigma := \sigma_\infty$ acting on $\mathcal{R} := \mathcal{R}_\infty$ for $\mathcal{R}_\infty$ defined just below (6.2). Put

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

Let $I_\infty = \mathcal{R}(\sigma - 1)\mathcal{R} = \mathcal{R}\mathcal{R}_-$. Note that $r_\pm := |Q_\pm|$ is independent of Q by Corollary 6.2.

Let $\mathcal{S}_\Lambda = \mathcal{S} \widehat{\otimes}_W \Lambda = \Lambda[[\mathbf{\Delta}]]$. Then plainly $\mathcal{S}_\Lambda$ is flat over $\mathcal{S}_\Lambda^+ := \mathcal{S}_\Lambda^{\mathcal{G}}$, and $\mathcal{R}_-$ is generated over $\mathcal{R}_+$ by a single element δ with $\sigma(\delta) = -\delta$. By Proposition 6.4, we have $\mathcal{R} = \Lambda[[T_-]]$ and $\mathbb{T}^{Q_m} = \Lambda[[T_-]]/(s_+^{|\Delta_{Q_m}|} - 1)$. If a power series $\Phi(T_-)$ is fixed by σ, by equating the coefficients of the identity:

$$\Phi(T_-) = \sigma(\Phi(T_-)) = \Phi(-T_-),$$

we find that Φ is actually a power series of (T_-^2). Thus the fixed part $\mathcal{R}_+ := \mathcal{R}^{\mathcal{G}}$ for $\mathcal{G} = \{\mathrm{id}, \sigma_\infty\}$ is still a power series ring, and we have $\mathcal{R}_+ = \Lambda[[T_-^2]]$. Since $\mathbb{T}_\emptyset = \varprojlim_m \widetilde{R}_m$ by the original Taylor–Wiles argument (e.g., [HMI, page 194]), lifting it to Λ, we get

$$\mathbb{T} = \mathbb{T}^\emptyset = \mathcal{R}/\mathfrak{A}_\emptyset\mathcal{R} = \Lambda[[T_-]]/(S_+),\ \mathbb{T}_+ = \Lambda[[T_-^2]]/(S_+)$$

and $\mathbb{T}_-$ is the surjective image of $\mathcal{R}_-$. Since $\mathcal{R}_-$ is generated by one element δ over $\mathcal{R}_+$ (which can be given by T_-), its image $\mathbb{T}_-$ in $\mathbb{T}$ is

generated by one element θ over $\mathbb{T}_+$. This proves the assertion (1) for $Q=\emptyset$ and the assertion (2) for $\mathbb{T}$ and $\mathbb{T}_+$.

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

$$((R_n,\alpha),\widetilde{R}_{Q,n},(f_1,\dots,f_r),\sigma_n,\phi_n)\in\mathcal{I}_n \tag{6.5}$$

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

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

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

We now prove (2) for general $Q\in\mathcal{Q}$. 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 $\mathcal{S}_\Lambda=\mathcal{S}\widehat{\otimes}_W\Lambda=\Lambda[[\mathbf{\Delta}]]$, and write $s_+=1+S_+$ for the basis of $\mathbf{\Delta}$ corresponding to $\varprojlim_m\delta_{q_1}$. Since $d_-=1$, $\mathcal{R}_+=\Lambda[[T_-^2]]$ and $\mathfrak{s}_Q=\mathfrak{A}_Q\cap S_\Lambda$ is generated by $s^{|\Delta_q|}-1$, $\mathbb{T}^Q_+=\mathcal{R}_+/\mathfrak{s}_Q\mathcal{R}_+$ is a local complete intersection (e.g., [CRT, Exercise 18.1]). Similarly, $\mathbb{T}^Q=\Lambda[[T_-]]/(s_+^{|\Delta_q|}-1)$ is a local complete intersection. Q.E.D.

Here is an example.

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

$$\begin{aligned}W[[T_-]]/((1+S_+)^{p^n}-1)&=W[[T_-]]/((1+T_-^2)^{p^n}-1)\\&\hookrightarrow W[[T_-]]/(T_-^2)\times\prod_{1\neq\zeta\in\mu_{p^n}(\overline{\mathbb{Q}}_p)}W[\zeta][\sqrt{\zeta-1}]\end{aligned}$$

with

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

This tells us that $\mathbb{T}_Q/(\mathbb{T}_Q(\sigma-1)\mathbb{T}_Q)=W$ 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

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

with

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

Without specializing, we have

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

with

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

In this setting, for exterior derivative $f \mapsto df$ having values in

$$t_{\mathcal{R}/(1+S_+)^{p^n}-1))/\Lambda} \cong t^*_{\mathbb{T}^Q/\Lambda} = \mathfrak{m}_{\mathbb{T}^Q}/(\mathfrak{m}^2_{\mathbb{T}^Q}+\mathfrak{m}_\Lambda) \cong \mathfrak{m}_{\mathbb{T}_Q}/(\mathfrak{m}^2_{\mathbb{T}_Q}+\mathfrak{m}_W),$$

we have

$$d((1+S_+)^{p^n}-1) = d((1+T_-^2-T)^{p^n}-1) = p^n(1+T_-^2-T)^{p^n-1}(2T_-dT_- - dT).$$

Taking $n=0$, this shows that $T_-dT^- \in \mathfrak{m}_\Lambda$ and hence $dS_+ = 2T_-dT_- = 0$ in the cotangent space $t^*_{\mathbb{T}^\emptyset/\Lambda}$. For $Q \neq \emptyset$, we still have $T_-dT_- = 0$ as $T_- \in \mathfrak{m}_{\mathbb{T}^Q}$ and $\mathfrak{m}_{\mathbb{T}^Q}$ kills $t^*_{\mathbb{T}^Q/\Lambda}$ and hence compatible with the vanishing $\mathrm{Sel}_\emptyset(\overline{\chi}) = 0 = \mathrm{Sel}_Q(\overline{\chi})$.

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

$$\mathcal{R} = \Lambda[[T_-]] \text{ and } \mathcal{S} = \Lambda[[S_+]]. \tag{6.6}$$

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 $\mathbb{T}^\emptyset_- = \mathbb{T}_-$ is generated by its image θ. This proves the assertion (2). The assertion (1) follows directly from Theorem 6.5 as $d_- = 1$. Q.E.D.

§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 $\mathbb{T}$ and $\mathbb{T}/(t-\gamma^k)$ at the same time. So we write for simplicity $\mathbf{T}$ for either $\mathbb{T}$ or $\mathbb{T}/(t-\gamma^k)$ (choosing $k>0$), and put

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

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

Proposition 7.1. *Let ε be a generator of $O^\times$. Then we have*

$$S_+=f(Y)$$

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

$$\mathbf{T}^{\mathrm{ab}}:=\mathbf{T}/I=\mathbf{T}_+/I_+\cong\begin{cases}\Lambda/(\langle\varepsilon\rangle-1) & \text{if } B=\Lambda,\\ \frac{W}{(\gamma^{k\log_p(\varepsilon)/\log_p(1+p)}-1)} & \text{if } B=\Lambda/(t-\gamma^k),\end{cases}$$

where $I=\mathbf{T}(\sigma-1)\mathbf{T}$ and $X_+=X^{\mathcal{G}}$ for $X=\mathbf{T},I$. In particular, f is a non-unit.

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

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

This shows $(f(0))=(\langle\varepsilon\rangle-1)$. Q.E.D.

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

$$\Omega_{\mathbf{T}/B}\otimes_{\mathbf{T}}\mathbf{T}^{\mathrm{ab}}\cong I/I^2\cong\begin{cases}\Lambda/(\langle\varepsilon\rangle-1) & \text{if } B=\Lambda,\\ W/(\gamma^{k\log_p(\varepsilon)/\log_p(1+p)}-1) & \text{if } B=W.\end{cases}$$

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 $I = \mathbf{T}(\sigma - 1)\mathbf{T}$ regarded as an ideal of $\mathbf{T}$ is the zero ideal (since $\mathbf{T} \otimes_B \mathrm{Frac}(B) = I \otimes_B \mathrm{Frac}(B)$).

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

$$I/I^2 \xrightarrow{i} \Omega_{\mathbf{T}/B} \otimes_{\mathbf{T}} \mathbf{T}^{\mathrm{ab}} \to \Omega_{\mathbf{T}^{\mathrm{ab}}/B} \to 0.$$

Thus $I/I^2 \xrightarrow{i} \Omega_{\mathbf{T}/B} \otimes_{\mathbf{T}} \mathbf{T}^{\mathrm{ab}}$ is surjective. By Proposition 7.1, $\langle\varepsilon\rangle - 1 = S_+ + T_-^2 g(T_-^2)$ for $g(Y) \in \Lambda[[Y]]$. Thus in $\mathbb{T} = \Lambda[[T_-]]/(S_+)$, $\langle\varepsilon\rangle - 1 \in I^2$, and therefore $\Lambda \cap I^2 = \Lambda \cap I = (\langle\varepsilon\rangle - 1)$. This means that the projection $\pi : \mathbb{T}/I^2 \twoheadrightarrow \mathbb{T}/I$ has a section $s : \mathbb{T}/I = \Lambda/(\langle\varepsilon\rangle - 1) \hookrightarrow \mathbb{T}/I^2$ sending $a \in \Lambda/\langle\varepsilon\rangle - 1) = \Lambda/(\Lambda \cap I^2)$ into $\mathbb{T}/I^2$ by the structure morphism $\Lambda \hookrightarrow \mathbb{T}$ mod I^2. Then $D(t) = t - s(\pi(t))$ gives a derivation over Λ. The universality of $\Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} \mathbf{T}^{\mathrm{ab}}$ gives a unique morphism $\iota : \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} \mathbf{T}^{\mathrm{ab}} \to I/I^2$ inducing D. Since ι is onto by construction, $i \circ \iota : \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} \mathbf{T}^{\mathrm{ab}} \to \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} \mathbf{T}^{\mathrm{ab}}$ is an onto $\mathbf{T}^{\mathrm{ab}}$-linear map, which must be an isomorphism. Thus we have $\Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} \mathbf{T}^{\mathrm{ab}} \cong I/I^2$.

From the exact sequence

$$0 \to (S_+)/(S_+)^2 = \mathbf{T} \cdot dS_+ \to \mathbf{T} \cdot dT_- \to \Omega_{\mathbf{T}/B} \to 0, \tag{7.1}$$

tensoring with $\mathbf{T}^{\mathrm{ab}} = \mathbf{T}/I$ over $\mathbf{T}$, we get another exact sequence

$$\mathbf{T}^{\mathrm{ab}} \cdot dS_+ \to \mathbf{T}^{\mathrm{ab}} \cdot dT_- \to (\Omega_{\mathbf{T}/B} \otimes_{\mathbf{T}} \mathbf{T}^{\mathrm{ab}}) = (I/I^2) \to 0. \tag{7.2}$$

We may assume that $f(T_-) = (\langle\varepsilon\rangle - 1) + \sum_{\alpha=1}^{\infty} a_\alpha Y^\alpha$. Since we have $\frac{dY^\alpha}{dT_-} = 2\alpha(T_-)^{2\alpha-1}$, $df(Y)|_{T_-=0} = (\frac{dY^\alpha}{dT_-}|_{T_-=0})dT_- = 0$. Therefore, we get

$$(I/I^2) = \mathrm{Coker}(\mathbf{T}^{\mathrm{ab}} \cdot dS_+^- \to \mathbf{T}^{\mathrm{ab}} \cdot dT_-) = \frac{\mathbf{T}^{\mathrm{ab}} \cdot dT_-}{df(Y))|_{T_-=0}} = \mathbf{T}^{\mathrm{ab}} \cdot dT_-.$$

This shows

$$\Omega_{\mathbf{T}/B} \otimes_{\mathbf{T}} \mathbf{T}^{\mathrm{ab}} \cong I/I^2 \cong \begin{cases} \Lambda/(\langle\varepsilon\rangle - 1) & \text{if } B = \Lambda, \\ W/(\gamma^{k \log_p(\varepsilon)/\log_p(1+p)} - 1) & \text{if } B = W, \end{cases} \tag{7.3}$$

as desired. Q.E.D.

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

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

Theorem 7.4 (B. Mazur)**.** *Assume* (h1–6)*. We have a canonical identity* $\Omega_{\mathbb{T}/\Lambda} \cong \mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))^{\vee}$.

Proof. By Theorem 2.1, the couple $(\mathbb{T}, \rho_{\mathbb{T}})$ is the universal couple for the deformation functor $\mathcal{D}$. Thus we need to prove $\Omega_{R/\Lambda} \cong \mathrm{Sel}_{\mathbb{Q}}(Ad(\boldsymbol{\rho}))$ for the universal couple $(R, \boldsymbol{\rho})$ of $\mathcal{D}$. For the Teichmüller lift ψ of $\det(\overline{\rho})$ and $\boldsymbol{\kappa} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \Lambda^{\times}$ given by

$$\boldsymbol{\kappa}(\sigma) = \psi(\sigma) t^{\log_p(\nu_p(\sigma))/\log_p(1+p)}$$

for $t = 1+T$ and the p-adic cyclotomic character ν_p, the couple $(\Lambda, \boldsymbol{\kappa})$ is the universal couple of minimally ramified deformation outside p. Since $\det(\rho)$ for $\rho \in \mathcal{D}(A)$ is such a deformation, we have a unique W-algebra homomorphism $\iota_A : \Lambda \to A$ such that $\iota_A \circ \boldsymbol{\kappa} = \det(\rho)$. In this way, R is a Λ-algebra by ι_R, and the unique W-algebra homomorphism $\pi : R \to A$ with $\pi \circ \boldsymbol{\rho} \cong \rho$ becomes Λ-algebra homomorphism under the Λ-algebra structure induced by ι_A. Note also that the identification $R \cong \mathbb{T}$ in Theorem 2.1 sends the Λ-algebra structure of R to the weight Λ-algebra structure of $\mathbb{T}$.

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 $\mathrm{GL}_2(A)$ giving rise elements in $\mathcal{D}(A)$; so, $\mathcal{D}(A) = \Phi(A)/\cong$. For each $\rho \in \mathcal{D}(R[X])$ 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 ι_R induces the Λ-module structure on X), and the projection of $\pi : R \to R[X]$ inducing ρ is a Λ-derivation of R with values in X. We consider the W-algebra homomorphism $\xi : R \to R[X]$ with $\xi \mod X = \mathrm{id}$. Then we can write $\xi(r) = r \oplus d_\xi(r)$ with $d_\xi(r) \in X$. By the definition of the product, we get $d_\xi(rr') = r d_\xi(r') + r' d_\xi(r)$ and $d_\xi(W) = 0$. Thus d_ξ is an W-derivation, i.e., $d_\xi \in Der_W(R, X)$. For any derivation $d : R \to X$ over W, $r \mapsto r \oplus d(r)$ is obviously an W-algebra homomorphism, and we get

$$\begin{aligned}(7.4)\quad \big\{\pi \in \Phi(R[X]) \big| \pi \mod X = \boldsymbol{\rho}\big\} / \approx_X \\ \cong \big\{\pi \in \Phi(R[X]) \big| \pi \mod X \cong \boldsymbol{\rho}\big\} / \cong \\ \cong \big\{\xi \in \mathrm{Hom}_{\Lambda\text{-alg}}(R, R[X]) \big| \xi \mod X = \mathrm{id}\big\} \\ \cong Der_\Lambda(R, X) \cong \mathrm{Hom}_R(\Omega_{R/\Lambda}, X),\end{aligned}$$

where "$\approx_X$" is conjugation under $(1 \oplus M_n(X)) \cap GL_2(R[X])$.

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

$$\begin{aligned}\boldsymbol{\rho}(\sigma\tau) \oplus u'_\pi(\sigma\tau) &= (\boldsymbol{\rho}(\sigma) \oplus u'_\pi(\sigma))(\boldsymbol{\rho}(\tau) \oplus u'_\pi(\tau)) \\ &= \boldsymbol{\rho}(\sigma\tau) \oplus (\boldsymbol{\rho}(\sigma)u'_\pi(\tau) + u'_\pi(\sigma)\boldsymbol{\rho}(\tau)),\end{aligned}$$

and we have

$$u'_\pi(\sigma\tau) = \boldsymbol{\rho}(\sigma)u'_\pi(\tau) + u'_\pi(\sigma)\boldsymbol{\rho}(\tau).$$

Define $u_\pi(\sigma) = u'_\pi(\sigma)\boldsymbol{\rho}(\sigma)^{-1}$. Then, $x(\sigma) = \pi(\sigma)\boldsymbol{\rho}(\sigma)^{-1}$ has values in $SL_2(R[X])$ as $\iota_R(\det(\boldsymbol{\rho})) = \iota_{R[X]}(\det(\pi))$, and $x = 1 \oplus u \mapsto u = x - 1$ is an isomorphism from the multiplicative group of the kernel of the reduction map $SL_2(R[X]) \twoheadrightarrow SL_2(R)$ given by

$$\{x \in SL_2(R[X]) | x \equiv 1 \mod X\}$$

onto the additive group

$$Ad(X) = \{x \in M_2(X) | \mathrm{Tr}(x) = 0\} = Ad(\boldsymbol{\rho}) \otimes_R X.$$

Thus we may regard that u has values in $Ad(X) = Ad(\boldsymbol{\rho}) \otimes_R X$.

We also have

$$\begin{aligned}&(7.5)\quad u_\pi(\sigma\tau) = u'_\pi(\sigma\tau)\boldsymbol{\rho}(\sigma\tau)^{-1} \\ &= \boldsymbol{\rho}(\sigma)u'_\pi(\tau)\boldsymbol{\rho}(\sigma\tau)^{-1} + u'_\pi(\sigma)\boldsymbol{\rho}(\tau)\boldsymbol{\rho}(\sigma\tau)^{-1} = Ad(\boldsymbol{\rho})(\sigma)u_\pi(\tau) + u_\pi(\sigma).\end{aligned}$$

Hence u_π is a 1-cocycle unramified outside Np. It is a straightforward computation to see the injectivity of the map:

$$\left\{\pi \in \Phi(R[X]) \middle| \pi \mod X \approx \boldsymbol{\rho}\right\} / \approx_X \hookrightarrow H^1_{ct}(F, Ad(X))$$

given by $\pi \mapsto [u_\pi]$. We put $F_+(X)) = F_+(\boldsymbol{\rho}) \otimes_R X$ for $F_+(\boldsymbol{\rho})$ as in the introduction. Then we see from the fact that $\mathrm{Tr}(u_\pi) = 0$ that

$$(7.6)\qquad u_\pi(I_p) \subset F_+(X) \Leftrightarrow u'_\pi(I_p) \subset F_+(X) \Leftrightarrow \delta_\pi(I_p) = 1.$$

Over the decomposition group $D_p := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, we have

$$(7.7)\qquad u_\pi(D_p) \subset F_-(X) \Leftrightarrow u'_\pi(D_p) \subset F_-(X),$$

where D_p acts trivially on $F_-(X)/F_+(X)$ (i.e., $F_-(\boldsymbol{\rho})$ is upper triangular in $Ad(X)$ under $\boldsymbol{\rho}|_{D_p}$ made upper triangular). Thus the conditions (7.6) and (7.7) is equivalent to requiring $[u_\pi] \in H^1(\mathbb{Q}, Ad(X))$ under restriction map to D_p to be inside $\mathrm{Res}^{-1}_{D_p/I_p}(H^1(I_p, F_+(\boldsymbol{\rho})) \subset H^1(D_p, F_-(\boldsymbol{\rho}))$.

If $\overline{\epsilon}$ ramifies, this is equivalent just to asking that $u_\pi|_{I_p}$ has values in $F_+(\boldsymbol{\rho})$.

For primes $l \nmid Np$, π is unramified at l; so, u_π is trivial on I_l. If $l|N$, we have $\boldsymbol{\rho}|_{I_l} = \epsilon_l \oplus 1$ and $\pi|_{I_l} = \epsilon_l \oplus 1$. Thus $\pi|_{I_l}$ factors through the image of I_l in the maximal abelian quotient of $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ which is isomorphic to $\mathbb{Z}_l^\times$. Thus $u_\pi|_{I_l}$ factors through $\mathbb{Z}_l^\times$. Since $p \nmid \varphi(N)$, $p \nmid l-1$, which implies $u_\pi|_{I_l}$ is trivial; thus u_π unramified everywhere outside p.

Since $R = \varprojlim_n R/\mathfrak{m}_R^n$ for the finite rings $R/\mathfrak{m}_R^n$, we have $R^\vee = \varinjlim_n (R/\mathfrak{m}_R^n)^\vee$. Since H^1 and $\mathrm{Hom}(\Omega_{R/\Lambda}, ?)$ commute with injective limits, taking $X := (R/\mathfrak{m}_R^n)^\vee$ and then passing to the limit, we get

$$\Omega_{R/W}^\vee \cong \mathrm{Hom}_R(\Omega_{R/\Lambda}, R^\vee) \cong \mathrm{Sel}_{\mathbb{Q}}(Ad(\boldsymbol{\rho})) \tag{7.8}$$

as desired. Q.E.D.

Corollary 7.5. *We have* $\mathrm{Sel}_{\mathbb{Q}}(Ad(\mathrm{Ind}_F^{\mathbb{Q}}\Phi))^\vee \cong \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} W[C] \cong \mathbb{T}/I$, *where* C *is the* p*-primary part of* $Cl_F(\mathfrak{c}p^\infty)$ *and* $\Phi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to W[C]^\times$ *given by* $\Phi([x,F]) = \varphi^-([x,F])[x]$ *ofr the Artin symbol* $[x,F]$ *with* $x \in Cl_F(\mathfrak{c}p^\infty)$ *with projection* $[x] \in C$. *If* h_F *is prime to* p, *we have* $\Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} W[C] \cong \mathbb{T}/I \cong \Lambda/(\langle\varepsilon\rangle - 1)$.

Proof. By Corollary 2.3, $\mathbb{T}/I \cong W[C]$ with $\rho_{\mathbb{T}} \cong \mathrm{Ind}_F^{\mathbb{Q}}\Phi$. Then we obtain this result replacing the R-module X in the above proof of Mazur's theorem by a $\mathbb{T}/I$-module X. The last assertion is the restatement of (7.3) and Corollary 7.3. Q.E.D.

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 $\Lambda[[T_-]]/(S_+) = \mathbb{T}$, we have an exact sequence

$$0 \to \mathbb{T}dS_+ \to \mathbb{T}dT_- \to \Omega_{\mathbb{T}/\Lambda} \to 0.$$

We apply a theorem of Tate [MR70, A.3] for

$$(C, R, A, f_1, g_1) = (\mathbb{T}, \Lambda, \Lambda[[T_-]] = \mathcal{R}, S_+, T_- - \theta)$$

under the notation there. Define $\delta \in \mathcal{R} \otimes_\Lambda \mathbb{T} = \mathbb{T}[[T_-]]$ by $S_+ = \delta(T_- - \theta)$, and write $\beta : \mathcal{R} \otimes_\Lambda \mathbb{T} = \mathbb{T}[[T_-]] \to \mathbb{T}$ for the projection; so, $\beta(T_-) = \theta$. Then we have $dS_+ = \delta dT_- + (T_- - \theta)d\delta$. This shows $\Omega_{\mathbb{T}/\Lambda} = \mathbb{T}/(\beta(\delta))$. Thus by Theorem 7.4, $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))^\vee \cong \mathbb{T}/(L)$ with $L := \beta(\delta)$ is cyclic over $\mathbb{T}$. Since $\mathfrak{d}_{\mathbb{T}/\Lambda} = (L)$ for the different $\mathfrak{d}_{\mathbb{T}/\Lambda}$ by [MR70, Appendix], L is a non-zero divisor as $\mathbb{T}$ is reduced and free of finite rank over Λ.

Then $\Omega_{\mathbb{T}/\Lambda}\otimes\mathbb{T}/(\theta)$ is in turn isomorphic to $I/I^2\cong\mathbb{T}/(\theta)\cong\Lambda/(\langle\varepsilon\rangle-1)$ by Corollary 7.3 and Proposition 7.2. Thus

$$\mathbb{T}/(\beta(\delta))\otimes_{\mathbb{T}}\mathbb{T}/(\theta)\cong\Omega_{\mathbb{T}/\Lambda}\otimes_{\mathbb{T}}\mathbb{T}/(\theta)\cong\mathbb{T}/(\theta);$$

so, $(\beta(\delta))\subset(\theta)$. Indeed, evaluating $S_+=\delta(T_--\theta)$ at $T_-=0$, we get $\langle\varepsilon\rangle-1=-\delta(0)\theta$. By Corollary 7.5, we have $\Omega_{\mathbb{T}/\Lambda}\otimes\mathbb{T}/(\theta)\cong\mathrm{Sel}_{\mathbb{Q}}(Ad(\mathrm{Ind}_F^{\mathbb{Q}}\Phi))^\vee$.

References

Books

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

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

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

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

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

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

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

Articles

[BD15] J. Bellaïche and M. Dimitrov, On the Eigencurve at classical weight one points, Duke Math. J. **165** (2016), 245–266.

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

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

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

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

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

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

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

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

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

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

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

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

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

[H17] H. Hida, Anticyclotomic cyclicity conjecture, preprint, 47 pages, 2017, posted at `http://www.math.ucla.edu/~hida/AntCv9.pdf`.

[KR15] C. Khare and R. Ramakrishna, Lifting torsion Galois representations, Forum of Mathematics, Sigma (2015), **3**, 37 pages doi:10.1017/fms.2015.17

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

[MTT] B. Mazur, J. Tate and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Inventiones Math. **84** (1986), 1–48.

[Ra14] R. Ramakrishna, Maps to weight space in Hida families, Indian J. Pure Appl. Math., **45** (2014), 759–776.

[Sh72] G. Shimura, Class fields over real quadratic fields and Hecke operators, Ann of Math. **95** (1972), 130–190.

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

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

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

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