THE UNIVERSAL ORDINARY DEFORMATION RING ASSOCIATED TO A REAL QUADRATIC FIELD

HARUZO HIDA

Abstract. We study ring structure of the big ordinary Hecke algebra $\mathbb{T}$ with the modular deformation $\rho_{\mathbb{T}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ of an induced Artin representation $\mathrm{Ind}_F^{\mathbb{Q}} \varphi$ from a real quadratic field F with a fundamental unit ε, varying a prime $p \geq 3$ split in F. Under mild assumptions (H0–3) below (on the prime p), we prove that $\mathbb{T}$ is an integral domain free of even rank $e > 0$ over Λ for the weight Iwasawa algebra Λ étale outside $\mathrm{Spec}(\Lambda/p(\langle\varepsilon\rangle - 1))$ for $\langle\varepsilon\rangle := (1+T)^{\log_p(\varepsilon)/\log_p(1+p)} \in \mathbb{Z}_p[[T]] \subset \Lambda$. If $p \nmid e$, $\mathbb{T}$ is shown to be a normal noetherian domain of dimension 2 with ramification locus exactly given by $(\langle\varepsilon\rangle - 1)$. Moreover, only under p-distinguishedness (H0), we prove that any modular specialization of weight ≥ 2 of $\rho_{\mathbb{T}}$ is indecomposable over the inertia group at p (solving a conjecture of Greenberg without exception).

1. Introduction

This is a continuation of the research started in [H20] in Iwasawa's anniversary volume. Let $F = \mathbb{Q}[\sqrt{D}]$ be a real quadratic field inside $\mathbb{R}$ with discriminant D and integer ring O. The inclusion $F \subset \mathbb{R}$ gives rise to an infinite place of F denoted by ∞. Take an algebraic closure $\overline{\mathbb{Q}}$ of F in $\mathbb{C}$. Write ς for a field automorphism of $\overline{\mathbb{Q}}$ acting non-trivially on F, and fix a finite order character $\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \overline{\mathbb{Q}}^{\times}$ with conductor $\mathfrak{f}\infty$, where $\mathfrak{f} \neq 0$ is an O-ideal. For each prime $p \geq 3$ split in $F/\mathbb{Q}$, fix an embedding i_p of $\overline{\mathbb{Q}}$ into an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and hence a prime factor $\mathfrak{p}|p$ in O induced by i_p. Thus we have a decomposition $(p) = \mathfrak{p}\mathfrak{p}^{\varsigma}$. Let $\mathbb{Z}_p[\varphi]$ be the discrete valuation ring inside $\overline{\mathbb{Q}}_p$ generated by the values of $i_p \circ \varphi$. Write $\mathbb{F}$ for the residue field of $\mathbb{Z}_p[\varphi]$, and let $W \subset \mathbb{Z}_p[\varphi]$ be the ring of Witt vectors with coefficients in $\mathbb{F}$. We denote by $\overline{\varphi} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathbb{F}^{\times}$ the reduction of φ modulo the maximal ideal $\mathfrak{m}_{\mathbb{Z}_p[\varphi]}$ of $\mathbb{Z}_p[\varphi]$. Write $\mathfrak{c}$ for the prime-to-p part of $\mathfrak{f}$. Put $\rho := \mathrm{Ind}_F^{\mathbb{Q}} \varphi$ and $\overline{\rho} := \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$ which are 2-dimensional representations.

Assuming $\mathfrak{p}^{\varsigma} \nmid \mathfrak{f}$, $\overline{\rho}$ is p-ordinary. When exists, we let $R = R_{\mathbb{Q}}$ be the p-ordinary minimal universal deformation ring of $\overline{\rho}$ over W with prime-to-p conductor $N := N_{F/\mathbb{Q}}(\mathfrak{c})D$. Note $N \geq 5$ (as the discriminant $D = 4$ implies that $F = \mathbb{Q}[\sqrt{-1}]$ is imaginary). It is known that R is noetherian. Writing I_l for the inertia subgroup at a prime l, a deformation $\rho_A : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(A)$ for a local p-profinite W-algebra A with residue field $\mathbb{F}$ is said to be *minimal* if $\rho_A(I_l) \cong \overline{\rho}(I_l)$ by the reduction map modulo $\mathfrak{m}_A$ for all primes $l|N$. We have the corresponding local ring $\mathbb{T}$ of the big ordinary Hecke algebra of prime-to-p level N which is canonically a surjective image of R. The algebra $\mathbb{T}$ is naturally a Λ-algebra for the weight Iwasawa algebra $\Lambda := W[[T]]$, and $\mathbb{T}$ is free of finite rank over Λ ([H86] for $p \geq 5$ and [GME, §3.2.3–4] in general if $Np \geq 4$). Define the anti-cyclotomic part $\phi^- : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to A^{\times}$ of a character $\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to A^{\times}$ by $\phi^- = \phi\phi_{\varsigma}^{-1}$, where $\phi_{\varsigma}(h) = \phi(\varsigma^{-1}h\varsigma)$. Write $F(\rho) = \overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$ for any Galois representation ρ and $Cl_{F(\rho)}$ for the class group of $F(\rho)$ if $[F(\rho) : \mathbb{Q}] < \infty$. Consider the following conditions:

- (H0) the local character $\overline{\varphi}^-|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ is non-trivial (so, $\overline{\rho}$ is absolutely irreducible).
- (H1) $\mathfrak{p}^{\varsigma} \nmid \mathfrak{f}$ (ordinarity; so, the prime to p conductor of $\overline{\rho}$ is given by $N_{F/\mathbb{Q}}(\mathfrak{c})D$).
- (H2) the p-quotient $Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}} \mathbb{F}$ does not contain a non-trivial isotypic component of an irreducible factor of $\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$ (this follows if the class number of $F(\overline{\varphi}^-)$ is prime to p), and the local character $\overline{\varphi}^-|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ is different from the reduction modulo p of the Teichmüller character $\omega = \omega_p$ acting on $\mu_p(\overline{\mathbb{Q}}_p)$.
- (H3) the class number h_F of F is prime to p.

Date: March 10, 2021.
1991 *Mathematics Subject Classification.* primary 11R23, 11F25, 11F33, 11F80; secondary 11F11, 11G18, 11F27.
The author is partially supported by the NSF grant: DMS 1464106.

Under (H0), the universal ring $R_{\mathbb{Q}}$ exists. Since $R_{\mathbb{Q}}$ only depends on $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$, we may replace φ by the Teichmüller lift of $\overline{\varphi}$; so, without losing generality, we assume that φ has order prime to p. We will show as Theorem 2.2 that $\mathbb{T}$ is generated over Λ by a single non-unit Θ for general $\overline{\rho}$ not necessarily an induced representations under assumptions milder than (H0–3) in the induced cases (generalizing the result obtained in [H20] for an induced representation). The identity $R \cong \mathbb{T}$ is known under (H0) ([TW95] and [Th16]). Assuming $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$, we have an involution σ over Λ acting on $\mathbb{T}$ and R corresponding to the operation $\rho \mapsto \rho \otimes \chi$ for $\chi := \left(\frac{F/\mathbb{Q}}{}\right)$ [H20, §2]. Let $\mathbb{T}_+$ be the subring of $\mathbb{T}$ fixed by σ. As is well known (e.g., [H98, §2]), σ is non-trivial on $\mathbb{T}$; so, $\mathbb{T} \neq \Lambda$ and $t^*_{\mathbb{T}/\mathbb{T}_+} := \mathfrak{m}_{\mathbb{T}}/(\mathfrak{m}_{\mathbb{T}}^2 + \mathfrak{m}_{\mathbb{T}_+}) \neq 0$ is generated by the image of $\Theta \in \mathbb{T}$. Replacing Θ by $\Theta^\sigma - \Theta$, we assume that $\Theta^\sigma = -\Theta$ (which will be assumed throughout the paper as long as $\mathbb{T}$ is generated by one element over $\mathbb{T}_+$). We write $t = 1 + T \in \Lambda^\times$ and put $\langle\varepsilon\rangle = t^{\log_p(\varepsilon)/\log_p(1+p)}$ for the fundamental unit ε of F and the p-adic logarithm $\log_p$. The first theorem we prove in Section 4 is

Theorem A: *Assume* (H0–3). *Then $\mathbb{T}$ is an integral domain free of finite even rank $e > 0$ over the weight Iwasawa algebra Λ, and $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a Dedekind domain in which each prime factor of $(\langle\varepsilon\rangle - 1)$ fully ramifies. The ring $\mathbb{T}$ is isomorphic to a power series ring $W[[x]]$ of one variable (via $\Theta \leftrightarrow x$) if and only if $\langle\varepsilon\rangle - 1$ is a prime in Λ (and in this case, we have the identity $(\langle\varepsilon\rangle - 1) = (x)^e$). If $p \nmid e$, $\mathbb{T}$ is a normal domain unramified outside $(\langle\varepsilon\rangle - 1)$, and if $e = 2$, then $\Theta = \sqrt{1 - \langle\varepsilon\rangle}$ up to units.*

Under (H0–3), we show in Theorem 4.1 that we can normalize Θ so that Θ satisfies an Eisenstein polynomial over Λ with respect to each prime factor P of $(\langle\varepsilon\rangle - 1)$ in Λ. Without assuming (H2–3), the number of generators of $\mathbb{T}$ over Λ is more than one. However, only assuming p-distinguishedness (H0) and ordinarity (H1), we prove in Corollary 10.4 the existence of an element $\theta \in \mathbb{T}$ with $\theta^\sigma = -\theta$ such that $\mathrm{Frac}(\mathbb{T}_+[\theta]) = \mathrm{Frac}(\mathbb{T})$ and the integral closure of $\mathbb{T}$ and $\mathbb{T}_+[\theta]$ coincides in their common total quotient ring. This is close to the conjecture: "$\mathbb{T} = \mathbb{T}_+[\sqrt{1 - \langle\varepsilon\rangle}]$" made in a Documenta paper [H98, Conjecture 2.2 (1)] (as an even power of θ coincides with $1 - \langle\varepsilon\rangle$ if we extend scalars from W). The conjecture was made assuming $\mathfrak{f}|\mathfrak{p}$ which implies (H0–1). If we fix an anticyclotomic character φ^- of order ≥ 3 ramified at all infinite places and run primes $\mathfrak{p}$ outside $\mathfrak{f}$, primes satisfying (H0–3) have large Dirichlet density (over F). Indeed, since the conditions (H2–3) do not affect the density, the density is given by the density of primes p such that $\varphi^-([p, F_{\mathfrak{p}}]) \neq 1$, which is given by $\frac{\mathrm{ord}(\varphi^-)-1}{\mathrm{ord}(\varphi^-)}$ for the order $\mathrm{ord}(\varphi^-)$ of φ^- by Chebotarev density theorem. By Bellaïche–Dimitrov [BD16], the rigid analytic localization at each prime factor P of $\langle\varepsilon\rangle - 1$ in the eigencurve associated to $\mathrm{Spec}(\mathbb{T})$ was shown to be a discrete valuation ring (a local result at P in rigid analysis). The ramification of prime divisors P of $(\langle\varepsilon\rangle - 1)$ in the eigencurve was studied in [Di14] via localization at weight 1 Artin points and in [Be17] by an approach in rigid analysis local at P, where one can find a sufficient condition for the ramification index e to be equal to 2. Here we call a prime (or a point) $P \in \mathrm{Spec}(\mathbb{T})(\overline{\mathbb{Q}}_p)$ "Artin" if the associated Galois representation has finite image. We reprove in Proposition 4.3 smoothness given in [BD16] by our global methods through formal geometry. Theorem A and Corollary 10.4 almost determine the global structure of $\mathbb{T}$ over Λ; so, Theorem A in particular asserts that $\mathrm{Spec}(\mathbb{T})$ can ramifies over Λ only at Artin primes $P|(\langle\varepsilon\rangle - 1)$ and possibly at $P|(e)$. Numerical examples given in [DHI98, Table 1] confirm this fact as $\varepsilon^{k-1} - 1$ and the absolute different of the weight k Hecke field fixed by the involution do not have common factor within the table (see Cho's thesis [C99, Chapter 7] about non-common factors). More examples can be found in [DG12, §7.3].

Let Φ be the universal character deforming $\overline{\varphi}$ with minimal ramification outside $\mathfrak{p}$. In [H20, Corollary B], we identified the Pontryagin dual $\mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_F^{\mathbb{Q}} \Phi^-)^\vee$ of the Selmer group $\mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_F^{\mathbb{Q}} \Phi^-)$ with $\Lambda/(\langle\varepsilon\rangle - 1)$ under (H3). Since $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))^\vee$ (defined in (2.1)) is a $\mathbb{T}$-module isomorphic to $\Omega_{\mathbb{T}/\Lambda}$ by Theorem A.1 and $\Omega_{\mathbb{T}/\Lambda} \cong \mathbb{T}/(\Theta)^{e-1}$ up to p-torsion for the element $\Theta \in \mathbb{T}$, Theorem A implies

Corollary B: *Assume* (H0–3). *Then we have an isomorphism* $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))^\vee \cong \mathbb{T}/(\Theta^{e-1})$ *of $\mathbb{T}$-modules if $p \nmid e$ and in general,* $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))^\vee \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}/(\Theta^{e-1})$ *as $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$-modules. Moreover* $\mathrm{Sel}_{\mathbb{Q}}(\mathrm{Ind}_F^{\mathbb{Q}} \Phi^-)^\vee \cong \Lambda/(\langle\varepsilon\rangle - 1)$ *as Λ-modules, where* $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))^\vee$ *is the Pontryagin dual of the adjoint Selmer group* $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))$.

Here is an expectation generalizing [H98, Conjecture 2.2]:

Semi-simplicity conjecture: *Suppose* (H0–3). *Then we have $e = 2$, and hence the Selmer group* $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))^\vee \otimes_W \mathrm{Frac}(W)$ *is a semi-simple* $\mathbb{T}$*-module over the field* $\mathrm{Frac}(W)$ *of fractions of* W.

Under (H0–3), if the above conjecture holds, by Corollary B, we have $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}})) \cong \Lambda/(\langle\varepsilon\rangle - 1)$ and hence $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho_{\mathbb{T}}))^\vee \otimes_W \mathrm{Frac}(W)$ is semi-simple as $\langle\varepsilon\rangle - 1$ is square-free.

Let $\mathbb{T}_F$ be the local ring of the big cuspidal p-ordinary F-Hilbert modular Hecke algebra over Λ of prime-to-p level $\mathfrak{C} := \mathfrak{c} \cap \mathfrak{c}^\varsigma$ having residual Galois representation $\overline{\varphi} \oplus \overline{\varphi}_\varsigma$. Here "$p$-ordinarity" is not a standard one as we will describe in §5.4. We will prove that $\mathbb{T}_F$ is the universal ring among pseudo characters deforming $\overline{\varphi} + \overline{\varphi}_\varsigma$ with an appropriate determinant condition of Chenevier [Ch14]. We have the base-change algebra homomorphism $\beta : \mathbb{T}_F \to \mathbb{T}_+$ over the weight Iwasawa algebra $\Lambda := W[[T]]$ dual to deformations ρ sent to $\mathrm{Tr}(\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)})$ (see [DHI98, §3.4]).

Theorem C: *Assume* (H0–2). *Then β induces an isomorphism $\mathbb{T}_F \cong \mathbb{T}_+$, and $\mathbb{T}_F$ is the (minimal) universal deformation ring over* $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ *of the modulo p pseudo-character* $\mathrm{Tr}(\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)})$.

In [H98, Conjecture 2.2 (3)], we predicted that β is onto under $\mathfrak{f}|\mathfrak{p}$, but actually β is shown to be an isomorphism under an extra assumption (H2). Theorem C implies the Galois side of [DHI98, Conjecture 1.5] (which is stronger than [ibid. Conjecture 3.8] applied to $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$), and the analytic side would be proven if we can prove the adjoint class number formula for $\rho_{\mathbb{T}}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}$ and the integral period relation [DHI98, Conjecture 1.3] without assuming absolute irreducibility of $\overline{\rho}$ over F. The expected p-integral period relation and the adjoint class number formula have been shown in [TU20] if the residual representation is full (i.e., its image contains $\mathrm{SL}_2(\mathbb{F}_p)$).

By the determination of the image under $\rho_{\mathbb{T}}$ of an inertia subgroup at p, we produce the element $\theta \in \mathbb{T}$ mentioned after stating Theorem A, and we prove in Section 10 that $\theta \notin P$ for $P \in \mathrm{Spec}(\mathbb{T})(\overline{\mathbb{Q}}_p)$ if and only if the Galois representation ρ_P associated to P is p-locally indecomposable (as conjectured by R. Greenberg), supplementing results in [GV04], [Z14] and [CWE19] (see the introduction of [CWE19] for more details of Greenberg's conjecture and another related conjecture by R. Coleman):

Theorem D: *Assume* (H0–1). *Let f be a Hecke eigenform of level N whose Galois representation ρ_f is a minimal deformation of $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$. If f has weight ≥ 2, ρ_f restricted to the inertia subgroup at p is indecomposable. Indeed, for any prime divisor* $P \in \mathrm{Spec}(\mathbb{T})(\overline{\mathbb{Q}}_p)$ *outside* $(\langle\varepsilon\rangle - 1)$, $\rho_P = (\rho_{\mathbb{T}} \bmod P)$ *is indecomposable over the inertia subgroup at p.*

The indecomposability is proven for non CM modular deformation of an induced representation $\mathrm{Ind}_K^{\mathbb{Q}} \overline{\varphi}$ for an imaginary quadratic field K in [CWE19] under the conditions analogous to (H0–2) and an extra condition requiring $\overline{\varphi}^-$ has order ≥ 3. This theorem does not require the extra condition nor (H2), and we discuss in [EMI, §8.5] to what extent we can remove the assumptions made in [CWE19] in the case of imaginary K. If $\overline{\rho}$ is also induced from an imaginary quadratic field K, $\varphi^- = \left(\frac{FK/F}{}\right)$ by [H15, Proposition 5.2 (2)]; so, by (H0), p is either inert or ramified in K. This implies that there is no CM irreducible component of $\mathrm{Spec}(\mathbb{T})$; so, no CM forms f of weight ≥ 2 such that ρ_f is a deformation of $\overline{\rho}$.

Here is an outline of the paper. Without assuming the "$R = \mathbb{T}$" theorem (due to Taylor–Wiles and others), under some mild conditions, we exhibit the presentation $\Lambda[[X]]/(S) \cong \mathbb{T}$ for a p-tamely ramified odd absolutely irreducible p-distinguished residual representations (see Theorem 2.2) not necessarily induced from a quadratic field. For $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$, assuming (H0–2), by this presentation theorem, $\mathbb{T}$ is free of rank 2 over $\mathbb{T}_+$, and $\mathbb{T}_+$ is in particular a local complete intersection over Λ (flat over Λ). After recalling the definition of adjoint Selmer groups in Section 3, analyzing the distinguished polynomial factor $D(X)$ of the power series $S = S(X)$, we show in Section 4 that $D(X)$ is an Eisenstein polynomial (relative to each prime divisor of $(\langle\varepsilon\rangle - 1)$) with constant term given by a unit multiple of $\langle\varepsilon\rangle - 1$. Thus $\mathbb{T}$ is an integral domain fully ramified over Λ at each prime factor of $\langle\varepsilon\rangle - 1$, proving Theorem A and reproving the local smoothness result of [BD16]. Under (H0), we have a representation $\rho_{\mathbb{T}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T})$ universal among modular deformations of $\overline{\rho}$ with minimal ramification data. Since the residual representation of $\rho_{\mathbb{T}}$ restricted to $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ is no longer irreducible, we do not expect to have an $R = \mathbb{T}$ theorem over F in the usual sense. However, we are able to identify the subring $\mathbb{T}_+$ with the universal ordinary pseudo character ring with a Cayley–Hamilton representation $\boldsymbol{\rho}^{ord} := \rho_{\mathbb{T}}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}$ having values in a generalized matrix

$\mathbb{T}_+$-algebra ($\mathbb{T}_+$-GMA) in the sense of Bellaïche–Chenevier [FGS]. Ordinarity for pseudo characters over F is defined similarly to [WWE17] and [CV03, page 93] (but we need some extra care as we have two primes at p in F). We recall the theory of pseudo characters in Section 5, make explicit the universal reducible Cayley–Hamilton representation in Section 6 and $\boldsymbol{\rho}^{ord}$ in Section 8 and prove Theorem C in Section 7 via universality of the reducible locus. After recalling in Section 9 a generalization of a result of Iwasawa from [H21], Theorem D is proven in Section 10 after a careful analysis (via the results in Section 9) of the image of an inertia subgroup at $\mathfrak{p}$ under $\rho_{\mathbb{T}}$ showing the obstruction of decomposability is given precisely by the ideal $(\langle\varepsilon\rangle - 1)$ (Corollary 10.4). In Appendix A, we prove a precise control of the adjoint Selmer group used in the main text, and in Appendix B, we construct a p-adic L-function on Spec($\mathbb{T}$) interpolating the adjoint L-values. In these two appendices, we do not assume that $\overline{\rho}$ is an induced representation.

We supply back-ground details of the result presented here in a forthcoming book [EMI, Chapters 7–8] and discuss related open questions.

Throughout this paper, writing B for a base p-profinite noetherian local ring with residue field $\mathbb{F}$, all deformation functors are from the category $CNL = CNL_{/B}$ of local noetherian p-profinite B-algebras with residue field $\mathbb{F}$ whose morphisms are continuous local B-algebra homomorphisms. The ring B is either W or $\Lambda = W[[T]]$. For each object A of CNL, we denote by $\mathfrak{m}_A$ its maximal ideal, and for each p-profinite A-module M, $M^\vee$ denotes its Pontryagin dual module. When A as above is an A_0-algebra for $A_0 \in CNL$, we write $t^*_{A/A_0} = \mathfrak{m}_A/(\mathfrak{m}_A^2 + \mathfrak{m}_{A_0}) = \Omega_{A/A_0} \otimes_A \mathbb{F}$ (the cotangent space of A over A_0). We call a prime ideal P of a ring A a prime divisor of $\alpha \in A$ (resp. of an A-ideal $\mathfrak{a}$) if P has height 1 and $P \supset (\alpha)$ (resp. $P \supset \mathfrak{a}$). For a number field X and an integral ideal $\mathfrak{a}$ of X, we write $Cl_X(\mathfrak{a})$ (resp. $Cl^+_X(\mathfrak{a})$) for the ray class group modulo $\mathfrak{a}$ (resp. in the strict sense). If $\mathfrak{a}$ is trivial, we just write Cl_X and Cl^+_X. For each representation ψ of Gal(Y/X), we denote by $F(\psi)$ for the splitting field $Y^{\mathrm{Ker}(\psi)}$ of ψ. If ψ is a character with values in $\overline{\mathbb{Q}}_p$, we write $\mathbb{Z}_p[\psi]$ for the subring generated by the values of ψ over $\mathbb{Z}_p$. For a topological group $\mathcal{H}$, we write $\mathcal{H}^{ab}$ for the maximal (continuous) abelian quotient of $\mathcal{H}$. We fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. We write $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and identifying $\overline{\mathbb{Q}}_p$ with $\mathbb{C}$ once and for all, we regard $\overline{\mathbb{Q}}$ also a subfield of $\overline{\mathbb{Q}}_p$. Since $F \subset \mathbb{R} \subset \mathbb{C}$, we have a unique embedding $F \hookrightarrow \overline{\mathbb{Q}}$ which induces by the above identification a unique p-adic place and infinite place of F.

Contents

2. Presentation of the universal deformation ring

In this section, we start with a general odd residual representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ ($\mathbb{F}/\mathbb{F}_p$: finite) of prime-to-p conductor N. The following set-up is always assumed in this section:

(s1) Fix a prime $p \geq 3$ and an **absolutely irreducible odd** representation $\overline{\rho}$.

(s2) Write $F(\rho) := \overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$ for any Galois representation ρ.

(s3) $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \cong \overline{\epsilon} \oplus \overline{\delta}$ (*residually split at* p); $\overline{\delta} \neq \overline{\epsilon}$; $\overline{\delta}$ unramified.

(s4) Ramification index of every prime in $F(\overline{\rho})_{/\mathbb{Q}}$ is prime to p;

(s5) Write $F^{(p)}(\overline{\rho})$ for the maximal p-profinite extension of $F(\overline{\rho})$ *unramified outside* p with $G := \mathrm{Gal}(F^{(p)}(\overline{\rho})/\mathbb{Q})$, and set D_l (resp. I_l) for the decomposition (resp. inertia) subgroup at a prime l of G.

(s6) Let $(R, \boldsymbol{\rho} : G \to \mathrm{GL}_2(R))$ be the p-ordinary universal deformation over the category CNL of local p-profinite W-algebras with residue field $\mathbb{F}$. Here $W = W(\mathbb{F})$ is the Witt vector ring with coefficients in $\mathbb{F}$. So the functor $A \mapsto \mathcal{D}(A)$ represented by R is given by

$$\mathcal{D}(A) = \{\rho_A : G \to \mathrm{GL}_2(A) | \rho_A \bmod \mathfrak{m}_A = \overline{\rho},\ \rho_A|_{D_p} = \left(\begin{smallmatrix} \epsilon & * \\ 0 & \delta \end{smallmatrix}\right), \delta|_{I_p} = 1 \text{ and } (\delta \bmod \mathfrak{m}_A) = \overline{\delta}\}/\Gamma(\mathfrak{m}_A),$$

where $\Gamma(\mathfrak{m}_A) = \mathrm{Ker}(\mathrm{GL}_2(A) \xrightarrow{\bmod \mathfrak{m}_A} \mathrm{GL}_2(\mathbb{F}))$ acts on deformations by conjugation.

Since $Ad(\rho \otimes \xi) = Ad(\rho)$ with a Galois character ξ for a deformation ρ, as long as the statement concerns with $Ad(\rho)$, we assume, replacing $\overline{\rho}$ by a suitable character twist, that for a ramified prime $l \neq p$ in $F(\overline{\rho})/\mathbb{Q}$,

(l) If $\overline{\rho}|_{I_l} \cong \overline{\epsilon}_l \oplus \overline{\delta}_l$, then $\overline{\epsilon}_l \neq \overline{\delta}_l$.

If $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$ for a character $\overline{\varphi} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathbb{F}^{\times}$ satisfying (H0–1), the representation $\overline{\rho}$ satisfies the requirements (s1–5). We need to verify the conditions (s3–4). Since $\overline{\varphi}$ has values in $\mathbb{F}^{\times}$ and $p \nmid |\mathbb{F}^{\times}|$, we have $p \nmid [F(\overline{\rho}) : \mathbb{Q}] = |\mathrm{Im}(\overline{\rho})|$ as $p > 2$. This shows (s4). Since p splits in F, $D_p \subset H := \mathrm{Gal}(F^{(p)}(\overline{\rho})/F)$, and hence $\overline{\rho}|_{D_p} \cong \overline{\varphi} \oplus \overline{\varphi}_{\varsigma}$; so, (s3) holds by (H0).

The condition (s3) together with (l) does not implies (s4). In other words, there can be a prime $l \neq p$ for which $\overline{\rho}|_{D_l}$ cannot be diagonal but still $\overline{\rho}(I_l)$ has order prime to p. For example, if $\overline{\rho}|_{D_l}$ is an induced representation from a ramified quadratic extension of $\mathbb{Q}_l$ of a ramified character, $\overline{\rho}(I_l)$ is a non-abelian dihedral group which cannot be diagonalized in $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ (and there are more complicated examples of non-dihedral non-abelian irreducible image if $l = 2$ [W74, §36]).

By (s4), for a prime $l \neq p$, I_l is finite with order prime to p. Therefore the universal ring deforming $\det(\overline{\rho})$ over G is the Iwasawa algebra $\Lambda := W[[T]]$ with universal character κ satisfying $\kappa([1+p, \mathbb{Q}_p]) = t$ ($t := 1+T$) (i.e., $\kappa([z, \mathbb{Q}_p]) = t^{\log_p(z)/\log_p(1+p)}$). Since $\det(\boldsymbol{\rho})$ is a deformation of $\det(\overline{\rho})$, we have a unique Λ-algebra structure $\iota_R : \Lambda \to R$ so that $\iota_R \circ \kappa = \det(\boldsymbol{\rho})$, giving a canonical Λ-algebra structure on R.

For each $\rho \in \mathcal{D}(A)$, write $Ad(\rho)$ for the three dimensional adjoint representation acting on $\mathfrak{sl}_2(A)$ by conjugation action of ρ. For the Pontryagin dual $A^{\vee}$ of A, we define the discrete Galois module $Ad(\rho)^*$ by $Ad(\rho) \otimes_A A^{\vee}$ with Galois action through the factor $Ad(\rho)$.

Let N be the prime to p conductor of $\overline{\rho}$. Let $\mathbf{h}$ be the big Hecke algebra described in [H20, §1] of prime-to-p level N (though we do not assume that N is cube-free as in [H20]). We have a local ring $\mathbb{T}$ of $\mathbf{h}$ whose residual representation is isomorphic to $\overline{\rho}$. Let $\rho_{\mathbb{T}} : G \to \mathrm{GL}_2(\mathbb{T})$ be the Galois representation of $\mathbb{T}$ such that $\mathrm{Tr}(\rho_{\mathbb{T}}(\mathrm{Frob}_l))$ for primes l outside $\{l|Np\}$ is given by the image in $\mathbb{T}$ of the Hecke operator $T(l)$. The algebra $\mathbb{T}$ is an algebra over Λ via $\det(\rho_{\mathbb{T}})$ which is a deformation of $\det(\overline{\rho})$ over G. As already mentioned, $\mathbb{T}$ is free of finite rank over Λ.

Lemma 2.1. *Suppose that the prime-to-p level of $\mathbb{T}$ coincides with the prime-to-p conductor of $\overline{\rho}$. Then the local ring $\mathbb{T}$ is reduced.*

The reducedness of $\mathbb{T}$ easily follows from minimality of $\mathbb{T}$ (which implies the assumption of the lemma), but it seems no exact reference of this fact; so, let us insert here the argument proving this fact.

Proof. We use the notation in [GME, Corollary 3.2.22] in the proof, and write $K := W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ (the field of fractions of W). By our choice, the prime-to-p conductor of the residual representation $\overline{\rho}$ gives the prime-to-p level N of the Hecke algebra. Therefore each modular deformation parameterized by $\mathbb{T}$ has the prime to p-conductor N (so, any Hecke eigenform belonging to $\mathbb{T}$ has prime to p-conductor

N; i.e., N-new). Pick a weight $k > 2$ and $\mathbb{T}_k = \mathbb{T}/(t-\gamma^k)\mathbb{T}$ for $t = 1+T$ and $\gamma = 1+p$. By the control theorem [GME, Corollary 3.2.22], $\mathbb{T}_k$ is a direct factor of the ordinary Hecke algebra $\mathbf{h}_k := \mathbf{h}_k^{ord}(\Gamma_0(Np), \psi\omega^{-k}; W)$ generated by all $T(n)$ over W inside $\mathrm{End}_W(S_k^{ord}(\Gamma_0(Np), \psi\omega^{-k}; W))$ for a Dirichlet character ψ modulo Np independent of k and the Teichmüller character ω (in [GME, Corollary 3.2.22], the symbol χ is used for ψ here). We can decompose $\mathbf{h}_k \otimes_W K = \mathbf{h}_k(K)^{new} \times \mathbf{h}_k(K)^{old}$ so that $\mathbf{h}_k(K)^{new}$ (resp. $\mathbf{h}_k(K)^{old}$) acts on the subspace of $S_k^{ord}(\Gamma_0(Np), \psi\omega^{-k}; K)$ ($K := W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$) spanned by the N-new (resp. N-old) forms. If $\psi\omega^{-k}$ has conductor prime to p and $k > 2$, new forms in $S_k(\Gamma_0(Np), \psi\omega^{-k})$ are non-p-ordinary [MFM, Theorem 4.6.17 (2)]. Thus we know $\mathbf{h}_k^{ord}(\Gamma_0(Np), \psi\omega^{-k}; W) \cong \mathbf{h}_k^{ord}(\Gamma_0(N), \psi\omega^{-k}; W)$ by $k > 2$, and if $\psi\omega^{-k}$ has p-conductor equal to p, every N-new form in $S_k^{ord}(\Gamma_0(Np), \psi\omega^{-k})$ is a new form. Then by the theory of new forms [MFM, §4.6], $\mathbf{h}_k(K)^{new}$ is a semi-simple commutative K-algebra. Let $\mathbf{h}_k^{old}$ be the projected image of $\mathbf{h}_k$ in $\mathbf{h}_k(K)^{old}$. If $\mathbb{T}_k$ projects to $\mathbf{h}_k^{old}$ non-trivially, we have $\mathbb{T}_k/\mathfrak{m}_{\mathbb{T}_k} \cong \mathbf{h}_k^{old}/\mathfrak{m}$ for a maximal ideal $\mathfrak{m}$ of $\mathbf{h}_k^{old}$. Then the $\mathfrak{m}$-residual representation has prime-to-p conductor less than N, a contradiction; so, $\mathbb{T}_k \subset \mathbf{h}_k(K)^{new}$ and hence $\mathbb{T}_k$ is reduced. Since $\mathbb{T}$ is embedded into $\prod_k \mathbb{T}_k$ by the diagonal embedding, $\mathbb{T}$ must be reduced. □

For each $\lambda \in \mathrm{Hom}_{CNL}(\mathbb{T}, \overline{\mathbb{Q}}_p)$, we have a p-adic modular form $f_\lambda = \sum_{n=1}^{\infty} \lambda(T(n))q^n$ with $\rho_\lambda := \lambda \circ \rho_{\mathbb{T}} \in \mathcal{D}(W_\lambda)$ ($W_\lambda := W[\lambda(T(n))]_n \subset \overline{\mathbb{Q}}_p$) such that $\rho_\lambda|_{D_p} = \left(\begin{smallmatrix} \epsilon_\lambda & u_\lambda \\ 0 & \delta_\lambda \end{smallmatrix}\right)$. If $\det(\rho_\lambda) = \nu_p^{k-1}$ (for the p-adic cyclotomic character $\nu_p : G \to \mathbb{Z}_p^\times$) on a *open* subgroup of I_p with $2 \le k \in \mathbb{Z}$, f_λ is classical. When $k = 1$, f_λ is classical if and only if ρ_λ has finite image.

For a subfield M of $F(\rho_{\mathbb{T}})$, writing G_M for the subgroup of G fixing M and $D_\wp \subset G_M$ for the decomposition subgroup of a prime $\wp|p$ of M, we define the Selmer group $\mathrm{Sel}(Ad(\rho))$ for any $\rho \in \mathcal{D}(A)$ by

$$\mathrm{Sel}_M(Ad(\rho_A)) := \mathrm{Ker}(H^1(G_M, Ad(\rho_A)^*) \to \prod_{\wp|p} \frac{H^1(D_\wp, Ad(\rho_A)^*}{F^+_{-,\wp} H^1(D_\wp, Ad(\rho_A)^*)}), \tag{2.1}$$

where $\wp$ runs over all prime factors of p in M, and choosing $a_\wp \in \mathrm{GL}_2(A)$ so that $a_\wp \rho_A a_\wp^{-1}|_{D_\wp} = \left(\begin{smallmatrix} \epsilon_\wp & * \\ 0 & \delta_\wp \end{smallmatrix}\right)$ with $\delta_\wp$ unramified and $\delta_\wp \bmod \mathfrak{m}_A = \overline{\delta}$, $a_\wp F^+_{-,\wp} H^1(D_\wp, Ad(\rho)^*) a_\wp^{-1}$ is made of cohomology classes *upper triangular over $D_\wp$ and upper nilpotent over the inertia subgroup $I_\wp$ of $D_\wp$*. In prevalent definitions of the Selmer group, local unramifiedness conditions for primes outside p is imposed. However by (s4) (and the definition of G), the unramifiedness is automatically satisfied (and the local condition does not appear here). We just write $\mathrm{Sel}(Ad(\rho))$ for $\mathrm{Sel}_{\mathbb{Q}}(Ad(\rho))$.

We generalize, to non-induced $\overline{\rho}$, the following fact in [H20] proven for an induced residual representation $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$ under some extra assumptions.

Theorem 2.2. *Let the notation be as above. Assume that $Cl_M \otimes_{\mathbb{Z}[G]} Ad(\overline{\rho}) = 0$ for $M = F(Ad(\overline{\rho}))$ and that the Galois module $Ad(\overline{\rho})|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ does not contain $\mathbb{F}(1) := \mu_p(\overline{\mathbb{Q}}_p) \otimes_{\mathbb{F}_p} \mathbb{F}$ as a Galois subquotient. Then we have $\mathbb{T} \cong \Lambda[[X]]/(S)$ for the one variable power series ring $\Lambda[[X]]$.*

The theorem does not assert $\mathbb{T} \neq \Lambda$ (i.e., the power series $S = S(X)$ can be linear in X). If $\mathbb{T} \neq \Lambda$, writing Θ for the image of X in $\mathbb{T}$, the characteristic polynomial $D(X)$ of the Λ-linear endomorphism of $\mathbb{T}$: $x \mapsto \Theta x$ gives the distinguished polynomial factor $D(X)$ of $S(X)$, and $\mathbb{T} \cong \Lambda[X]/(D(X))$.

Proof. Since $\mathbb{T}$ is free of finite rank over Λ, if $\mathbb{T}$ is generated by one element $\Theta \in \mathfrak{m}_{\mathbb{T}}$ over Λ, the multiplication by Θ on $\mathbb{T}$ has its characteristic polynomial $D(X)$ of degree $e = \mathrm{rank}_\Lambda \mathbb{T}$ which is a distinguished polynomial with respect to $\mathfrak{m}_\Lambda$ satisfying $\mathbb{T} = \Lambda[X]/(D(X))$. Since $\mathbb{T}$ is generated by $\mathrm{Tr}(\rho_{\mathbb{T}})$ and by p-distinguishedness (s3), the morphism $\pi : R \to \mathbb{T}$ with $\pi \circ \boldsymbol{\rho} \cong \rho_{\mathbb{T}}$ is surjective. Thus we need to prove that R is generated by at most one element over Λ. In other words, we prove that $t^*_{R/\Lambda} := \mathfrak{m}_R/(\mathfrak{m}_R^2 + \mathfrak{m}_\Lambda)$ has dimension ≤ 1 over $\mathbb{F}$.

As is well known, we have $t^*_{R/\Lambda} = \Omega_{R/\Lambda} \otimes_R \mathbb{F} \cong \mathrm{Sel}(Ad(\overline{\rho}))^\vee$ canonically; see Theorem A.1. Write $\overline{G} = \mathrm{Gal}(F(Ad(\overline{\rho}))/\mathbb{Q})$. If $p \nmid |\overline{G}|$, plainly $H^1(\overline{G}, Ad(\overline{\rho})^*) = 0$. Otherwise, by Dickson's classification, $\overline{G}$ is isomorphic to either $\mathrm{PSL}_2(\mathbb{F}')$, $\mathrm{PGL}_2(\mathbb{F}')$ for a subfield $\mathbb{F}'$ of $\mathbb{F}$ or A_5 (when $p = 3$), and we know $H^1(\overline{G}, Ad(\overline{\rho})^*) = 0$ (e.g., [Wi95, Proposition 1.11] and [CPS75]). Thus by restriction, for $M = F(Ad(\overline{\rho}))$, we find $\mathrm{Sel}(Ad(\overline{\rho})) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}[G]}(G_M, Ad(\overline{\rho})^*)$. Plainly this map factors through $\mathrm{Sel}_M(Ad(\overline{\rho}))$ inducing an injection $\mathrm{Sel}(Ad(\overline{\rho})) \hookrightarrow \mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}}$. Thus we need to show $\dim_{\mathbb{F}} \mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}} \le 1$ under our assumptions.

Let $\mathcal{O}$ be the integer ring of M, $\mathcal{O}_p = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and $\widehat{\mathcal{O}_p^\times} = \varprojlim_n \mathcal{O}_p^\times/(\mathcal{O}_p^\times)^{p^n}$ (the maximal p-profinite quotient of $\mathcal{O}_p^\times$). Similarly set $\widehat{\mathcal{O}_{\mathfrak{p}}^\times} = \varprojlim_n \mathcal{O}_{\mathfrak{p}}^\times/(\mathcal{O}_{\mathfrak{p}}^\times)^{p^n}$ for each prime factor $\mathfrak{p}|p$. We fix a prime $\mathcal{O}$-ideal $\mathfrak{p}_0|p$ and choose the inertia group I_0 at $\mathfrak{p}_0$ of G_M so that $\rho_{\mathbb{T}}|_{I_0}$ has values in upper triangular subgroup with the trivial quotient character. For each $\mathfrak{p}|p$, we pick $g_{\mathfrak{p}} \in G$ and put $I_{\mathfrak{p}} := g_{\mathfrak{p}} I_0 g_{\mathfrak{p}}^{-1} \subset G_M$ is a inertia subgroup of $\mathfrak{p}$. By local class field theory, the image $I_{\mathfrak{p}}^{ab}$ of $I_{\mathfrak{p}}$ in the maximal abelian quotient G_M^{ab} of G_M is the surjective image of $\widehat{\mathcal{O}_{\mathfrak{p}}^\times}$. By class field theory, $\widehat{\mathcal{O}_p^\times} \to G_M^{ab} \twoheadrightarrow C_M$ for $C_M := Cl_M \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is exact, and applying $\mathrm{Hom}_{\mathbb{Z}[\overline{G}]}(?, Ad(\overline{\rho}))$, we get an exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}[\overline{G}]}(C_M, Ad(\overline{\rho})) \cap \mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}} \to \mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}} \xrightarrow{\pi} \mathrm{Hom}_{\mathbb{Z}_p[\overline{G}]}(\widehat{\mathcal{O}_p^\times}, Ad(\overline{\rho}))$$

with $\mathrm{Im}(\pi)$ made of ramified Selmer cocycles at p by local class field theory. Here π factors through the dual map: $\mathrm{Hom}_{\mathbb{Z}_p[\overline{G}]}(I_0^{ab}, Ad(\overline{\rho})) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_p[\overline{G}]}(\widehat{\mathcal{O}_p^\times}, Ad(\overline{\rho}))$ of the surjective Artin map: $\widehat{\mathcal{O}_p^\times} \twoheadrightarrow I_0^{ab}$. Therefore, identifying the image of I_0 in the maximal abelian quotient of G_M with $\widehat{\mathcal{O}_{\mathfrak{p}_0}^\times}$ by class field theory, $\phi \in \pi(\mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}})$ has values over $\widehat{\mathcal{O}_{\mathfrak{p}_0}^\times}$ in the upper nilpotent subalgebra $\mathfrak{n} \subset \mathfrak{sl}_2(\mathbb{F})$ and in $Ad(\overline{\rho}(g_{\mathfrak{p}}))(\mathfrak{n}) = g_{\mathfrak{p}} \mathfrak{n} g_{\mathfrak{p}}^{-1}$ over $\widehat{\mathcal{O}_{\mathfrak{p}}^\times}$.

Since the p-decomposition subgroup $\overline{D} \subset \overline{G}$ of a prime $\mathfrak{p}_0|p$ has order prime to p by (s3), the isomorphism class of a p-torsion-free $\mathbb{Z}_p[\overline{D}]$-module L of finite type is determined by the isomorphism class of $\mathbb{Q}_p[\overline{D}]$-modules $L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. By p-adic logarithm and the normal basis theorem in Galois theory, $\widehat{\mathcal{O}_{\mathfrak{p}_0}^\times} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathrm{Ind}_1^{\overline{D}} \mathbb{Q}_p = \mathbb{Q}_p[\overline{D}]$ as $\mathbb{Q}_p[\overline{D}]$-modules. Hence we conclude $\widehat{\mathcal{O}_{\mathfrak{p}_0}^\times} \cong \mu_p(M_{\mathfrak{p}_0}) \oplus \mathrm{Ind}_1^{\overline{D}} \mathbb{Z}_p$. Hence, up to p-torsion, the p-profinite completion $\widehat{\mathcal{O}_p^\times}$ is isomorphic to $\mathrm{Ind}_{\overline{D}}^{\overline{G}} \widehat{\mathcal{O}}_{\mathfrak{p}_0}^\times = \mathrm{Ind}_1^{\overline{G}} \mathbb{Z}_p = \mathbb{Z}_p[\overline{G}]$. If $\mu_p(M_{\mathfrak{p}_0}) = \{1\}$, as $\widehat{\mathcal{O}}_{\mathfrak{p}_0}^\times$ is sent onto the $\mathfrak{p}_0$ inertia subgroup of G_M^{ab} by class field theory, we get

$$\mathrm{Hom}_{\mathbb{Z}_p[\overline{G}]}(\widehat{\mathcal{O}_p^\times}, Ad(\overline{\rho})) \overset{(1)}{=} \mathrm{Hom}_{\mathbb{Z}_p[\overline{D}]}(\widehat{\mathcal{O}}_{\mathfrak{p}_0}^\times, Ad(\overline{\rho})) \overset{(2)}{=} \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p, Ad(\overline{\rho})) \cong Ad(\overline{\rho})$$

from Shapiro's lemma in which $\pi(\mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}})$ is sent by the identity (1) into $\mathrm{Hom}_{\mathbb{Z}_p[\overline{D}]}(\widehat{\mathcal{O}}_{\mathfrak{p}_0}^\times, \mathfrak{n})$ ($\mathfrak{n} = \mathbb{F}$ with $\overline{D}$ acting via $\overline{\epsilon}\overline{\delta}^{-1}$) and then by (2) into $\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p, \mathfrak{n}) \cong \mathfrak{n} = \mathbb{F}$ having dimension 1 over $\mathbb{F}$. Thus the theorem follows from our assumption: $\mathrm{Hom}_{\mathbb{Z}[\overline{G}]}(Cl_M, Ad(\overline{\rho})) = Cl_M \otimes_{\mathbb{Z}[\overline{G}]} Ad(\overline{\rho}) = 0$; so, $\dim_{\mathbb{F}} \mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}} = \dim_{\mathbb{F}} \pi(\mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}}) \leq 1$. This finishes the proof when $\mu_p(M_{\mathfrak{p}_0}) = \{1\}$.

Now assume that $\mu_p(M_{\mathfrak{p}_0})$ has order p. By our assumption, $Ad(\overline{\rho})|_{\overline{D}}$ does not contain $\overline{\omega}$ for $\overline{\omega} := \nu_p \mod (p)$. We have $\widehat{\mathcal{O}_p^\times} \cong \mathrm{Ind}_{\overline{D}}^{\overline{G}} \mu_p(\overline{\mathbb{Q}}) \oplus \mathrm{Ind}_1^{\overline{G}} \mathbb{Z}_p$, since $\widehat{\mathcal{O}_{\mathfrak{p}_0}^\times} \cong \mu_p(M_{\mathfrak{p}_0}) \oplus \mathrm{Ind}_1^{\overline{D}} \mathbb{Z}_p$. Since $Ad(\overline{\rho})|_{\overline{D}}$ does not contain $\overline{\omega}$, by Frobenius reciprocity, $\mathrm{Ind}_{\overline{D}}^{\overline{G}} \mu_p(M_{\mathfrak{p}_0}) \otimes_{\mathbb{Z}[\overline{G}]} Ad(\overline{\rho}) = 0$, and we find

$$\mathrm{Hom}_{\mathbb{Z}_p[\overline{G}]}(\widehat{\mathcal{O}_p^\times}, Ad(\overline{\rho})) \cong \mathrm{Hom}_{\mathbb{Z}_p[G]}(\mathrm{Ind}_1^{\overline{G}} \mathbb{Z}_p, Ad(\overline{\rho})).$$

Then by the same argument as above, we conclude $\dim_{\mathbb{F}} \mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}} = \dim_{\mathbb{F}} \pi(\mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}}) \leq 1$ as desired. □

Here is what happens if $Ad(\overline{\rho})|_{\mathrm{Gal}(M_{\mathfrak{p}_0}/\mathbb{Q}_p)}$ contains $\overline{\omega}$:

Corollary 2.3. *We assume that $M_{\mathfrak{p}_0} = \mathbb{Q}_p[\mu_p]$ and $Ad(\overline{\rho})|_{\mathrm{Gal}(M_{\mathfrak{p}_0}/\mathbb{Q}_p)}$ contains $\overline{\omega}$ in addition to $Cl_M \otimes_{\mathbb{Z}[G]} Ad(\overline{\rho}) = 0$. Then R can have two generators over Λ; in other words, $\dim_{\mathbb{F}} \mathrm{Sel}_{\mathbb{Q}}(Ad(\overline{\rho}))$ can be equal to 2.*

Proof. In this case, $\widehat{\mathcal{O}_p^\times} \cong \mathrm{Ind}_{\overline{D}}^{\overline{G}} \mu_p(\overline{\mathbb{Q}}_p) \oplus \mathrm{Ind}_1^{\overline{G}} \mathbb{Z}_p$. Since $Ad(\overline{\rho}) = \overline{\omega} \oplus 1 \oplus \overline{\omega}^{-1}$ by (s3),

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathrm{Ind}_{\overline{D}}^{\overline{G}} \mu_p(\overline{\mathbb{Q}}), Ad(\overline{\rho})) \cong \mathbb{F}.$$

Since $\overline{D}$ acts by $\overline{\omega}$ on the upper nilpotent elements in $\mathfrak{sl}(\mathbb{F})$, combined with the argument in the proof of Theorem 2.2 dealing with $\mathrm{Ind}_1^{\overline{G}} \mathbb{Z}_p \subset \widehat{\mathcal{O}_p^\times}$, we find that $\dim_{\mathbb{F}} \mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}} \leq 2$. As we will see below in Theorem 3.9, if $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$ as in the introduction, $\mathrm{Sel}(Ad(\overline{\rho})) = \mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}}$, and therefore R can have two generators. □

Remark 2.4. If $Ad(\overline{\rho})$ contains $\overline{\omega}$ (so, (H2) fails), $\overline{\rho}|_{D_p} \cong \xi \otimes \left(\begin{smallmatrix} \nu_p & * \\ 0 & 1 \end{smallmatrix}\right) \mod \mathfrak{m}_W$. By (s3) (and the solution of Serre's mod p modularity conjecture by Khare and Wintenberger), we have a weight 2 Hecke eigenform form f of level N associated to $\mathbb{T}$ giving rise to a W-algebra homomorphism $\lambda : \mathbb{T} \to \overline{\mathbb{Q}}_p$ with $f = \sum_{n=1}^{\infty} \lambda(T(n))q^n$. Since f cannot be a theta series of the real quadratic field F as its weight is 2, we find $\lambda \circ \sigma \neq \lambda$ giving rise to another Hecke eigenform f' belonging to $\mathbb{T}$ of weight 2. Then by level raising [R84, Propositions 3.3–4] (see also [HMI, Lemma 3.7 and Proposition 3.40] for level raising of the Hecke algebra), we should have one more Hecke eigenform g of weight 2 belonging to $\mathbb{T}$ such that g is congruent to f modulo $\mathfrak{m}_{W'}$ (possibly for an extension $W'_{/W}$) and g is multiplicative at p with conductor Np. Thus $\mathrm{rank}_\Lambda \mathbb{T} \geq 3$ and hence $\mathbb{T} \not\cong \Lambda[\sqrt{1 - \langle\varepsilon\rangle}]$ in this case.

As is well known, if $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$, $Ad(\overline{\rho}) \cong \overline{\chi} \oplus \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$ (see the proof of Lemma 3.2). For a general coefficient ring $A \in CNL_{/W}$, we write $\chi_A : G \to A^\times$ for the character $\left(\frac{F/\mathbb{Q}}{}\right)$ regarded as having values in A. If $A = \mathbb{F}$, we write $\overline{\chi}$ for $\chi_{\mathbb{F}}$. Any $A[G]$-module M, we define a discrete $A[G]$-module $M^* = M \otimes_A A^\vee$ with G-action through the factor M. Recall the definition of $\mathrm{Sel}(\chi_A)$ and $\mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \phi)$ for a (minimal) deformation $\phi : G \to A^\times$ of $\overline{\varphi}$ over G from [H20, §4]:

$$\begin{aligned} \mathrm{Sel}(\chi_A) &:= \mathrm{Ker}(H^1(G, \chi_A^*) \to H^1(I_p, \chi_A^*)) = \mathrm{Hom}(Cl_F, A^\vee) \\ \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \phi^-) &:= \mathrm{Ker}(H^1(G, (\mathrm{Ind}_F^{\mathbb{Q}} \phi^-)^*) \to H^1(D_{\mathfrak{p}^\varsigma}, (\phi_\varsigma^-)^*)). \end{aligned} \tag{2.2}$$

It is shown in [H20, §4] that $\mathrm{Sel}(Ad(\overline{\rho})) = \mathrm{Sel}(\overline{\chi}) \oplus \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-)$, and by the same argument, we have a canonical isomorphism $\mathrm{Sel}(Ad(\mathrm{Ind}_F^{\mathbb{Q}} \phi)) = \mathrm{Sel}(\chi_A) \oplus \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \phi^-)$ (see Theorem 3.9 for a more detailed statement of this fact). Though we had extra assumptions [H20, (h2–3)], these extra assumptions do not interfere with the computation there. Indeed the computation is easier in our case as $H^1(G, X)$ for any $\mathbb{F}[G]$-module X is unramified at $l \neq p$ since the inertia subgroup at l in G has order prime to p (so [H20, (h2–3)] does not matter). By the exact sequence in the proof of Theorem 2.2:

$$\mathrm{Hom}_{\mathbb{Z}[\overline{G}]}(Cl_M, Ad(\overline{\rho})) \hookrightarrow \mathrm{Sel}_M(Ad(\overline{\rho}))^{\overline{G}} \xrightarrow{\pi} \mathrm{Hom}_{\mathbb{Z}_p[\overline{G}]}(\widehat{\mathcal{O}_p^\times}, Ad(\overline{\rho}))$$

with $M = F(Ad(\overline{\rho})) = F(\overline{\varphi}^-)$, we have $\dim_{\mathbb{F}} \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) = \dim_{\mathbb{F}} \mathrm{Sel}_M(\mathrm{Ind}_F^{\mathbb{Q}} \varphi^-)^{\overline{G}} \leq 1$ under (H2) (as everywhere unramified Selmer cocycle with values in $\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$ comes from the subspace $\mathrm{Hom}(Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}[\mathrm{Gal}(F(\varphi^-)/F)]} \overline{\varphi}^-, Ad(\overline{\rho}))$ inside $\mathrm{Hom}_{\mathbb{Z}[\overline{G}]}(Cl_M, Ad(\overline{\rho}))$). We record this fact as

Lemma 2.5. *Suppose* $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$. *Then* $\mathrm{Sel}(Ad(\overline{\rho})) = \mathrm{Sel}(\overline{\chi}) \oplus \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-)$ *and* $\mathrm{Sel}(\overline{\chi}) = \mathrm{Hom}(Cl_F, \mathbb{F})$. *Under* (H0–2), *we have* $\dim_{\mathbb{F}} \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) \leq 1$.

The key point of Theorem 2.2 is that $\mathbb{T}$ is generated by a single element over Λ, and therefore this automatically implies the presentation $\mathbb{T} = \Lambda[[X]]/(S)$ as $\mathbb{T}$ is free of finite rank over Λ (for the characteristic polynomial $S = S(X)$ over Λ of $x \mapsto \Theta x$ acting on $\mathbb{T}$). Only under (s1–5) without assuming $CL_M \otimes_{\mathbb{Z}[G]} Ad(\overline{\rho}) = 0$, we have

$$\mathbb{T} \cong \Lambda[[X_1, \ldots, X_r]]/(S_1, \ldots, S_r) \text{ (i.e., local complete intersection over } \Lambda) \tag{2.3}$$

for $r = \dim_{\mathbb{F}} \mathrm{Sel}(Ad(\overline{\rho}))$, at least when $R = \mathbb{T}$ is known (see [TW95], [DFG04], [Th16] and [Ka16]).

3. Adjoint Selmer groups

Hereafter we assume $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$. We study the action of σ on the adjoint Selmer groups and, at the end of this section, the relation of the adjoint Selmer group with more classical Iwasawa modules. Also in the middle of this section, without assuming $R = \mathbb{T}$ (though it is known in this case by [Th16]), we shall give a short proof of the presentation (2.3) for a real quadratic field F (see Theorem 3.4).

Let $H := \mathrm{Gal}(F(\overline{\rho})^{(p)}/F) \triangleleft G$. In the theory of dualizing modules, there is a general notion of "different" for a finite flat extension A/B of rings (see Appendix C in this paper and [MR70, Appendix]). In our case where $A/B = \mathbb{T}/\mathbb{T}_+$, following the computation by Tate in [MR70], the different equals $I = \mathbb{T}(\sigma - 1)\mathbb{T}$ which is well defined without assuming the assumptions (H0–3) of Theorem 2.2, though it may not be principal without assuming (H2). For a while, we only assume (H0–1). Since σ acts trivially on $\mathbb{T}/I$, writing $\rho := (\rho_{\mathbb{T}} \bmod I)$, we find $\rho \cong \rho \otimes \chi$ for $\chi = \left(\frac{F/\mathbb{Q}}{}\right)$. Then by an integral version of Mackey's theorem [DHI98, Lemma 3.2], $\rho \cong \mathrm{Ind}_F^{\mathbb{Q}} \Psi$ for a character

$\Psi : H \to (\mathbb{T}/I)^\times$ unramified outside $\mathfrak{c}\mathfrak{p}$ deforming $\overline{\varphi}$. To make Ψ explicit, let C be the Galois group over F of the maximal p-abelian extension F_C of F inside $F(\overline{\rho})^{(p)}$ unramified outside $\mathfrak{p}\infty$. Thus C is a p-abelian finite group fitting into the exact sequence: $(O_{\mathfrak{p}}^\times/\overline{\varepsilon^{\mathbb{Z}}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow C \twoheadrightarrow C_F$ for the p-class group $C_F := Cl_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Here $\overline{\varepsilon^{\mathbb{Z}}}$ is the subgroup of $O_{\mathfrak{p}}^\times$ topologically generated by the fundamental unit ε. Note that $(O_{\mathfrak{p}}^\times/\overline{\varepsilon^{\mathbb{Z}}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p = \widehat{O_{\mathfrak{p}}^\times}/\varepsilon^{(p-1)\mathbb{Z}_p}$. Since $C_\Lambda := (O_{\mathfrak{p}}^\times/\overline{\varepsilon^{\mathbb{Z}}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is naturally a subgroup of C and $\Lambda_\varepsilon := \Lambda/(\langle\varepsilon\rangle - 1) \cong W[C_\Lambda]$ by sending $t \in \Lambda$ to the class of $(1+p) \in C_\Lambda$, we have a canonical inclusion $\Lambda_\varepsilon \hookrightarrow W[C]$. We identify Λ_ε with its image in $W[C]$. Define a character $\Phi : H \to W[C]^\times$ by $\Phi(\tau) = \varphi(\tau)\tau|_{F_C}$. By sending $h \in H$ to $[h,\varsigma] = h\varsigma h^{-1}\varsigma^{-1}$, we have an isomorphism $C = \mathrm{Gal}(F_C/F) \cong \mathrm{Gal}(F(\Phi^-)/F(\varphi^-))$.

Since $(W[C], \Phi)$ is a universal pair for the deformation functor of $\overline{\varphi}$ unramified outside $\mathfrak{p}\mathfrak{c}\infty$ (over H), we have a canonical surjective algebra homomorphism $W[C] \twoheadrightarrow \mathbb{T}/I$ inducing Ψ. Since $\mathrm{Ind}_F^{\mathbb{Q}} \Phi$ is a deformation of $\overline{\rho}$ over H, we find that Φ is a specialization of Ψ, and therefore this is an isomorphism (see [CV03, Corollary 2.3] and [H20, Corollary 2.3]).

Note that for this fact $\mathbb{T}/I \cong W[C]$, we do not need $R \cong \mathbb{T}$ as all deformations $\phi : H \to \overline{\mathbb{Q}}_p^\times$ unramified at $\mathfrak{p}^\varsigma$ of φ gives rise to a modular form of weight 1 (i.e., the theta series $\theta(\phi)$ of ϕ). By the existence of the fundamental unit, ϕ factors through the finite group $Cl_F(\mathfrak{p}^\infty\mathfrak{f}\infty)$. Then regarding ϕ an ideal character, $\theta(\phi) = \sum_{\mathfrak{a}} \phi(\mathfrak{a})q^{N(\mathfrak{a})}$ ($N(\mathfrak{a}) = N_{F/\mathbb{Q}}(\mathfrak{a})$) is a modular form of weight 1 (a result of Hecke; see [MFM, Theorem 4.8.3]).

We identify $\mathbb{T}/I$ with $W[C]$ and Φ with Ψ. Thus we have a short exact sequence $I \hookrightarrow \mathbb{T} \twoheadrightarrow \mathbb{T}/I$. Taking "+"-eigenspace of σ, we get another $I_+ \hookrightarrow \mathbb{T}_+ \twoheadrightarrow \mathbb{T}/I$; so, we obtain

Lemma 3.1. *Under* (H0–1)*, we have a canonical isomorphism* $\mathbb{T}_+/I_+ \cong \mathbb{T}/I \cong W[C]$ *as* Λ*-algebras. In particular,* σ *acts non-trivially on* $\mathbb{T}$ *and* $\mathbb{T} \neq \mathbb{T}_+$ *which implies* $\Omega_{\mathbb{T}/\mathbb{T}_+} \otimes_{\mathbb{T}} \mathbb{F} \neq 0$.

Proof. We need to prove the last assertion. Since $\mathbb{T}/I = W[C]$ is free of finite rank over W and $\mathbb{T}$ is free of finite rank over Λ, $I = \mathbb{T}(\sigma - 1)\mathbb{T} \neq 0$. Thus σ acts non-trivially on $\mathbb{T}$, and hence $\mathbb{T} \neq \mathbb{T}_+$. □

We like to normalize the image of the variable X in $\mathbb{T}$ under the presentation $\mathbb{T} = \Lambda[[X]]/(S)$ in Theorem 2.2. On $\mathbb{T}$ (resp. R), we have an involution σ with the property that $\sigma \circ \rho_{\mathbb{T}} \cong \rho_{\mathbb{T}} \otimes \chi$ (resp. $\sigma \circ \boldsymbol{\rho} \cong \boldsymbol{\rho} \otimes \chi$) for the quadratic character $\chi = \left(\frac{F/\mathbb{Q}}{}\right)$. Here writing $\rho_{\mathbb{T}} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we define $\sigma \circ \rho_{\mathbb{T}} := \left(\begin{smallmatrix} a^\sigma & b^\sigma \\ c^\sigma & d^\sigma \end{smallmatrix}\right)$ (and $\sigma \circ \boldsymbol{\rho}$ has the same meaning). We write R_+ for the subring fixed by σ. As long as $B \in CNL_W$ is a subalgebra of $\mathbb{T}_+$ or R_+, σ acts on $\Omega_{?/B}$ naturally for $? = R, \mathbb{T}$. In particular σ acts on $\Omega_{\mathbb{T}/\mathbb{T}_+}$ and on Ω_{R/R_+} by -1. Hence we choose the image Θ of X so that $\sigma(\Theta) = -\Theta$ and $\Omega_{\mathbb{T}/\mathbb{T}_+}$ is generated by $d\Theta$ over $\mathbb{T}$.

Take $\rho_A \in \mathcal{D}(A)$. Thus ρ_A is induced by $\pi : R \to A$. We suppose to have an involution σ_A acting on A such that $\sigma_A \circ \pi = \pi \circ \sigma$. Then σ acts on $\Omega_{R/\Lambda} \otimes_{R,\pi} A$ so that $\sigma(\omega \otimes a) = \sigma(\omega) \otimes \sigma_A(a)$ for $\omega \in \Omega_{R/\Lambda}$ and $a \in A$. As is well known (see Theorem A.1), $\Omega_{R/\Lambda} \otimes_{R,\pi} A \cong \mathrm{Sel}(Ad(\rho_A))^\vee$ canonically as A-modules, we have an action of σ on $\mathrm{Sel}(Ad(\rho_A))$ via this isomorphism.

We now make explicit how σ acts on Selmer cocycles. Regard χ as having values in $A^\times$ (we write χ_A if we need to indicate the coefficient ring A of χ), and define $\rho_A \cdot \chi : G \to \mathrm{GL}_2(A)$ for $\rho_A \in \mathcal{D}(A)$ by literally multiplying the matrix $\rho_A(g)$ by the scalar $\chi(g)$ (so, $\rho_A \cdot \chi \cong \rho_A \otimes \chi$). Let $j := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and writing $\rho_A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we put $\rho_A^{\sigma_A} = \sigma_A \circ \rho_A := \left(\begin{smallmatrix} a^{\sigma_A} & b^{\sigma_A} \\ c^{\sigma_A} & d^{\sigma_A} \end{smallmatrix}\right)$. We normalize ρ_A so that $j(\rho_A \cdot \chi)j^{-1} = \rho_A^{\sigma_A}$ (see the argument proving Lemma 7.3 how we normalize ρ_A in this way). For each 1-cocycle $u : G \to Ad(\rho_A)^*$, we define $u^{[\sigma]}(g) = ju(g)^{\sigma_A}j^{-1}$. From $u(gh) = Ad(\rho_A)(g)u(h) + u(g)$, we find

$$\begin{aligned} u^{[\sigma]}(gh) &= j\rho_A^{\sigma_A}(g)jju(h)^{\sigma_A}jj\rho_A(g^{-1})^{\sigma_A}j + ju(g)^{\sigma_A}j = Ad(j\rho_A^{\sigma_A}j)(g)u^{[\sigma]}(h) + u^{[\sigma]}(g) \\ &= Ad(\rho_A \cdot \chi)(g)u^{[\sigma]}(h) + u^{[\sigma]}(g) = Ad(\rho_A)(g)u^{[\sigma]}(h) + u^{[\sigma]}(g). \end{aligned}$$

Since the conjugation of j preserves the upper triangular p-decomposition subgroup and p-inertia subgroup of $\mathrm{Gal}(F(\boldsymbol{\rho})/\mathbb{Q})$, in this way, σ acts on $\mathrm{Sel}(Ad(\rho_A))$.

Pick a character $\phi : H \to A^\times$ deforming $\overline{\varphi}$ unramified outside $\mathfrak{p}^\varsigma$. Suppose $\rho_A = \mathrm{Ind}_F^{\mathbb{Q}} \phi \in \mathcal{D}(A)$. Consider the standard matrix form of the induced representation: $\rho_A(g) = \left(\begin{smallmatrix} \phi(g) & \phi(g\varsigma) \\ \phi(\varsigma^{-1}g) & \phi(\varsigma^{-1}g\varsigma) \end{smallmatrix}\right)$, extending ϕ well defined over H by 0 outside H. Then σ_A is trivial, and $[\sigma]$ is just a conjugate action of j. Indeed, we have $j(\rho_A \cdot \chi)j^{-1} = \rho_A$.

Lemma 3.2. *Let the notation be as above. Write* $\rho_A := \mathrm{Ind}_F^{\mathbb{Q}} \phi$. *Then under the decomposition* $\mathrm{Sel}(Ad(\rho_A)) = \mathrm{Sel}(\chi_A) \oplus \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \phi^-)$ *in* Lemma 2.5, *the involution* σ *acts on* $\mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \phi^-)$ (*resp.* $\mathrm{Sel}(\chi_A)$) *by* -1 (*resp.* $+1$).

Proof. Since σ acts trivially on A as ρ_A is an induced representation, we have $u^{[\sigma]} = juj^{-1}$ by definition. We have $Ad(\rho_A) \cong \chi_A \oplus \mathrm{Ind}_F^{\mathbb{Q}} \phi^-$ by the matrix form of $\mathrm{Ind}_F^{\mathbb{Q}} \phi$ as described above. In this decomposition, χ_A is realized on diagonal matrices $T := \{\mathrm{diag}[a, -a] \in Ad(\rho_A) = \mathfrak{sl}_2(A) | a \in A\}$ and $\mathrm{Ind}_F^{\mathbb{Q}} \phi^-$ is realized on the anti-diagonal matrices $A \subset \mathrm{Ad}(\overline{\rho})$. Since j acts by $+1$ on T and -1 on A, the action of σ on $\mathrm{Sel}(\chi_A)$ is by $+1$ and on $\mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \phi^-)$ is by -1. □

We now show the presentation (2.3) for $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$. Here is a ring theoretic lemma:

Lemma 3.3. *Let A be a complete local noetherian ring finite flat over Λ. Then A is a local complete intersection over Λ if and only if for a non-zero divisor $\delta \in \mathfrak{m}_A$, $A/(\delta)$ is a local complete intersection. Moreover if $A/(\delta)$ is a local complete intersection free of finite rank over W, we have* $\dim_{\mathbb{F}} t^*_{(A/(\delta))/W} \leq 1 + \dim_{\mathbb{F}} t^*_{A/\Lambda}$.

Proof. We first prove the "if"-part. Let $m = \dim_{\mathbb{F}} t^*_{A/\Lambda}$ for $t^*_{A/\Lambda} := \mathfrak{m}_A/(\mathfrak{m}_A^2 + \mathfrak{m}_\Lambda)$, and take a presentation $\Lambda[[x_1, \ldots, x_m]] \twoheadrightarrow A$ for the m-variable power series ring $\Lambda[[x_1, \ldots, x_m]]$ over Λ. Write the kernel of this map as $\mathfrak{a}$. Lifting δ to $\widetilde{\delta} \in \Lambda[[x_1, \ldots, x_m]]$ so that $\widetilde{\delta}$ has image δ in A, we have $\Lambda[[x_1, \ldots, x_m]]/(\mathfrak{a} + (\widetilde{\delta})) = A/(\delta)$. Write $\mu(\mathfrak{b})$ for the minimal number of generators of an ideal $\mathfrak{b}$ of a ring. Since $A/(\delta)$ is a local complete intersection of dimension 1, $\mathfrak{a} + (\widetilde{\delta})$ is generated by a regular sequence of length $m+1$ as $\mu(\mathfrak{a} + (\widetilde{\delta}))$ is equal to $m + 1 = \dim \Lambda[[x_1, \ldots, x_m]] - \dim A/(\delta)$ for the complete intersection ring $A/(\delta)$ (cf. Theorems 17.4 (i) and (iii) (3) and 21.2 of [CRT]). Since the height of $\mathfrak{a}+(\widetilde{\delta})$ is $m+1$ and the height of $\mathfrak{a}$ is m (by $\dim A = 1+\dim A/(\delta)$ as δ is a non-zero divisor; see [CRT, Theorem 17.4 (i)]), we conclude $\mu(\mathfrak{a} + (\widetilde{\delta})) = \mu(\mathfrak{a}) + 1 = m + 1$ from $\mu(\mathfrak{a}) \leq \mu(\mathfrak{a} + (\widetilde{\delta}))$. Then by [CRT, Theorem 17.4 (iii)], we conclude that a minimal set of generators $a_1, \ldots, a_m$ of $\mathfrak{a}$ is a regular sequence. Thus $A \cong \Lambda[[x_1, \ldots, x_m]]/(a_1, \ldots, a_m)$ is a local complete intersection by [CRT, Theorem 21.2 (ii)].

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

Suppose that $A/(\delta)$ is free of finite rank over W. Then we have $\dim_{\mathbb{F}} t^*_{A/\Lambda} = m$. On the other hand, we have $\dim_{\mathbb{F}} t^*_{(A/(\delta))/W} \leq m + 1$ as $A/(\delta) = W[[T, x_1, \ldots, x_m]]/(\mathfrak{a} + (\widetilde{\delta}))$. □

Here is a case where the presentation as in (2.3) is valid for $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$:

Theorem 3.4. *Suppose* $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$ *for a real quadratic field F. Under* (H0–2), *we have*

$$\mathbb{T} = \Lambda[[X_1^+, \ldots, X_{r_+}^+, X^-]]/(S_1, \ldots, S_{r_++1})$$

for $r_+ = \dim_{\mathbb{F}} \mathrm{Sel}(\overline{\chi}) = \dim_{\mathbb{F}_p} Cl_F \otimes_{\mathbb{Z}} \mathbb{F}_p$ *such that* $\sigma(\Theta_j^+) = \Theta_j^+$ *and* $\sigma(\Theta) = -\Theta$ *for the image* Θ (*resp.* Θ_j^+) *of* X^- (*resp.* X_j^+). *Moreover* Θ *is a non-zero divisor.*

Under (H0–1) and minimality, it is well known that $\mathbb{T}$ is generated over Λ by trace of $\rho_{\mathbb{T}}$; so, the natural map $R \to \mathbb{T}$ is surjective.

Proof. Note $\dim \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) \leq 1$ by Lemma 2.5. By Lemma 3.1, $\mathbb{T} \neq \mathbb{T}_+$, and hence $t^*_{\mathbb{T}/\mathbb{T}_+} \neq 0$. Since σ acts by -1 on $t^*_{\mathbb{T}/\mathbb{T}_+} := \mathfrak{m}_{\mathbb{T}}/(\mathfrak{m}_{\mathbb{T}}^2 + \mathfrak{m}_{\mathbb{T}_+}) \neq 0$ and $\mathrm{Sel}(Ad(\overline{\rho}))^\vee \cong t^*_{\mathbb{T}/\Lambda} = \mathfrak{m}_{\mathbb{T}}/(\mathfrak{m}_{\mathbb{T}}^2 + \mathfrak{m}_\Lambda)$ surjects down to $t^*_{\mathbb{T}/\mathbb{T}_+}$ (as $(\mathfrak{m}_{\mathbb{T}}^2 + \mathfrak{m}_{\mathbb{T}_+}) \supset (\mathfrak{m}_{\mathbb{T}}^2 + \mathfrak{m}_\Lambda)$), we must have $\dim \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) = 1$ as $\mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-)^\vee$ covers $t^*_{\mathbb{T}/\mathbb{T}_+}$, and hence $\dim_{\mathbb{F}} t^*_{\mathbb{T}/\mathbb{T}_+} = 1$. Therefore I is generated by at most a single element. Since σ is non-trivial on $\mathbb{T}$, I is a proper ideal of $\mathbb{T}$; so, I is generated by $\Theta \in \mathfrak{m}_{\mathbb{T}}$ with $\sigma(\Theta) = -\Theta$. Since $\mathbb{T}/I = \mathbb{T}/(\Theta) \cong W[C]$, Θ is a non-zero divisor. Indeed, since $\mathbb{T}$ is reduced by Lemma 2.1, if Θ were a zero divisor, its restriction to an irreducible component of $\mathrm{Spec}(\mathbb{T})$ vanishes and hence $\dim \mathbb{T}/(\Theta) \geq 2$, a contradiction. This fact that Θ is a non-zero divisor also follows from Lemma 3.3 as $W[C]$ is a local complete intersection finite flat over W. Since the group algebra $W[C]$ is a local complete intersection, by Lemma 3.3 applied to $(A, \delta) = (\mathbb{T}, \Theta)$, $\mathbb{T}$ is a local complete intersection flat over Λ generated by $r_+ + 1$ elements for the dimension r_+ of the "+"-eigenspace of σ of $t^*_{\mathbb{T}/\Lambda}$.

Note that $r_+ = \dim_{\mathbb{F}} \mathrm{Sel}(\overline{\chi})$ by Lemma 3.2, and we can choose the generators Θ_j^+ and Θ as in the theorem. □

We record the following fact we have proved in the above proof of Theorem 3.4:

Corollary 3.5. *Under* (H0–2)*, we have* $\dim_{\mathbb{F}} \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) = 1$*, and under* (H3)*,* $\mathrm{Sel}(\overline{\chi}) = 0$.

Proposition 3.6. *Assume* (H0–1)*. Then for* $r_- = \dim_{\mathbb{F}} \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-)$*,* $\mathbb{T}$ *is generated over* $\mathbb{T}_+$ *by* r_- *elements* $\Theta_1, \dots, \Theta_{r_-}$ *with* $\sigma(\Theta_j) = -\Theta_j$ *for all* j*.*

As mentioned in the introduction, we have $R \cong \mathbb{T}$ by [Th16] in our setting.

Proof. Note that $t^*_{\mathbb{T}/\Lambda} \cong \mathrm{Sel}(Ad(\overline{\rho}))^\vee = \mathrm{Sel}(\overline{\chi})^\vee \oplus \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-)^\vee$ compatible with the action of σ (see Theorem A.1). By Lemma 3.1, $\Omega_{\mathbb{T}/\mathbb{T}_+} \otimes_{\mathbb{T}} \mathbb{F} \neq 0$. Look into the first fundamental exact sequence:

$$\Omega_{\mathbb{T}_+/\Lambda} \otimes_{\mathbb{T}_+} \mathbb{F} \xrightarrow{i} \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} \mathbb{F} \to \Omega_{\mathbb{T}/\mathbb{T}_+} \otimes_{\mathbb{T}} \mathbb{F} \to 0.$$

Plainly the action of σ on $\Omega_{\mathbb{T}/\mathbb{T}_+} \otimes_{\mathbb{T}} \mathbb{F} \cong \mathfrak{m}_{\mathbb{T}}/(\mathfrak{m}_{\mathbb{T}}^2 + \mathfrak{m}_{\mathbb{T}_+})$ is equal to -1 and σ fixes point by point $\Omega_{\mathbb{T}_+/\Lambda} \otimes_{\mathbb{T}_+} \mathbb{F}$. Thus the "$-$" eigenspace $\mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-)$ of $\Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} \mathbb{F} = \mathrm{Sel}(Ad(\overline{\rho}))^\vee$ is isomorphic to $\Omega_{\mathbb{T}/\mathbb{T}_+} \otimes_{\mathbb{T}} \mathbb{F}$. This implies that $\mathbb{T}$ is generated over $\mathbb{T}_+$ by r_- elements Θ_j as in the proposition. □

When $\dim_{\mathbb{F}} \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) = r_-$, we choose the generators $\{\Theta_i\}_{i=1}^{r_-}$ of $\mathbb{T}$ over $\mathbb{T}_+$ so that $\sigma(\Theta_i) = -\Theta_i$, and write $\Theta = \Theta_1$ if $r_- = 1$.

Corollary 3.7. (1) *If the conditions* (H0–2) *are satisfied,* $I = \mathbb{T}(\sigma - 1)\mathbb{T}$ *is principal generated by* Θ *with* $\sigma(\Theta) = -\Theta$*,* $\mathbb{T}/(\Theta) \cong \mathbb{T}_+/(\Theta^2) \cong (\Theta)/(\Theta^2) \cong W[C]$ *as* $\mathbb{T}$*-modules, and* $\mathbb{T}$ *and* $\mathbb{T}_+$ *are local complete intersections free of finite rank over* Λ*.*

(2) *If further the conditions* (H0–3) *are satisfied, for* Θ *as above,*

$$\mathbb{T} = \Lambda[\Theta], \mathbb{T}_+ = \Lambda[\Theta^2] \quad \text{and} \quad \mathbb{T}/(\Theta) \cong \mathbb{T}_+/(\Theta^2) \cong \Lambda_\varepsilon.$$

Proof. By Theorem 3.4, $\mathbb{T}$ is a local complete intersection free of finite rank over Λ. Since $\mathbb{T}_+$ is a direct factor of $\mathbb{T}$ as Λ-modules, $\mathbb{T}_+$ is Λ-projective, and hence Λ-free of finite rank. Since $\mathbb{T}/(\Theta) = W[C]$ and $\mathbb{T}$ is reduced by Lemma 2.1, Θ is a non-zero divisor of $\mathbb{T}$ (as explained in the proof of Theorem 3.4). Thus $(\Theta)/(\Theta^2) \cong \mathbb{T}/(\Theta) \cong W[C]$, and $I_+ = (\Theta^2)$. By Lemma 3.1, $W[C] \cong \mathbb{T}_+/I_+ = \mathbb{T}_+/(\Theta^2)$. Since Θ^2 is a non-zero divisor and $W[C]$ is a local complete intersection over W, by Lemma 3.3, we conclude $\mathbb{T}_+$ is a local complete intersection. This proves (1)

Since $\mathbb{T} = \Lambda[\Theta]$ with $\sigma(\Theta) = -\Theta$ by Theorem 2.2 (combined with Proposition 3.6), we find $\mathbb{T}_+ = \Lambda[\Theta^2]$. By (H3), we find $W[C] = \Lambda_\varepsilon$ from $\mathbb{T} = \Lambda[\Theta]$, proving (2). □

Let K^-/F be the maximal p-abelian anticyclotomic sub-extension inside $F(\overline{\rho})^{(p)}$ of F, where the word "anti-cyclotomic" means ς acts on $\tau \in \mathrm{Gal}(K^-/F)$ by $\varsigma\tau\varsigma^{-1} = \tau^{-1}$. Note that K^-/F coincides with maximal anti-cyclotomic extension unramified outside p, as the inertia subgroups of G at primes in the level N has order prime to p. Recall [H20, Definition 4.3]:

Definition 3.8. Let $\phi : \mathrm{Gal}(F(\overline{\rho})/F) \to W^\times$ be one of the character φ^- and φ^-_ς. Let $\mathcal{Y}^-$ be the Galois group over $K^-F(\phi)$ of the maximal p-abelian extension $L = L_\phi$ of $K^-F(\phi) = F(\Phi^-)$ unramified outside $\mathfrak{p}$ and totally split at $\mathfrak{p}^\varsigma$. 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 $\mathcal{Y}(\phi) := \mathcal{Y}^- \otimes_{\mathbb{Z}_p[\mathrm{Gal}(F(\phi)/F)],\phi} W$. Interchanging the role of $\mathfrak{p}$ and $\mathfrak{p}^\varsigma$ in the above definition, we define $\mathcal{Y}_\varsigma(\phi)$ (which is the ς-conjugate of $\mathcal{Y}(\phi_\varsigma)$).

As assumed in the introduction above Theorem A, φ has order prime to p; so, $F(\phi) \cap K^- = F$ (as K^- is a p-abelian extension of F). This assures us that $\mathrm{Gal}(K^-F(\phi)/F) \cong \mathrm{Gal}(F(\phi)/F) \times \mathrm{Gal}(K^-/F)$ in the above definition.

Since $F(\varphi^-) \subset F(\overline{\rho})$ and only prime factors of p ramifies in $K^-F(\varphi^-)/F(\varphi^-)$, $L_{\varphi^-} \subset F(\overline{\rho})^{(p)}$.

Theorem 3.9. *Write* $\chi_{W[C]}$ *for the* $W[C]$*-free module of rank* 1 *on which* G *acts by* $\chi_{W[C]}$ *as before. Under* (H0–1)*, we have canonical isomorphisms*

$$\mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \Phi^-)) \cong (\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W)^\vee, \ \mathrm{Sel}(\chi_{W[C]}) \cong C_F^\vee \otimes_{\mathbb{Z}_p} W[C],$$
$$\mathrm{Sel}(Ad(\mathrm{Ind}_F^{\mathbb{Q}} \Phi)) \cong (C_F^\vee \otimes_{\mathbb{Z}_p} W[C]) \oplus (\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W)^\vee,$$

and $\mathcal{Y}(\varphi^-)\otimes_{\mathbb{Z}_p[\varphi^-]}W\cong W[C]$ *up to finite torsion. If further the conditions* (H2) *are satisfied, we have*

$$\mathcal{Y}(\varphi^-)\otimes_{\mathbb{Z}_p[\varphi^-]}W\cong \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}}\Phi^-)^\vee\cong \mathbb{T}/(\Theta)\cong W[C].$$

Proof. We have the decomposition $Ad(\mathrm{Ind}_F^{\mathbb{Q}}\Phi)\cong \chi_{W[C]}\oplus \mathrm{Ind}_F^{\mathbb{Q}}\Phi^-$ (over $W[C]$). This combined with the functoriality of the Greenberg's Selmer group, we have

$$\mathrm{Sel}(Ad(\mathrm{Ind}_F^{\mathbb{Q}}\Phi))\cong \mathrm{Sel}(\chi_{W[C]})\oplus(\mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}}\Phi^-)\otimes_{\mathbb{Z}_p[\varphi^-]}W).$$

General functoriality of the formation of Selmer groups with respect to induction is given in [HMI, Proposition 3.80] and this fact is verified just above [HMI, Theorem 5.33] for an imaginary quadratic field (actually for a CM quadratic extension), but the fact being imaginary is not used in the proof there (see [EMI, §7.4.2] for a down-to-earth exposition of this fact). Thus this splitting of the Selmer group is valid for any quadratic extensions of a totally real field. By (s4) valid in this induced case, Selmer cocycle is unramified outside p. Thus actually, we do not need to worry about local conditions outside p (although in the proof of [HMI, Proposition 3.80] local conditions including those at primes outside p are taken care of, as (s4) is not supposed in this proposition in [HMI]).

Since $\mathbb{Z}_p[\varphi^-]\subset\mathbb{Z}_p[\varphi]=W$, we need to extend scalars to W if necessary. By the same proof of [HMI, Theorem 5.33] (where the imaginary quadratic case is exposed), we get $\mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}}\Phi^-)=\mathcal{Y}(\varphi^-)^\vee$, $\mathrm{Sel}(\chi_{W[C]})=\mathrm{Sel}(\chi)\otimes_{\mathbb{Z}_p}W[C]$ and $\mathrm{Sel}(\chi)=\mathrm{Sel}(\chi_{\mathbb{Z}_p})=\mathrm{Hom}(Cl_F,\mathbb{Q}_p/\mathbb{Z}_p)=C_F^\vee$. In [HMI], a more common definition replacing G by the Galois group of the maximal extension of $\mathbb{Q}$ inside $\overline{\mathbb{Q}}$ unramified outside Np is used, but the argument to relate the adjoint Selmer group to $\mathcal{Y}(\varphi^-)$ is the same as the one in [HMI] since $L_{\varphi^-}\subset F(\overline{\rho})^{(p)}$ as remarked above. This shows the first isomorphism.

The fact $\mathcal{Y}(\varphi^-)\otimes_{\mathbb{Z}_p[\varphi^-]}W\cong W[C]$ up to finite torsion follows from [H20, Proposition 5.1]. To pin-down this fact, writing $\mathfrak{R}_\epsilon$ for the integer ring of $F(\epsilon\varphi^-)$ for a character $\epsilon: C\to\overline{\mathbb{Q}}_p^\times$, we first note that the $\mathrm{Gal}(F(\epsilon\varphi^-)/F)$-module $\mathfrak{R}_\epsilon^\times\otimes_{\mathbb{Z}}W$ modulo torsion does not contain $\epsilon\varphi^-$ as a factor. Strictly speaking, this fact is proven in [H20, Proposition 5.1] when $\epsilon=1$. However the triviality in the case of φ^- implies the general case by Nakayama's lemma applied to the augmentation ideal of $W[C]$ (or one can prove the general case in exactly the same way as the proof of [H20, Proposition 5.1] since the proof does not use the fact that φ^- has order prime to p). Then for the fixed prime factor $\mathfrak{p}|p$ on F, writing $\mathfrak{R}_{\epsilon,\mathfrak{p}}=\mathfrak{R}_\epsilon\otimes_O O_{\mathfrak{p}}$ for the $\mathfrak{p}$-adic completion, let $X:=\mathfrak{R}_{\epsilon,\mathfrak{p}}^\times/\overline{\mathfrak{R}}_\epsilon^\times\otimes_{\mathbb{Z}_p}W[\epsilon]$. Then we have an identity: $X\cong W[\epsilon]$ up to finite torsion. By class field theory, $\mathcal{Y}(\varphi^-)\otimes_{\mathbb{Z}_p[\varphi^-]}W$ contains the p-profinite part of X as a subgroup of finite index, we find that $\mathcal{Y}(\varphi^-)\otimes_{\mathbb{Z}_p[\varphi^-]}W\cong W[C]$ up to finite torsion.

We now prove the last identity. The control theorem Theorem A.1 applied to $A=\mathbb{T}/I=W[C]$ and $\rho_0=\mathrm{Ind}_F^{\mathbb{Q}}\Phi$ implies $\Omega_{\mathbb{T}/\Lambda}\otimes_{\mathbb{T}}\mathbb{T}/I=\mathrm{Sel}(Ad(\rho_{\mathbb{T}}))^\vee\otimes_{\mathbb{T}}\mathbb{T}/I\cong\mathrm{Sel}(Ad(\mathrm{Ind}_F^{\mathbb{Q}}\Phi))^\vee$. By Lemma 3.2, σ acts by -1 on $\mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}}\Phi^-)\subset\mathrm{Sel}(Ad(\mathrm{Ind}_F^{\mathbb{Q}}\Phi))$, and therefore, taking the "$-$"-eigenspace, we have $(\Omega_{\mathbb{T}/\Lambda}\otimes_{\mathbb{T}}\mathbb{T}/I)^{\sigma=-1}\cong\mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}}\Phi^-)^\vee$, and the "$-$"-eigenspace $(\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}}\mathbb{T}/I)^{\sigma=-1}$ vanishes. By the first fundamental sequence [CRT, Theorem 25.1] tensored with $\mathbb{T}/I=W[C]$ over $\mathbb{T}$ produces the following exact sequence compatible with the action of σ:

$$\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T}/I\to\Omega_{\mathbb{T}/\Lambda}\otimes_{\mathbb{T}}\mathbb{T}/I\to\Omega_{\mathbb{T}/\mathbb{T}_+}\otimes_{\mathbb{T}}\mathbb{T}/I\to 0.$$

Plainly σ acts on $\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T}/I$ trivially as σ fixes $\mathbb{T}/I$ and $\mathbb{T}_+$, and hence $(\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T}/I)^{\sigma=-1}=0$. Then, taking the "$-$"-eigenspace of σ, we get $(\Omega_{\mathbb{T}/\Lambda}\otimes_{\mathbb{T}}\mathbb{T}/I)^{\sigma=-1}\cong\Omega_{\mathbb{T}/\mathbb{T}_+}\otimes_{\mathbb{T}}\mathbb{T}/I$. By Theorem 3.4, we find $\mathbb{T}=\mathbb{T}_+[X]/(f(X))$ for $f(X)=X^2-\Theta^2$ by $X\mapsto\Theta$. Thus $\mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}}\Phi^-)^\vee\cong\Omega_{\mathbb{T}/\mathbb{T}_+}\otimes_{\mathbb{T}}\mathbb{T}/I\cong\mathbb{T}/(f'(\Theta))=\mathbb{T}/I=W[C]$ by $a\cdot d\Theta\leftrightarrow a\in\mathbb{T}/I$ as desired. □

4. Proof of Theorem A.

Here is a detailed version of Theorem A:

Theorem 4.1. *Assume* (H0–3). *Write* $A=\mathbb{T}$ *or* $\mathbb{T}_+$. *Let* $e=\mathrm{rank}_\Lambda\mathbb{T}$. *Then the following four assertions hold:*

(1) *If* $\langle\varepsilon\rangle-1$ *is a prime in* Λ, *then the ring* A *is isomorphic to a power series ring* $W[[x]]$ *of one variable over* W*; hence,* A *is a regular local domain and is factorial;*
(2) *The ring* A *is an integral domain, and for a prime factor* P *of* $\langle\varepsilon\rangle-1$, *the localization* A_P *of* A *at* P *is a discrete valuation ring fully ramified over* Λ_P*;*

(3) *If p is prime to $a = \mathrm{rank}_\Lambda A$, the ramification locus of A/Λ is given by* $\mathrm{Spec}(\Lambda/(\langle\varepsilon\rangle - 1))$, *the different for $A_{/\Lambda}$ is principal and generated by Θ^{a-1} and A is a normal integral domain of dimension 2 unramified outside $(\langle\varepsilon\rangle - 1)$ over Λ;*

(4) *If $p|e$, $A_{\mathbb{Q}} := A \otimes_{\mathbb{Z}} \mathbb{Q}$ is a Dedekind domain unramified outside $(\langle\varepsilon\rangle - 1)$ over $\Lambda_{\mathbb{Q}} := \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$, and the relative different for $A_{\mathbb{Q}}$ over $\Lambda_{\mathbb{Q}}$ is principal and generated by Θ^{a-1};*

(5) *If $e = 2$, $\mathbb{T}$ is a normal integral domain; $\mathbb{T}_+ = \Lambda$ and $\mathbb{T} = \Lambda[\sqrt{1 - \langle\varepsilon\rangle}]$.*

After proving this theorem, we explore what we can prove under assumptions milder than (H0–3). There is an imaginary quadratic version of this structure theorem in [EMI, §8.5.4].

If $\langle\varepsilon\rangle - 1$ is not a prime ($\Leftrightarrow \varepsilon^{p-1} \equiv 1 \mod \mathfrak{p}^2$), by the existence of ambiguous classes, $\mathbb{T}$ cannot be factorial even if $e = 2$. Perhaps there is no example known of a prime $p \geq 5$ split in $F = \mathbb{Q}[\sqrt{5}]$ such that $\langle\varepsilon\rangle - 1$ is not a prime in $\mathbb{Z}_p[[T]]$. More generally we consider $F = \mathbb{Q}[\sqrt{d}]$ with square-free $0 < d \in \mathbb{Z}$ and describe how to decide if $\mathfrak{p}^2 | \varepsilon^{k-1} - 1$. Since $p > 2$, $\mathfrak{p}^2|(\varepsilon^{p-1} - 1) \Leftrightarrow \mathfrak{p}^2|(\varepsilon^{2(p-1)} - 1)$. On the other hand, $\varepsilon^{2(p-1)} - 1 = \varepsilon^{2(p-1)} - \varepsilon^{p-1}\varepsilon^{\varsigma(p-1)} = \varepsilon^{p-1}(\varepsilon^{p-1} - \varepsilon^{\varsigma(p-1)})$. Define $\alpha \in \mathbb{Z}$ so that $\varepsilon^2 - \alpha\varepsilon \pm 1 = 0$. Consider the corresponding Fibonacci type recurrence relation $f_n = \alpha f_{n-1} \mp f_{n-2}$. Then, for the solution f_n with initial values $f_0 = 0$ and $f_1 = 1$, we have $f_n = \frac{\varepsilon^n - \varepsilon^{n\varsigma}}{\varepsilon - \varepsilon^\varsigma}$. Thus we have $\frac{\varepsilon^{p-1} - \varepsilon^{\varsigma(p-1)}}{\sqrt{d}} = f_{p-1}C$ for $C = \frac{\varepsilon - \varepsilon^\varsigma}{\sqrt{d}}$. If $d = 5$, we have $C = 1$. In any case we conclude:

$$\langle\varepsilon\rangle - 1 \text{ is not a prime in } \Lambda \Leftrightarrow p^2 | f_{p-1}C. \tag{4.1}$$

For $\mathbb{Q}[\sqrt{5}]$ (i.e., $d = 5$), such primes are called Wall-Sun-Sun primes (named after Donald Dines Wall, Zhi Hong Sun and Zhi Wei Sun; see [SS92]) and are defined to be primes with $p^2 | f_{p-1}$ when p splits in $\mathbb{Q}[\sqrt{5}]$. There are no Wall-Sun-Sun primes less than 9.7×10^{14} and this bound is extended to 2.6×10^{17} by the PrimeGrid project. These primes are conjectured to exist infinitely many [Kl07] but are not found yet. For $d \neq 5$, $p = 191, 643$ are examples of a split prime with $p^2 | f_{p-1}$ for $\mathbb{Q}[\sqrt{10}]$ (this fact was pointed out to me by B. Palvannan). There seem many such primes for $\mathbb{Q}[\sqrt{10}]$. If $\varepsilon^{p-1} \equiv 1 \mod \mathfrak{p}^2$, the modulo p version of the Leopoldt conjecture discussed in [BGKK18] fails and the ordinary deformation ring $\mathbb{T}$ is not regular (i.e., the ordinary deformation problem is obstructed but not much (see [BGKK18, §2–3]).

Proof. Since the proof is the same for $\mathbb{T}$ and $\mathbb{T}_+$, we prove the assertions for $A = \mathbb{T}$. By (H2–3) and Corollary 3.5, $\dim_{\mathbb{F}} \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) = 1$ and $\mathrm{Sel}(\overline{\chi}) = 0$. Recall $\mathbb{T} = \Lambda[\Theta]$ by Theorem 3.4 with Θ such that $\sigma(\Theta) = -\Theta$ (or by Theorem 2.2 combined with the remark above Theorem A) and that Θ is the image of X in the presentation $\mathbb{T} = \Lambda[[X]]/(S)$ in Theorem 2.2. Put $\mathcal{J} = (\Theta) = \Theta\mathbb{T}$. For all $0 \neq u \in \mathbb{T}$, $[u] : x \mapsto ux$ induces the linear endomorphism $\mathrm{gr}(u)$ of the corresponding graded algebra $\mathrm{gr}_{\mathcal{J}}(\mathbb{T}) := \bigoplus_{n=0}^\infty \mathcal{J}^n/\mathcal{J}^{n+1}$ (with $\mathcal{J}^0 = \mathbb{T}$). The filtration $\{\mathcal{J}^n\}_{n=0,1,\dots}$ of $\mathbb{T}$ is exhaustive and separated. Then $[u]$ is injective if $\mathrm{gr}(u)$ is injective [BCM, III.2.8, Corollary 1]. By Corollary 3.7, we have $\mathrm{gr}_{\mathcal{J}}(\mathbb{T}) \cong \Lambda_\varepsilon[x]$ for the polynomial ring $\Lambda_\varepsilon[x]$, where the variable x corresponds to the image $\overline{\Theta}$ of the generator Θ of $\mathcal{J}$ in the first graded piece $\mathcal{J}/\mathcal{J}^2$. Take n so that $u \in \mathcal{J}^n$ but $u \notin \mathcal{J}^{n+1}$. Then $\mathrm{gr}(u) : \mathrm{gr}_{\mathcal{J}}(\mathbb{T}) \to \mathrm{gr}_{\mathcal{J}}(\mathbb{T})$ is multiplication by a polynomial of degree n.

Assume first that $\langle\varepsilon\rangle - 1$ is a prime; so, $(\langle\varepsilon\rangle - 1) = (T)$ in Λ and $\Lambda_\varepsilon = W$. Then $\mathrm{gr}_{\mathcal{J}}(\mathbb{T})$ is an integral domain isomorphic to the polynomial ring $W[x]$ ($x = \overline{\Theta}$); so, if $u \neq 0$, $\mathrm{gr}(u)$ is injective, and hence, $[u]$ is injective; so, u is not a zero divisor. We conclude that $\mathbb{T}$ is an integral domain. The projection $\mathbb{T} \twoheadrightarrow \mathbb{T}/\mathcal{J} = W$ has a section as $\mathbb{T}$ is a W-algebra. Thus we conclude $\mathbb{T} = \varprojlim_n \mathbb{T}/\mathcal{J}^n \cong W[[x]]$ by sending Θ to x. As is well known (e.g., [CRT, Theorems 19.5 and 20.8]), a power series ring over a discrete valuation ring is a unique factorization domain and is regular; so, we get the assertion (1).

Now we treat the general case where $\langle\varepsilon\rangle - 1$ can have several prime divisors. Pick a prime divisor P of $\langle\varepsilon\rangle - 1$. Consider the localization $\mathbb{T}_P = \mathbb{T} \otimes_\Lambda \Lambda_P$ and $\mathcal{J}_P = \mathcal{J}\mathbb{T}_P$. Then $\mathcal{J}_P^n/\mathcal{J}_P^{n+1} \cong \Lambda_\varepsilon \otimes_\Lambda \Lambda_P = P^n\mathbb{T}_P/P^{n+1}\mathbb{T}_P \cong \kappa(P)$ for $\kappa(P) = \Lambda_P/P\Lambda_P$. Therefore $\mathcal{J}\mathbb{T}_P = P\mathbb{T}_P = \Theta\mathbb{T}_P$ by Nakayama's lemma. Thus $\mathrm{gr}_{\mathcal{J}\mathbb{T}_P}(\mathbb{T}_P)$ is isomorphic to the polynomial ring $\kappa(P)[x]$ with $x = \overline{\Theta}$ over the residue field $\kappa(P) = \Lambda_P/P\Lambda_P$. Therefore, by [CRT, Theorem 28.3], the P-adic completion $\widehat{\mathbb{T}}_P$ of $\mathbb{T}_P$ is isomorphic to the power series ring $\kappa(P)[[x]]$ by sending Θ to x, and hence $\mathbb{T}_P$ is a discrete valuation ring with a prime element Θ. Since P is an associate minimal prime of $\mathbb{T}/\mathcal{J} = W[C] = \Lambda_\varepsilon$ and $\mathbb{T}/\mathcal{J}$ is fixed point by point by σ, σ acts on $\mathbb{T}_P$ so that it acts on $\kappa(P)[x] = \mathrm{gr}_{\mathcal{J}\mathbb{T}_P}(\mathbb{T}_P)$ fixing $\kappa(P)$ and $\sigma(x) = -x$. Thus $\mathbb{T}_P \neq \mathbb{T}_{+,P} \supset \Lambda_P$ and $e > 0$. Since $\mathbb{T}_P/P\mathbb{T}_P = \kappa(P)$, $\mathbb{T}_P$ is fully ramified over

Λ_P. Since $\mathbb{T}$ is free of finite rank e over Λ, $\mathbb{T}_P$ is free of finite rank e over Λ_P, and $\mathbb{T}$ injects into $\mathbb{T}_P$. In particular $\mathbb{T}$ is an integral domain. This proves the assertion (2).

We claim that $S = S(X) = \langle\varepsilon\rangle - 1 + X^2 f(X^2)$ for $f(X^2) \in \Lambda[[X^2]]$. Indeed by Corollary 3.7, we have $\Lambda/(\langle\varepsilon\rangle - 1) \cong \mathbb{T}/(\Theta) = \Lambda[[X]]/(X, S) = \Lambda/(S(0))$. Thus the constant term of S generates the ideal $(\langle\varepsilon\rangle - 1)$; so, replacing S by a Λ-unit multiple, we may assume $S(0) = \langle\varepsilon\rangle - 1$.

Suppose that $S \in \mathfrak{m}_\Lambda[[X]]$. Then $\mathbb{T} = \Lambda[[X]]/(S)$ surjects down to $\Lambda[[X]]/\mathfrak{m}_\Lambda[[X]] \cong \mathbb{F}[[X]]$, which is not a Λ-module of finite type. Since $\mathbb{T} = \Lambda[[X]]/(S)$ is Λ-free of rank e, $\overline{S} \neq 0$ for $\overline{S} := (S \bmod \mathfrak{m}_\Lambda[[X]])$. The reduced power series $\overline{S} \in \mathbb{F}[[X]]$ has reduced order $m > 0$ (i.e., $S = \sum_{n=0}^{\infty} a_n X^n$ with $a_0, \dots, a_{m-1} \in \mathfrak{m}_\Lambda$ but $a_m \notin \mathfrak{m}_\Lambda$). By a local ring version of Weierstrass' preparation theorem (e.g., [BCM, VII.3.8, Proposition 6]), we get a unique factorization $S(X) = U(X)D(X)$ for a monic distinguished polynomial $D(X)$ of degree m with respect to $\mathfrak{m}_\Lambda$ and a unit $U(X) \in \Lambda[[X]]^\times$. Thus we see $e := \mathrm{rank}_\Lambda \mathbb{T} = \mathrm{rank}_\Lambda \Lambda[X]/(D(X)) = m$. Then evaluating at $X = 0$, we get $\langle\varepsilon\rangle - 1 = S(0) = U(0)D(0)$. Since $U(0) \in \Lambda^\times$, $\mathbb{T} \cong \Lambda[X]/(D(X))$, and $D(X)$ is the characteristic polynomial of the Λ-linear map $\mathbb{T} \ni x \mapsto \Theta x \in \mathbb{T}$.

For a prime divisor $P|(\langle\varepsilon\rangle - 1)$, let $\widehat{\Lambda}_P := \varprojlim_n \Lambda_P/P^n\Lambda_P$, which is a discrete valuation ring. Then by Weierstrass preparation theorem for $\widehat{\Lambda}_P$, we have $S(X) = D_P(X)U_P(X)$ for a unit power series $U_P(X) \in \widehat{\Lambda}_P[[X]]^\times$ and a monic distinguished polynomial $D_P(X)$ with respect to P. Thus $\mathbb{T}_P = \mathbb{T} \otimes_\Lambda \widehat{\Lambda}_P$ is isomorphic to $\Lambda_P[X]/(D_P(X))$, and hence $D_P(X)$ is the characteristic polynomial of the $\widehat{\Lambda}_P$-linear map $\widehat{\mathbb{T}}_P \ni x \mapsto \Theta x \in \widehat{\mathbb{T}}_P$. Therefore $D_P(X) = D(X)$.

Note that $(D_P(0)) = (D(0)) = (\langle\varepsilon\rangle - 1)$ and hence $D_P(0)$ is square-free in $\widehat{\Lambda}_P$. Thus $D_P(X)$ is an Eisenstein polynomial in $\widehat{\Lambda}_P[X]$ [BCM, VIII.5.4]. Since $\widehat{\Lambda}_P$ is a discrete valuation ring, by [BCM, VIII.4.3], $D_P(X)$ is irreducible in $\mathrm{Frac}(\widehat{\Lambda})[X]$, and $\widehat{\Lambda}_P[X]/(D_P(X))$ is a discrete valuation ring fully ramified over $\widehat{\Lambda}_P$, reproving (2).

By (2), $\mathbb{T}/\Lambda$ is fully ramified at each prime factor of $\langle\varepsilon\rangle - 1$ with ramification index $e = \mathrm{rank}_\Lambda \mathbb{T}$. Then $\mathbb{T} = \Lambda[X]/(D(X))$ is a local domain by [BCM, VIII.5.4]. The polynomial $D(X) = X^e + a_{e-1}X^{e-1} + \cdots + a_0$ satisfies $(\langle\varepsilon\rangle - 1)|a_i$ and $(a_0) = (\langle\varepsilon\rangle - 1)$. Write $u = \frac{\langle\varepsilon\rangle - 1}{\Theta^e} \in \mathbb{T}^\times$ and $a_j = (\langle\varepsilon\rangle - 1)^{\alpha_j} u_j$ for $\alpha_j \geq 1$ and $\alpha_0 = 1$ $(0 \leq j < e)$ such that $u_j \in \Lambda$ is either 0 or $(\langle\varepsilon\rangle - 1) \nmid u_j$ for $j = 1, \dots, e-1$ and $u_0 \in \Lambda^\times$. Then

$$0 = D(\Theta) = \Theta^e + a_{e-1}\Theta^{e-1} + \cdots + a_0 = (\langle\varepsilon\rangle - 1)(u^{-1} + u_0 + \sum_{j=1}^{e-1} (\langle\varepsilon\rangle - 1)^{\alpha_j - 1} u_j \Theta^j).$$

Since $\langle\varepsilon\rangle - 1$ is not a zero-divisor of $\mathbb{T}$, we find $u^{-1} = -u_0 - \sum_{j=1}^{e-1} (\langle\varepsilon\rangle - 1)^{\alpha_j - 1} u_j \Theta^j \in \mathbb{T}$, and hence $u \in \mathbb{T}^\times$. Therefore

$$\frac{dD(X)}{dX}(\Theta) = e\Theta^{e-1} + a_{e-1}(e-1)\Theta^{e-2} + \cdots + a_1 = \Theta^{e-1}(e + \sum_{j=1}^{e-1} u^{\alpha_j} u_j j \Theta^{\alpha_j e - e + j}).$$

If $p \nmid e$, $(e + \sum_{j=1}^{e-1} u^{\alpha_j} u_j j \Theta^{\alpha_j e - e + j})$ is a unit; so, $(\frac{dD(X)}{dX}(\Theta)) = (\Theta^{e-1})$, and the ramification of $\mathbb{T}/\Lambda$ is limited to prime factors of (Θ^{e-1}). Since $(\Theta^{e-1}) \cap \Lambda = (\langle\varepsilon\rangle - 1)$, the ramification locus of $\mathbb{T}_{/\Lambda}$ is $\mathrm{Spec}(\Lambda/(\langle\varepsilon\rangle - 1))$ if $p \nmid e$. Therefore if $p \nmid e$, $\mathbb{T}_P$ is a discrete valuation ring for all height 1 prime $P|\langle\varepsilon\rangle - 1$. Since $\mathbb{T}$ is Λ-free, we have $\mathbb{T} = \bigcap_P \mathbb{T}_P$ which is a normal local domain (proving (3)).

Suppose $p|e$. Write $e = p^r e'$ with $p \nmid e'$. Since

$$0 = D(\Theta) = \Theta^e + a_{e-1}\Theta^{e-1} + \cdots + a_0 = \Theta^e(1 + u_0 u + \sum_{j=1}^{e-1} u^{\alpha_j} u_j \Theta^{\alpha_j e - e + j}),$$

we have $-uu_0 \equiv 1 \mod \Theta$; so, $v = (-uu_0)^{1/e'} \in \mathbb{T}$. Then $\mathbb{T}[v^{1/p^r}]/\mathbb{T}$ can ramify only at p as v is a unit. By replacing Θ by $\Theta' = v^{1/p^r}\Theta$, we find $\Theta'^e = -a_0$, and $\mathbb{T}[v^{1/p^r}] = \Lambda[v^{1/p^r}, \Theta']$, which can ramify over Λ only at p and prime factors of $\langle\varepsilon\rangle - 1$ (as $(\langle\varepsilon\rangle - 1) = (a_0)$). In particular $\mathbb{T}[\frac{1}{p}] = \bigcap_P \mathbb{T}_P$ for P running all prime divisors outside p, and $\mathbb{T}_P$ with $P \nmid (p)$ is a discrete valuation ring. This shows (4).

If $e = 2$, $\sigma(\Theta) = -\Theta$ implies $\Theta^2 \in \Lambda$. Thus $D(X) = X^2 - \Theta^2$ with $\Theta^2 = -a_0 = u_0(1 - \langle\varepsilon\rangle) \in \Lambda$ with $u = -u_0 \in \Lambda^\times$. Thus $u_0^2 = -uu_0 \equiv 1 \mod (\Theta)$. Since $(\Theta) \cap \Lambda = (\langle\varepsilon\rangle - 1)$ and $u_0, uu_0 \in \Lambda$, we find $u_0^2 = -uu_0 \equiv 1 \mod (\langle\varepsilon\rangle - 1)$, and $\sqrt{u_0} \in \Lambda^\times$. Thus replacing Θ by $\sqrt{u_0}\Theta$, we get $\Theta = \sqrt{1-\langle\varepsilon\rangle}$ and $\mathbb{T} = \Lambda[\sqrt{1-\langle\varepsilon\rangle}]$, proving (5). □

A proof similar to the one for Theorem 4.1 produces

Proposition 4.2. *Suppose* (H0–2). *Let* $\mathbb{T}'$ *(resp.* $\mathbb{T}'_+$*) be the* Λ*-subalgebra of* $\mathbb{T}$ *generated by* Θ *(resp.* Θ^2*) for* $\Theta \in \mathbb{T}$ *as in* Corollary 3.7 (1). *Denote by* A' *one of the rings* $\mathbb{T}'$ *or* $\mathbb{T}'_+$.

(1) *The ring* A' *is free of finite rank over* Λ *with presentation* $A' = \Lambda[X']/(D'(X))$ *with a distinguished polynomial* $D'(X') \in \Lambda[X']$ *with respect to* $(\Lambda, \mathfrak{m}_\Lambda)$ *such that* $D'(0) = \langle\varepsilon\rangle - 1$ *up to units in* Λ*;*
(2) *If* $\langle\varepsilon\rangle - 1$ *is a prime in* Λ*, then the ring* A' *is isomorphic to a power series ring* $W[[x]]$ *of one variable over* W*; hence,* A' *is a regular local domain and is factorial;*
(3) *The ring* A' *is an integral domain, and for a prime factor* P *of* $\langle\varepsilon\rangle - 1$*, the localization* A'_P *of* A' *at* P *is a discrete valuation ring fully ramified over* Λ_P*;*
(4) *If* p *is prime to* $e' = \mathrm{rank}_\Lambda A'$*, the ramification locus of* A'/Λ *is given by* $\mathrm{Spec}(\Lambda/(\langle\varepsilon\rangle - 1))$*, the relative different for* A'/Λ *is principal and generated by* $\Theta^{e'-1}$ *and* A' *is a normal integral domain of dimension* 2 *unramified outside* $(\langle\varepsilon\rangle - 1)$ *over* Λ*;*
(5) *If* $\mathrm{rank}_\Lambda \mathbb{T}' = 2$*,* $\mathbb{T}'$ *is a normal integral domain;* $\mathbb{T}'_+ = \Lambda$ *and* $\mathbb{T}' = \Lambda[\sqrt{1-\langle\varepsilon\rangle}]$.

In Section 10, we prove that a generator θ of the unipotent part of the p-inertia subgroup of $\mathrm{Gal}(F(\rho_\mathbb{T})/\mathbb{Q})$ coincides with Θ under (H0–2), and without assuming (H2), we prove in Corollary 10.4 that $\Lambda[\theta]$ in place of $\mathbb{T}'$ satisfies the assertions of the above proposition.

Proof. The proof of (2)–(5) is basically the same as the one given for Theorem 4.1 once we prove the assertion (1). We prove (1) for $A' = \mathbb{T}'$ and give a sketch for the rest. Since $\mathbb{T}'$ is Λ-torsion free Λ-module of finite type (as $\mathbb{T}$ is such), $V = \mathbb{T}' \otimes_\Lambda \mathrm{Frac}(\Lambda)$ is finite dimensional over $\mathrm{Frac}(\Lambda)$; so, we have the characteristic polynomial $D'(X') \in \mathrm{Frac}(\Lambda)[X']$ of degree e' of the multiplication by Θ on V. Since $x \mapsto \Theta x$ preserves $\mathbb{T}'$, $D'(X') \in \Lambda[X']$. Thus $\mathbb{T}' = \Lambda[X']/(D'(X'))$ hence $\mathbb{T}'$ is free of rank e' over Λ. Since $\Theta \in \mathfrak{m}_{\mathbb{T}'}$, $D'(X)$ is a distinguished polynomial of degree e' with respect to $(\Lambda, \mathfrak{m}_\Lambda)$.

We now show that we can choose Θ whose characteristic polynomial $D'(X)$ satisfies $(D'(0)) = (\langle\varepsilon\rangle - 1)$ as ideals. Let $\mathbb{T}'_+ = \mathbb{T}_+ \cap \mathbb{T}'$. Since $\mathbb{T}' = \mathbb{T}'_+[\Theta] \cong \mathbb{T}'_+[X]/(f(X))$ for $f(X) := X^2 - \Theta^2$, we have $\mathbb{T}'(\sigma - 1)\mathbb{T}' = f'(\Theta)\mathbb{T}' = \Theta\mathbb{T}'$ for $f'(X) = \frac{df(X)}{dX}$. By Theorem 3.4, we have $\mathbb{T}_+ = \Lambda[\Theta_1^+, \dots, \Theta_{r_+}^+, \Theta^2]$ and a cartesian diagram

$$\begin{array}{ccc} \mathbb{T} = \mathbb{T}_+ \otimes_{\mathbb{T}'_+} \mathbb{T}' & \longleftarrow & \mathbb{T}' \\ \uparrow & & \uparrow \\ \mathbb{T}_+ & \longleftarrow & \mathbb{T}'_+. \end{array}$$

Thus for the different $\mathfrak{d}_{A/R} = (\delta_{A/R})$ of Tate in [MR70, (A.1)] for a local complete intersection A/R, we have $\mathfrak{d}_{\mathbb{T}/\mathbb{T}_+} = \mathbb{T}(\sigma - 1)\mathbb{T} = I$, $\mathfrak{d}_{\mathbb{T}'/\mathbb{T}'_+} = \mathbb{T}'(\sigma - 1)\mathbb{T}'$ and $\mathfrak{d}_{\mathbb{T}/\mathbb{T}_+} \cap \mathbb{T}' = \mathfrak{d}_{\mathbb{T}'/\mathbb{T}'_+} = \Theta\mathbb{T}'$ (see Appendix C for more about the different). Thus $\Theta\mathbb{T}' \cap \Lambda = I \cap \mathbb{T}' \cap \Lambda = I \cap \Lambda = (\langle\varepsilon\rangle - 1)$. This shows

$$\mathbb{T}'/(\Theta') = (\Lambda + \Theta\mathbb{T}')/\Theta\mathbb{T}' \cong \Lambda/\Theta\mathbb{T}' \cap \Lambda = \Lambda_\varepsilon.$$

This produces an isomorphism of Λ-algebras:

$$\Lambda/(D'(0)) = \Lambda[X']/(X', D'(X')) = \mathbb{T}'/(\Theta') \cong \Lambda/(\langle\varepsilon\rangle - 1).$$

Writing $\mathrm{Ann}_\Lambda(M)$ for the annihilator of a Λ-module M, we find the identity of ideals

$$(D'(0)) = \mathrm{Ann}_\Lambda(\Lambda/(D'(0)) = \mathrm{Ann}_\Lambda(\Lambda/(\langle\varepsilon\rangle - 1)) = (\langle\varepsilon\rangle - 1).$$

Thus the setting is identical to the proof of Theorem 4.1. Then for the rest, we argue in the same way as in the proof of Theorem 4.1 replacing $(\Lambda[[X]], S, \mathbb{T}, e)$ by $(\Lambda[[X']], D', \mathbb{T}', e')$. □

For a subalgebra A of $\mathbb{T}$ and a prime $P \in \mathrm{Spec}(\mathbb{T})$, we take the localization A_P at $P \cap A$ and its completion $\widehat{A}_P = \varprojlim_n A_P/(P \cap A)^n A_P$. Here is a localized version of the above proposition:

Proposition 4.3. *Suppose* (H0–1). *Write* P *for a prime divisor of* $I = \mathbb{T}(\sigma - 1)\mathbb{T}$ *such that the projection* $\mathbb{T}/I = W[C] \to \mathbb{T}/P$ *induces the a character* ϕ *of* C*; so,* $P \cap \Lambda = (t - \phi(\gamma))$ $(\gamma = 1 + p)$. *Then we have a surjective* Λ*-algebra homomorphism* $\lambda = \lambda_\phi : \mathbb{T} \twoheadrightarrow \mathbb{I}$ *for an integral domain* $\mathbb{I} = \mathbb{I}_\phi$

torsion-free over Λ *giving an irreducible component* $\mathrm{Spec}(\mathbb{I})$ *of* $\mathrm{Spec}(\mathbb{T})$ *stable under* σ*, and any other irreducible components of* $\mathrm{Spec}(\mathbb{T})$ *do not intersect with* $\mathrm{Spec}(\mathbb{I})$ *at* P*. The component* $\mathbb{I}$ *satisfies*

(1) *The ring* $\mathbb{I}_P$ *is free of finite rank over* Λ_P *with presentation* $\widehat{\mathbb{I}}_P = \widehat{\Lambda}_P[[X]]/(D_\phi)$ *for an Eisenstein polynomial* $D_\phi(X) \in \widehat{\Lambda}_P[X]$ *with respect to* $(\Lambda_P, P\Lambda_P)$ *such that* $D_\phi(0) = \phi(\gamma) - t$*;*
(2) *The ring* $\widehat{\mathbb{I}}_P$ *is isomorphic to a power series ring* $\kappa[[x]]$ *of one variable over* $\kappa := \mathbb{T}_P/P\mathbb{T}_P$*;*
(3) *The localization* $\mathbb{I}_P$ *is a discrete valuation ring fully ramified over* Λ_P*;*
(4) *If* $\mathrm{rank}_{\widehat{\Lambda}_P} \widehat{\mathbb{I}}_P = 2$*,* $\widehat{\mathbb{I}}_P = \widehat{\Lambda}_P[\sqrt{\phi(\gamma) - t}]$ *with* $\sigma(\sqrt{\phi(\gamma) - t}) = -\sqrt{\phi(\gamma) - t}$*.*

Proof. Since $P\mathbb{T}_P/(P\mathbb{T}_P^2 + (T)) = \Omega_{\mathbb{T}_P/\Lambda_P} \otimes_{\mathbb{T}_P} \kappa = \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} \kappa$ and $\Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} \kappa = \kappa$ by Theorem 3.9, the ideal $P\mathbb{T}_P$ is a principal ideal generated by Θ_ϕ with $\sigma(\Theta_\phi) = -\Theta_\phi$.

Write $e_\phi := \mathrm{rank}_{\Lambda_P} \mathbb{T}_P$. Then the characteristic polynomial of the multiplication by Θ_ϕ is a distinguished polynomial $D_\phi(X)$ and $\mathbb{T}_P = \Lambda_P[X]$ and $\widehat{\mathbb{T}}_P = \widehat{\Lambda}_P[[X]]/(D_\phi(X))$. Since $P \cap \Lambda = (\phi(\gamma) - t)$, we get $(D_\phi(0)) = (\phi(\gamma) - t)$ as before. Since $D_\phi(0)$ is square-free, we conclude that D_ϕ is an Eisenstein polynomial; so, $\widehat{\mathbb{T}}_P$ is an integral domain, and hence $\mathbb{T}_P$ is an integral domain. Define $\mathbb{I}$ to be the image of $\mathbb{T}$ in $\mathbb{T}_P$. Then $\mathbb{I}_P = \mathbb{T}_P$, $\mathbb{I}_P$ is free of finite rank over Λ_P, and $\mathrm{Spec}(\mathbb{I})$ does not have intersection with any other irreducible components of $\mathrm{Spec}(\mathbb{T})$. Replacing $(\Lambda[[X]], S, \mathbb{T}, e, \Theta)$ by $(\widehat{\Lambda}_P[[X]], D_\phi, \widehat{\mathbb{T}}_P, e_\phi, \Theta_\phi)$ in the proof of Theorem 4.1, we conclude (1–4); in particular, if $e_\phi = 2$, $\widehat{\mathbb{T}}_P = \widehat{\Lambda}_P[\sqrt{\phi(\gamma) - t}]$. □

5. Universal pseudo character rings

Since we need to compare the rings universal among pseudo representations of different kind, we summarize their relations here. In this section, when we are dealing with deformation of the residual pseudo representation associated to $\overline{\varphi} \oplus \overline{\varphi}_\varsigma$, we always assume (H0–1); so, in particular, $\overline{\varphi} \neq \overline{\varphi}_\varsigma$.

5.1. **Pseudo representation of Wiles.** We note $G = \mathrm{Gal}(F(\overline{\rho})^{(p)}/F(\overline{\rho})) \rtimes \mathrm{Gal}(F(\overline{\rho})/\mathbb{Q})$ and $H = \mathrm{Gal}(F(\overline{\rho})^{(p)}/F(\overline{\rho})) \rtimes \mathrm{Gal}(F(\overline{\rho})/F)$ as $p > 2$ and $p \nmid [F(\overline{\rho}) : \mathbb{Q}]$. We fix such a decomposition; so, $\mathrm{Gal}(F(\overline{\rho})/\mathbb{Q}) \cong \Delta_G$ and $\mathrm{Gal}(F(\overline{\rho})/F) \cong \Delta$ for subgroups $\Delta \subset H$ and $\Delta \subset \Delta_G \subset G$. For the center Δ_+ of Δ_G, Δ_G/Δ_+ is a dihedral group. We identify the element ς with an element in Δ_G having order 2 in $D := \Delta_G/\Delta_+$ (inducing a non-trivial automorphism of F).

We have a commutative diagram with exact rows defining a subgroup $\Delta_+ \subset \Delta_G \cong \mathrm{Gal}(F(\overline{\rho})/\mathbb{Q})$

$$\begin{array}{ccccc} \Delta_+ & \xrightarrow{\hookrightarrow} & \Delta_G & \xrightarrow{\twoheadrightarrow} & D \\ \cap\big\downarrow & & \cap\big\downarrow \overline{\rho} & & \cap\big\downarrow \\ Z & \xrightarrow{\hookrightarrow} & \mathrm{GL}_2(\mathbb{F}) & \xrightarrow{\twoheadrightarrow} & \mathrm{PGL}_2(\mathbb{F}) \end{array}$$

for the center Z of $\mathrm{GL}_2(\mathbb{F})$. Then D is a dihedral group with maximal cyclic subgroup Δ_-, which fits into the following exact sequence

$$1 \to \Delta_+ \to \Delta \to \Delta_- \to 1.$$

Let $I_{\mathfrak{p}}$ (resp. $I_{\mathfrak{p}^\varsigma}$) be an inertia subgroup of $\mathfrak{p}$ (resp. $\mathfrak{p}^\varsigma$) in H and $D_{\mathfrak{p}} \triangleright I_{\mathfrak{p}}$ and $D_{\mathfrak{p}^\varsigma} \triangleright I_{\mathfrak{p}^\varsigma}$ be the decomposition subgroups. We may assume that $\Delta_{\mathfrak{p}} := \Delta \cap D_{\mathfrak{p}}$ is non-trivial and has element δ with non-trivial image in Δ_- by (H0). Let c be complex conjugation in H. Since the conductor of φ has one archimedean place ∞ in it, we have $\varphi(c) = -1$. Identifying $\mathrm{Gal}(F(\overline{\rho})/\mathbb{Q})$ with the subgroup Δ_G, we may assume

(D1) $\varsigma \in \Delta_G$ is represented by the anti-diagonal element $\begin{pmatrix} 0 & \varphi(\varsigma^2) \\ 1 & 0 \end{pmatrix}$,
(D2) c is represented by $\mathrm{diag}[-1, 1] \in \mathrm{GL}_2(W)$ and $\delta \in \Delta_{\mathfrak{p}}$ is represented by $\mathrm{diag}[\varphi(\delta), \varphi_\varsigma(\delta)]$ under $\rho_{\mathbb{T}}$, where $\mathrm{diag}[a, b] = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$,
(D3) $D_{\mathfrak{p}^\varsigma} = \varsigma^{-1} D_{\mathfrak{p}} \varsigma$.

By (D3), $\Delta_{\mathfrak{p}^\varsigma} := D_{\mathfrak{p}^\varsigma} \cap \Delta = \varsigma \Delta_{\mathfrak{p}} \varsigma^{-1}$. Since ς acts trivially by conjugation on Δ_+ and by "inverse" on Δ_-, we find $\Delta_{\mathfrak{p}} = \Delta_{\mathfrak{p}^\varsigma}$. We now take the Frobenius element $[p, F_{\mathfrak{p}}] = [p, \mathbb{Q}_p]$ and put $\phi := \lim_n [p, F_{\mathfrak{p}}]^{q^n}$ for $q = |\mathbb{F}|$. Thus c, ϕ and all elements in $I_{\mathfrak{p}} \cap \Delta = I_{\mathfrak{p}^\varsigma} \cap \Delta$ are diagonal and commute each other. We fix an element $\phi_0 \in \Delta_{\mathfrak{p}}$ with non-trivial $\varphi^-(\phi_0)$ (such ϕ_0 exists by (H0)). If $\mathfrak{p}$ is unramified, we may assume $\phi_0 = \phi$.

In the proof of Theorem C, Wiles' pseudo representation under normalization with respect to ϕ_0 is useful. Since ϕ_0 is diagonal with $\varphi^-(\phi_0) \neq 1$, by (D2), this normalization has the same effect as Wiles' normalization with respect to c. We define the pseudo representation with values in a profinite commutative ring A as a triple of continuous functions $\pi = \pi_A = (a, d : H \to A, x : H \times H \to A)$ satisfying the following three conditions:

(W1) $a(rs) = a(r)a(s) + x(r,s)$, $d(rs) = d(r)d(s) + x(s,r)$ and

$$x(rs,tu) = a(r)a(u)x(s,t) + a(u)d(s)x(r,t) + a(r)d(t)x(s,u) + d(s)d(t)x(r,u);$$

(W2) $a(1) = d(1) = 1$ and $x(r,s) = x(s,t) = 0$ if $s = 1, \phi_0$;

(W3) $x(r,s)x(t,u) = x(r,u)x(t,s)$.

We define $\mathrm{Tr}(\pi) := a + d$ and $\det(\pi)(r) := a(r)d(r) - x(r,r)$. As we mentioned, the normalization with respect to ϕ_0 and c is equivalent. Thus we freely refer to the formulas of Wiles' (normalized with respect to c). For example, we see easily $a(h) = \frac{1}{2}(\mathrm{Tr}(\pi(h)) - \mathrm{Tr}(\pi(hc)))$ and $d(h) = \frac{1}{2}(\mathrm{Tr}(\pi(h)) + \mathrm{Tr}(\pi(hc)))$ for all $h \in H$. Since $x(h,g) = a(hg) - a(h)a(g) = d(gh) - d(h)d(g)$, x is determined by a (or d) on H and hence by $\mathrm{Tr}(\pi)$.

Fix an ordered pair $(\mathfrak{p}, \mathfrak{p}^\varsigma)$ of p-adic places, and write τ_{ps} for the Wiles' pseudo representation $(\overline{a}, \overline{d}, \overline{x}) : H \to \mathbb{F}$ given by $\overline{a} = \overline{\varphi}$, $\overline{d} = \overline{\varphi}_\varsigma$ and $\overline{x} = 0$. Our $\mathfrak{p}$-ordinarity condition is $x(\sigma,\tau) = 0$ as long as $\tau \in D_\mathfrak{p}$ and $d|_{D_\mathfrak{p}}$ is unramified. The $\mathfrak{p}^\varsigma$-ordinarity condition is $x(\sigma,\tau) = 0$ as long as $\sigma \in \widetilde{\varsigma}^{-1} D_\mathfrak{p} \widetilde{\varsigma}$ and $\tau \in H$ and $a|_{\widetilde{\varsigma}^{-1} D_\mathfrak{p} \widetilde{\varsigma}}$ is unramified. We call "ordinary" the two conditions combined.

Consider the deformation functor $\mathcal{D}^{ps}_F : CNL_{/W} \to SETS$ sending $A \in CNL_{/W}$ to the set $\mathcal{D}^{ps}_F(A)$ of Wiles' pseudo representation $\pi = (a,d,x) : H \to A$ with $(\pi \bmod \mathfrak{m}_A) = \tau_{ps}$ satisfying the following two conditions:

(i) π is ordinary;

(ii) $\mathrm{Tr}(\pi)(g^{-1}hg) = \mathrm{Tr}(\pi)(h)$ for each $g \in G$ and $h \in H$.

If π satisfies the invariance condition (ii), $\mathfrak{p}$-ordinarity implies $\mathfrak{p}^\varsigma$-ordinarity. Discarding the condition (ii), we consider another deformation functor $\mathcal{D}^{ps,ord}_F$ imposing just ordinarity (i). The functors similar to $\mathcal{D}^{ps}_F$ and $\mathcal{D}^{ps,ord}_F$ appear in [CV03] and [Be17, §3.2], and the following result is easy (e.g., [Be17, Proposition 3.5] or [MFG, §2.3.2]):

Lemma 5.1. *There exist universal pairs $(R^{ps}, \boldsymbol{\pi}^{ps})$ and $(R^{ps,ord}, \boldsymbol{\pi}^{ps,ord})$ with $R^{ps}, R^{ps,ord}$ in the category $CNL_{/W}$ and $\boldsymbol{\pi}^{ps} \in \mathcal{D}^{ps}_F(R^{ps})$ and $\boldsymbol{\pi}^{ps,ord} \in \mathcal{D}^{ps,ord}_F(R^{ps})$ representing the functor $\mathcal{D}^{ps}_F$ and $\mathcal{D}^{ps,ord}_F$, respectively.*

Lemma 5.2. *We have*

(1) $\det(\pi)(rs) = \det(\pi)(r)\det(\pi)(s)$ (*i.e.* $\det(\pi)$ *is a homomorphism from* H *into* $A^\times$),

(2) $2\det(\pi)(r) = \mathrm{Tr}(\pi)(r)^2 - \mathrm{Tr}(\pi)(r^2)$ *for all* $r \in W[H]$,

(3) $\mathrm{Tr}(\pi)(rs) = \mathrm{Tr}(\pi)(sr)$ *for all* $r, s \in W[H]$,

(4) *Writing* $T(r) := \mathrm{Tr}(\pi)$, *we have*

$$T(r)T(s)T(t) + T(rst) + T(tsr) - T(rs)T(t) - T(st)T(r) - T(rt)T(s) = 0.$$

Proof. We see by (W1) specialized to $(t,u) = (r,s)$

$$\det(\pi)(rs) - \det(\pi)(r)\det(\pi)(s) = -x(r,r)x(s,s) + x(r,s)x(s,r) \overset{\text{(W3)}}{=} 0.$$

Since $\det(\pi)(1) = 1$ by (W2), we conclude that $\det(\pi)$ is a homomorphism. We have

$$\mathrm{Tr}(\pi)(r)^2 - \mathrm{Tr}(\pi)(r^2) = (a(r)+d(r))^2 - a(r^2) - d(r^2) \overset{\text{(W1)}}{=} 2a(r)d(r) - 2x(r,r) = \det(\pi)(r)$$

proving (2). The assertion (3) plainly follows from (W1) as $\mathrm{Tr}(\pi) = a + d$ is symmetric with respect to (r,s). The assertion (4) can be proved via a long but direct computation. Here they are:

(a1) $T(r)T(s)T(t) = a(r)a(s)a(t) + a(r)a(t)d(s) + d(r)a(s)a(t) + d(r)d(s)a(t) + a(r)a(s)d(t) + a(r)d(s)d(t) + a(s)d(r)d(t) + d(r)d(s)d(t)$,

(a2) $T(rst) \overset{\text{(W1)}}{=} a(r)a(s)a(t) + x(r,s)a(t) + d(r)d(s)d(t) + x(s,r)d(t) + x(rs,t) + x(t,rs)$,

(a3) $T(tsr) = T(rts) = a(r)a(t)a(s) + x(r,t)a(s) + d(r)d(t)d(s) + x(t,r)d(s) + x(rt,s) + x(s,rt)$,

(b1) $T(rs)T(t) = a(r)a(s)a(t) + a(t)x(r,s) + d(r)d(s)a(t) + x(s,r)a(t) + a(r)a(s)d(t) + x(r,s)d(1) + d(r)d(s)d(t) + x(s,r)d(t)$ (by (W1)),

(b2) $T(st)T(r) =$ the equation obtained by replacing $(r,s,t) \mapsto (s,t,r)$ in (b1), (b3) $T(rt)T(s) =$ the equation obtained by replacing $(r,s,t) \mapsto (r,t,s)$ in (b1).

Let $A = (a1) + (a2) + (a3)$ and $B = (b1) + (b2) + (b3)$. Then cancelling all monomials of $a(r), a(s), a(t), d(r), d(s), d(t)$ and all possible terms of the form $*(\cdot)x(\cdot,\cdot)$ with $* = a, d$, we get $A - B = A' - B'$ for $A' = x(rs,t) + x(t,rs) + x(rt,s) + x(s,rt)$ and $B' = a(t)x(s,r) + d(t)x(r,s) + a(r)x(s,t) + a(r)x(t,s) + d(r)x(s,t) + d(r)x(t,s) + a(s)x(t,r) + d(s)x(r,t)$. Then we conclude $A' = B'$ from the last relation of (W1). □

5.2. **Pseudo character, determinant and Cayley–Hamilton representation.** Let

$$W[[H]] := \varprojlim_{h \triangleleft H, h:open} W[H/h]$$

for h running over normal open subgroups. A pseudo character $T : W[[H]] \to A$ for a p-profinite commutative ring A with identity is a continuous map satisfying (e.g., [MFG, §2.2.2])

(T1) $T(1) = 2$;
(T2) $T(rs) = T(sr)$ for all $r, s \in W[[H]]$;
(T3) $T(r)T(s)T(t) + T(rst) + T(tsr) - T(rs)T(t) - T(st)T(r) - T(rt)T(s) = 0$.

This was first considered by R. Taylor and is more conceptual than Wiles' pseudo representation. The conditions (T1–3) are modeled with obvious properties satisfied by the trace of a 2-dimensional representation. However we need to add one more requirement that $\det(T)(\sigma) = \frac{1}{2}(T(\sigma)^2 - T(\sigma^2))$ is multiplicative to reconstruct a Cayley–Hamilton representation (to be defined) with trace given by the pseudo character. In this sense, pseudo character is a notion slightly weaker than Wiles' pseudo representation (see Lemma 5.2). We call a pseudo character T *Cayley–Hamilton* if $\det(T)$ is multiplicative (i.e., a group homomorphism from H into $A^\times$). Therefore, we introduce the notion of (functorial) determinant following Chenevier. We recall the definition given in [Ch14, §1.5]:

Definition 5.3. *Let R be an A-algebra and d be a positive integer. A d-dimensional A-valued determinant on R is a multiplicative A-polynomial law $D : R \to A$ which is homogeneous of degree d. When $R = A[\mathcal{G}]$ for some group $\mathcal{G}$, we say also that D is a determinant on $\mathcal{G}$.*

We assume in this paper $d = 2$ and $\mathcal{G} = H$. Then $D(gU + hV) = D(g)U^2 + f(g,h)UV + D(h)V^2$ for indeterminates U, V and $g, h \in H$. Then define $T(h) = f(h, 1)$. As seen in [Ch14, Lemma 1.9], T is a pseudo character and D determines T. We write for a 2-dimensional representation ρ of H, $T_\rho = \mathrm{Tr}(\rho)$ and $D_\rho = \det(\rho)$ as the determinant in the above sense. If A is a ring in which 2 is invertible, $T(h)$ recovers $D(h) = (T(h)^2 - T(h^2))/2$ as a function; so, having D is equivalent to having pseudo character with its determinant required to be multiplicative [Ch14, Proposition 1.29].

5.3. **Cayley–Hamilton representation.** We introduce representations with values in a generalized matrix algebra (GMA) as in [FGS], [Ch14] and [WE15]. We refer to [WWE18, §5.9] for the notion of ordinarity over $\mathbb{Q}$ for GMA representations (not treated in [FGS] and [Ch14]). Since we have two conjugacy classes of p-decomposition groups $D_\mathfrak{p}$ and $D_{\mathfrak{p}^\varsigma}$, we modify the definition (see below) of ordinarity depending on each factor $\mathfrak{p}$ and $\mathfrak{p}^\varsigma$. We follow [FGS, §1.3] to define a GMA A-algebra E. Let A be a commutative ring and E an A-algebra. We say that E is a generalized matrix algebra (GMA) of type $(d_1, \ldots, d_r)$ if R is equipped with:

- a family orthogonal idempotents $\mathcal{E} = \{e_1, \ldots, e_r\}$ with $\sum_i e_i = 1$,
- for each i, an A-algebra isomorphism $\psi_i : e_iEe_i \xrightarrow{\sim} M_{d_i}(A)$, such that the trace map $T : R \to A$, defined by $T(x) := \sum_i \mathrm{Tr}(\psi_i(e_ixe_i))$ satisfies $T(xy) = T(yx)$ for all $x, y \in E$. We call $\mathcal{E} = \{e_i, \psi_i, i = 1, \ldots, r\}$ the data of idempotents of E.

In this paper, we assume that $r = 2$ and $d_1 = d_2 = 1$; so, we can forget about ψ_i as an A-algebra automorphism of A is unique. Once we have $\mathcal{E}$, we identify $e_iEe_i = A$ and put $B = e_1Ee_2$ and $C = e_2Ee_1$. Then a generalized matrix algebra over A is a pair of an associative A-algebra E and $\mathcal{E}$. It is isomorphic to $A \oplus B \oplus C \oplus A$ as A-modules; so, we write instead $(E, \mathcal{E}) = \left(\begin{smallmatrix} A & B \\ C & A \end{smallmatrix}\right)$ which we call a GMA structure. There are A-linear maps $\psi : B \otimes_A C \to A$ and $\psi' : C \otimes_A B \to A$ (called the product law of E) such that the multiplication in E is given by 2-by-2 matrix product (and of course they need to satisfy rules to assure associativity; see [FGS, §1.3]). For $b \in B$ and $c \in C$, we often write simply $bc := \psi(b \otimes c)$ and $cb := \psi'(c \otimes b)$ if confusion is unlikely. We call A the scalar subring of $(E, \mathcal{E})$ and $(E, \mathcal{E})$ is called an A-GMA. The A-GMA's form a category over the category of A-algebras. Here, writing $E = \left(\begin{smallmatrix} A & B \\ C & A \end{smallmatrix}\right)$ and $E' = \left(\begin{smallmatrix} A' & B' \\ C' & A' \end{smallmatrix}\right)$, we say that $\phi_E : E \to E'$ is an A-GMA morphism over an algebra homomorphism $\phi_A : A \to A'$ if

(1) ϕ_E is an algebra homomorphism,
(2) ϕ_E sends each matrix entry of E to the corresponding entry of E',
(3) on the entries A, ϕ coincides with ϕ_A,
(4) on $\phi_E|_B : B \to B'$ and $\phi_E|_C : C \to C'$ are morphisms of A-modules.

A Cayley–Hamilton representation of $\mathcal{G}$ with coefficients in A is an A-algebra homomorphism $\rho : A[\mathcal{G}] \to E$, such that $(E, \mathcal{E})$ is an A-GMA, and such that in matrix coordinates, ρ is given by $\sigma \mapsto \left(\begin{smallmatrix} \rho^{\mathcal{E}}_{11}(\sigma) & \rho^{\mathcal{E}}_{12}(\sigma) \\ \rho^{\mathcal{E}}_{21}(\sigma) & \rho^{\mathcal{E}}_{22}(\sigma) \end{smallmatrix}\right)$. By abusing the language, we often say that $\rho : \mathcal{G} \to E^\times$ is a Cayley-Hamiltion representation if its A-linear extension is a Cayley-Hamiltion representation of the group algebra $A[\mathcal{G}]$. For a given ρ, if we change the set $\mathcal{E}$ of idempotents, the matrix expression changes; so, we added the superscript $\mathcal{E}$ to the matrix entries $\rho^{\mathcal{E}}_{ij}$ to indicate its dependence on $\mathcal{E}$. If the input of $\mathcal{E}$ is clear from the context, we omit the superscript $\mathcal{E}$. Given such a ρ, there is an induced A-valued pseudo character, denoted $T_\rho : \mathcal{G} \to A$, given by $T_\rho = \rho_{11} + \rho_{22}$ and $\det(\rho) = \rho_{11}\rho_{22} - \rho_{12}\rho_{21}$, cf. [WE15, Prop. 2.2.3]. It is called Cayley–Hamilton as ρ satisfies the equation $X^2 - T_\rho X + \det(\rho) = 0$ in the algebra E.

Taking $\mathcal{G}$ to be G or H, $\pi = (a, d, x)$ with $a = \rho_{11}$, $d = \rho_{22}$ and $x(g, h) = \rho_{12}(g)\rho_{21}(h)$ gives Wiles' pseudo-representation (normalized with respect to ϕ_0) as long as $\rho \otimes 1(\phi_0) \in E \otimes_A \mathbb{F}$ is diagonal non-scalar. We say that ρ has residual representation $\left(\begin{smallmatrix} \overline{\varphi} & 0 \\ 0 & \overline{\varphi}_\varsigma \end{smallmatrix}\right)$ (with this order $\overline{\varphi}$ at the top) if $(\rho_{11}(\sigma) \bmod \mathfrak{m}_A) = \overline{\varphi}(\sigma)$, $(\rho_{22}(\sigma) \bmod \mathfrak{m}_A) = \overline{\varphi}_\varsigma(\sigma)$, and $\rho_{12}(\sigma)\rho_{21}(\sigma) \equiv 0 \mod \mathfrak{m}_A$.

In H, we have two conjugacy classes of the p-decomposition groups depending on prime factors of p in K. Fix a decomposition subgroup $D_\mathfrak{p} \subset H$ for $\mathfrak{p}$ and put $D_{\mathfrak{p}^\varsigma} = \widetilde{\varsigma}^{-1} D_\mathfrak{p} \widetilde{\varsigma}$ for $\mathfrak{p}^\varsigma$. We define $\mathfrak{p}$-ordinarity (resp. $\mathfrak{p}^\varsigma$-ordinarity) of ρ to have $\mathcal{E}$ (resp. $\mathcal{E}^\varsigma$) such that $\rho^{\mathcal{E}}_{12}(\sigma) = 0$ for all $\sigma \in D_\mathfrak{p}$ and $\rho^{\mathcal{E}}_{22}(I_\mathfrak{p}) = 1$ (resp. $\rho^{\mathcal{E}^\varsigma}_{21}(\sigma) = 0$ for all $\sigma \in D_{\mathfrak{p}^\varsigma}$ and $\rho^{\mathcal{E}^\varsigma}_{11}(I_{\mathfrak{p}^\varsigma}) = 1$). Though $\mathcal{E}$ is defined on H and cannot be conjugated by ς, later we prove under (H0–2) an extension property claimed in Theorem C of the Cayley-Hamilton representation to a representation of G; so, we write $\mathcal{E}^\varsigma$ even if it is not a conjugate of $\mathcal{E}$ in proper sense. We say ρ is *ordinary* if it is $\mathfrak{p}$ and $\mathfrak{p}^\varsigma$-ordinary at the same time. This definition does not depends on the choice of $D_\mathfrak{p}$. If we replace $D_\mathfrak{p}$ by $\sigma D_\mathfrak{p} \sigma^{-1}$, $(E, \rho(\sigma)\mathcal{E}\rho(\sigma)^{-1})$ satisfies the required conditions. Here $\rho(\sigma)\mathcal{E}\rho(\sigma)^{-1} := \{\rho(\sigma)e_1\rho(\sigma)^{-1}, \rho(\sigma)e_2\rho(\sigma)^{-1}\}$ regarding $\rho(\sigma)$ as an element of E.

Lemma 5.4. *Let Γ be a profinite abelian group and $\rho = \left(\begin{smallmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{smallmatrix}\right) : A[\Gamma] \to E = \left(\begin{smallmatrix} A & B \\ C & A \end{smallmatrix}\right)$ be a Cayley–Hamilton representation into an A-GMA E for a p-profinite local algebra A with residue field $\mathbb{F}$. Then $\rho_{jj} : \Gamma \to A^\times$ $(j = 1, 2)$ are characters (i.e., ρ is reducible) and x (of Wiles' pseudo representation of Γ associated to $\rho|_\Gamma$) vanishes, and if Γ is prime-to-p profinite (i.e., the maximal p-profinite quotient is trivial), we have $\rho_{12} = \rho_{21} = 0$.*

Proof. Replacing B (resp. C) by the A-submodule generated by the image of ρ in B (resp. C), we may assume that ρ_{12} and ρ_{21} are onto. Write $\psi : B \otimes_A C \to A$ and $\psi' : C \otimes_A B \to A$ for the product laws of E. We may assume that $A[\Gamma] \to E$ is surjective, we can pick $x, y \in A[\Gamma]$ for any given $b, b' \in B$ and $c, c' \in C$ so that $\rho(x) = \left(\begin{smallmatrix} x_1 & b \\ c & x_2 \end{smallmatrix}\right)$ and $\rho(y) = \left(\begin{smallmatrix} y_1 & b' \\ c' & y_2 \end{smallmatrix}\right)$ for suitable $x_i, y_j \in A$. Since $\rho(x)\rho(y) = \rho(y)\rho(x)$, by computation, we find $\psi(b \otimes c') = \psi'(c \otimes b')$ for any $b, b' \in B$ and $c, c' \in C$. Choosing $b' = 0$ and $c = 0$, we find $\psi = 0$, and similarly, $\psi' = 0$. Therefore $x(g, h) = \psi(\rho_{12}(g) \otimes \rho_{21}(h)) = 0$, and ρ is reducible and $a = \rho_{11}, d = \rho_{22} : \Gamma \to A^\times$ are characters. Therefore ρ is reducible.

Suppose that Γ is prime-to-p profinite. Then by [FGS, Theorem 1.5.5] applied to $\rho \otimes 1 : \Gamma \to E \otimes_A \mathbb{F}$, we get $\mathrm{Hom}_A(B, \mathbb{F}) \hookrightarrow \mathrm{Ext}_{A[\Gamma]}(d \otimes 1, a \otimes 1) = 0$ as Γ is prime-to-p profinite. This shows $B \otimes_A \mathbb{F} = 0$, and by topological Nakayama's lemma, we find $B = 0$ and similarly $C = 0$, and hence $\rho_{12} = \rho_{21} = 0$. □

We now take $\mathcal{G}$ to be H. Write $E(\overline{\varphi}_\mathfrak{p} \oplus \overline{\varphi}_{\mathfrak{p}^\varsigma}) = \overline{\varphi} \oplus \overline{\varphi}_\varsigma = \left(\begin{smallmatrix} \overline{\varphi} & 0 \\ 0 & \overline{\varphi}_\varsigma \end{smallmatrix}\right)$ as a Cayley–Hamilton representation of $\mathbb{F}[H]$ into an $\mathbb{F}$-GMA $E_\mathbb{F} := \left(\begin{smallmatrix} \mathbb{F} & 0 \\ 0 & \mathbb{F} \end{smallmatrix}\right)$. We call ρ *an A-deformation* of $E(\overline{\varphi}_\mathfrak{p} \oplus \overline{\varphi}_{\mathfrak{p}^\varsigma})$ if $(\rho_{11}(\sigma) \bmod \mathfrak{m}_A) = \overline{\varphi}(\sigma)$, $(\rho_{22}(\sigma) \bmod \mathfrak{m}_A) = \overline{\varphi}_\varsigma(\sigma)$ and $\rho_{12}(\sigma)\rho_{21}(\sigma) \equiv 0 \mod \mathfrak{m}_A$. Though we have introduced outright the GMA as above, if T is Cayley–Hamilton, we can always lift T to a A-GMA representation (see [Ch14, Theorem 2.22 (ii)]); so, by doing this, we do not lose generality.

Conversely, given such a ρ, there is an induced A-valued pseudo character, denoted $T_\rho : H \to A$, given by $T_\rho = \rho_{11} + \rho_{22}$ and $\det(\rho) = \rho_{11}\rho_{22} - \rho_{12}\rho_{21}$, cf. [WE15, Prop. 2.2.3]. Comparing Wiles' pseudo representation with Cayley–Hamilton representation of Bellaïshe–Chenevier, we have $x(\sigma,\tau) = \rho_{12}(\sigma)\rho_{21}(\tau)$. Thus $\mathfrak{p}$-ordinarity (resp. $\mathfrak{p}^\varsigma$-ordinarity) of ρ is defined to be $\rho_{12}(\sigma) = 0$ for all $\sigma \in D_\mathfrak{p}$ and $\rho_{22}(I_\mathfrak{p}) = 1$ (resp. $\rho_{21}(\sigma) = 0$ for all $\sigma \in D_{\mathfrak{p}^\varsigma}$ and $\rho_{11}(I_{\mathfrak{p}^\varsigma}) = 1$). This definition depends on the fixed order of $(\overline{\varphi}, \overline{\varphi}_\varsigma)$ coming from $(\mathfrak{p}, \mathfrak{p}_\varsigma)$. If ρ is $\mathfrak{p}$-ordinary and $\mathfrak{p}^\varsigma$-ordinary at the same time, we call it an ordinary Cayley–Hamilton representation.

Write τ for the pseudo-character given by the trace of $E(\overline{\varphi}_\mathfrak{p} \oplus \overline{\varphi}_{\mathfrak{p}^\varsigma})$. The $\mathbb{F}$-GMA has two primitive idempotents $\overline{e}_1, \overline{e}_2$ so that on $\overline{e}_1$ (resp. $\overline{e}_2$), the Galois group acts by the character $\overline{\varphi}$ (resp. $\overline{\varphi}_\varsigma$). Thus we have a quadruple:

$$(E_\mathbb{F} := \begin{pmatrix} \overline{\varphi} & 0 \\ 0 & \overline{\varphi}_\varsigma \end{pmatrix}, \overline{\mathcal{E}} = \{\overline{e}_1, \overline{e}_2\}, D_{\overline{\varphi}\oplus\overline{\varphi}_\varsigma} : E_\mathbb{F} \to \mathbb{F}^\times, \overline{\varphi} \oplus \overline{\varphi}_\varsigma : H \to \overline{E}_\mathbb{F}^\times \text{ such that } \mathrm{Tr}(\overline{\varphi} \oplus \overline{\varphi}_\varsigma) = \overline{\varphi} + \overline{\varphi}_\varsigma).$$

Then the deformation determinant D with values in $A \in CNL_W$ of $D_{\overline{\varphi}\oplus\overline{\varphi}_\varsigma}$ is such that the base change $D \otimes_A \mathbb{F}$ is equal to $D_{\overline{\varphi}\oplus\overline{\varphi}_\varsigma}$. Consider the following deformation functor

$$\mathcal{D}_F : A \mapsto \{(E, D : E \to A, \rho^\mathcal{E} : H \to E^\times)\}/\cong \text{ and } \mathcal{D}^{pc} : A \mapsto \{(D : E \to A\}$$

where E is an A-GMA with a lift $\mathcal{E}$ of idempotents, $D : E \to A$ is a determinant such that $D \otimes_A \mathbb{F} = D_{\overline{\varphi}\oplus\overline{\varphi}_\varsigma}$ and $\rho : H \to E^\times$ is a Cayley–Hamilton representation with $D(\rho(h)) = \det(\rho(h))$. Here the equivalence "$\cong$" in the definition of $\mathcal{D}_F$ is an A-GMA isomorphism. An A-GMA morphism $\phi : (E, D, \rho)_{/A} \to (E', D', \rho')_{/A'}$ consists of a W-algebra local homomorphism $\phi_A : A \to A'$ and an A-GMA homomorphism $\phi_E : E \to E'$ such that $\phi_E \circ D = D'$ and $\phi_E \circ \rho \cong \rho'$. If the homomorphisms ϕ_A and ϕ_E as above are isomorphisms, the A-GMA morphism is an A-GMA isomorphism.

This functor $\mathcal{D}_F$ has an obvious morphism into $\mathcal{D}^{pc}$ given by $(E, D : E \to A, \rho^\mathcal{E} : H \to E^\times) \mapsto D$. The functor $\mathcal{D}_F$ is representable by a universal object $(R^u, E^u, D^u, T^u : E^u \to R^u, \rho^u_\mathbb{T} : H \to E^u)$ with $R \in CNL_W$ (see [Ch14, Proposition 1.23] and [WWE18, §5.5–6]). To simplify the notation, we just write this quadruple as $(R, \rho^u_\mathbb{T} : H \to E^{u,\times})$. By writing $\det(\rho^u_\mathbb{T})$ (resp. $\mathrm{Tr}(\rho^u_\mathbb{T})$), we mean $D^u : E^u \to R^u$ (resp. $T^u : E^u \to R^u$).

5.4. **Ordinary Cayley–Hamilton representation.** In H, we have two conjugacy classes of the p-decomposition groups depending on prime factors of p in K. Fix a decomposition subgroup $D_\mathfrak{p} \subset H$ for $\mathfrak{p}$ and put $D_{\mathfrak{p}^\varsigma}$ for $\mathfrak{p}^\varsigma$. We define $\mathfrak{p}$-ordinarity (resp. $\mathfrak{p}^\varsigma$-ordinarity) of ρ to have $\mathcal{E}$ (resp. $\mathcal{E}^\varsigma$) such that $\rho^\mathcal{E}_{12}(\sigma) = 0$ for all $\sigma \in D_\mathfrak{p}$ and $\rho^\mathcal{E}_{22}(I_\mathfrak{p}) = 1$ (resp. $\rho^{\mathcal{E}^\varsigma}_{21}(\sigma) = 0$ for all $\sigma \in D_{\mathfrak{p}^\varsigma}$ and $\rho^{\mathcal{E}^\varsigma}_{11}(I_{\mathfrak{p}^\varsigma}) = 1$). We say ρ is *ordinary* if it is $\mathfrak{p}$ and $\mathfrak{p}^\varsigma$-ordinary at the same time. This definition does not depends on the choice of $D_\mathfrak{p}$ and $D_{\mathfrak{p}^\varsigma}$. For example, if we replace $D_\mathfrak{p}$ by $\sigma D_\mathfrak{p} \sigma^{-1}$, $(E, \rho(\sigma)\mathcal{E}\rho(\sigma)^{-1})$ satisfies the required conditions. Here $\rho(\sigma)\mathcal{E}\rho(\sigma)^{-1} := \{\rho(\sigma)e_1\rho(\sigma)^{-1}, \rho(\sigma)e_2\rho(\sigma)^{-1}\}$ regarding $\rho(\sigma)$ as an element of E.

Remark 5.5. Requiring upper triangularity to both $\rho(D_\mathfrak{p})$ and $\rho(D_{\mathfrak{p}^\varsigma})$ is a notion different from the above definition of ordinarity. In other words, the quotient character of an ordinary Cayley–Hamilton representation in our sense has congruence to $\overline{\varphi}_\varsigma$ on $D_\mathfrak{p}$ and $\overline{\varphi}$ on $D_{\mathfrak{p}^\varsigma}$, and if we require upper triangularity on both $D_\mathfrak{p}$ and $D_{\mathfrak{p}^\varsigma}$, it has congruence to $\overline{\varphi}_\varsigma$ on both $D_\mathfrak{p}$ and $D_{\mathfrak{p}^\varsigma}$. For more details, see Remarks 7.5 and 7.6.

If $(E, \mathcal{E})$ can be embedded into the matrix algebra $M_2(\widetilde{A})$ for a complete local W-algebra $\widetilde{A}$ with residue field $\mathbb{F}$ containing A, the Cayley–Hamilton representation $\rho : H \to E^\times$ can be regarded as a representation into $\mathrm{GL}_2(\widetilde{A})$. Since $\overline{\rho} = \mathrm{Ind}_K^\mathbb{Q} \overline{\varphi}$ is irreducible over G, we may have an extension $\widetilde{\rho} : G \to \mathrm{GL}_2(\widetilde{A})$ of the GMA representation ρ to G. If an extension $\widetilde{\rho}$ exists, the extension is a usual representation into $\mathrm{GL}_2(\widetilde{A})$. As usual, we call $\widetilde{\rho}$ p-ordinary if $\widetilde{\rho}|_{G_p} \cong \left(\begin{smallmatrix} \epsilon & * \\ 0 & \delta \end{smallmatrix}\right)$ with unramified $\delta \equiv \varphi_\varsigma \mod \mathfrak{m}_{\widetilde{A}}$. The ordering of the residual representation $\begin{pmatrix} \overline{\varphi} & 0 \\ 0 & \overline{\varphi}_\varsigma \end{pmatrix}$ (with this order $\overline{\varphi}$ at the top) is fixed; so, plainly, to have compatibility of ordinarity of ρ over H and $\mathbb{Q}$-ordinarity of $\widetilde{\rho}$ (and to preserve residual order of the characters $\overline{\varphi}$ and $\overline{\varphi}_\varsigma$), we need to define $\mathfrak{p}^\varsigma$-ordinarity to have a set of idempotent $\mathcal{E}^\varsigma$ so that $\rho^{\mathcal{E}^\varsigma}|_{D_{\mathfrak{p}^\varsigma}}$ in the lower triangular form. Indeed, if $\widetilde{\rho}(\varsigma) = \left(\begin{smallmatrix} 0 & * \\ 1 & 0 \end{smallmatrix}\right)$, ρ is $\mathfrak{p}$-ordinary for $\mathcal{E}$ if and only if ρ is $\mathfrak{p}^\varsigma$-ordinary for the same $\mathcal{E}$ by choosing $D_{\mathfrak{p}^\varsigma} = \varsigma D_\mathfrak{p} \varsigma^{-1}$.

By [Ch14, Proposition 1.23] and [WWE18, Propositions 5.5.3 and 5.9.7], there exists a universal object

$$(R^{ord}, \mathcal{E}^{ord}, \boldsymbol{\rho}^{ord} : H \to E^{ord,\times}, T^{ord}, D^{ord})$$

made of the universal ordinary Cayley–Hamilton representation $\boldsymbol{\rho}^{ord}$ with values in the universal R^{ord}-GMA E^{ord} (with a lift $\mathcal{E}^{ord}$ of idempotents) and the universal ordinary pseudo character $T^{ord}: H \to R^{ord}$ with $T^{ord} = \mathrm{Tr}(\boldsymbol{\rho}^{ord})$ (resp. determinant) deforming φ (resp. $D_{\overline{\varphi}\oplus\overline{\varphi}_\varsigma}$).

Let us briefly recall the construction of $(R^{ord}, \boldsymbol{\rho}^{ord}: H \to E^{ord,\times})$. We consider the universal Cayley–Hamilton representation $\boldsymbol{\rho}^u : R^u[H] \to E^u = \left(\begin{smallmatrix} R^u & B^u \\ C^u & R^u \end{smallmatrix}\right)$ and its local version $\boldsymbol{\rho}^? : D_? \to E^{?,\times}$ for $E^? = \left(\begin{smallmatrix} R^? & B^? \\ C^? & R^? \end{smallmatrix}\right)$ for the decomposition subgroup $D_? \subset H$ of $? \in \{\mathfrak{p}, \mathfrak{p}^\varsigma\}$ (e.g., [Ch14, Proposition 1.23] and [WWE18, §5.4–5]); so, $\mathrm{Tr}(\boldsymbol{\rho}^u) = T$ and $\det(\boldsymbol{\rho}^u) = D$. Write it as $\boldsymbol{\rho}^? = \left(\begin{smallmatrix} \boldsymbol{\rho}^?_{11} & \boldsymbol{\rho}^?_{12} \\ \boldsymbol{\rho}^?_{21} & \boldsymbol{\rho}^?_{22} \end{smallmatrix}\right)$ for $? = u, \mathfrak{p}, \mathfrak{p}^\varsigma$. By the universality of $(R^?, E^?)$ for $? \in \{\mathfrak{p}, \mathfrak{p}^\varsigma\}$, we have a unique morphism of GMA's $(R^?, E^?) \xrightarrow{\pi^?} (R^u, E^u)$ such that $\boldsymbol{\rho}^u|_{D_?} = \pi^? \circ \boldsymbol{\rho}^?$.

Let $J^{\mathfrak{p}}$ (resp. $J^{\mathfrak{p}^\varsigma}$) be the two-sided ideal of $E^{\mathfrak{p}}$ (resp. $E^{\mathfrak{p}^\varsigma}$) generated by $\boldsymbol{\rho}^{\mathfrak{p}}_{21}(D_{\mathfrak{p}}) \subset \left(\begin{smallmatrix} 0 & 0 \\ C^u & 0 \end{smallmatrix}\right)$ and $\boldsymbol{\rho}^{\mathfrak{p}}_{22}(\delta) - 1 \in \left(\begin{smallmatrix} 0 & 0 \\ 0 & R^{\mathfrak{p}} \end{smallmatrix}\right)$ for δ in the inertia group $I_{\mathfrak{p}} \subset D_{\mathfrak{p}}$ (resp. by $\boldsymbol{\rho}^{\mathfrak{p}^\varsigma}_{12}(D_{\mathfrak{p}^\varsigma}) \subset \left(\begin{smallmatrix} 0 & B^{\mathfrak{p}^\varsigma} \\ 0 & 0 \end{smallmatrix}\right)$ and $\boldsymbol{\rho}^{\mathfrak{p}^\varsigma}_{11}(\delta) - 1 \in \left(\begin{smallmatrix} R^{\mathfrak{p}^\varsigma} & 0 \\ 0 & 0 \end{smallmatrix}\right)$ for $\delta \in I_{\mathfrak{p}^\varsigma} \subset D_{\mathfrak{p}^\varsigma}$). By [WWE18, Lemma 5.9.3] (strictly speaking by its proof replacing their residual representation by our $\overline{\varphi}\oplus\overline{\varphi}_\varsigma$), the ideal $J^?$ is well defined independent of the choice of the expression $\boldsymbol{\rho}^? = \left(\begin{smallmatrix} \boldsymbol{\rho}^?_{11} & \boldsymbol{\rho}^?_{12} \\ \boldsymbol{\rho}^?_{21} & \boldsymbol{\rho}^?_{22} \end{smallmatrix}\right)$ for $? = \mathfrak{p}, \mathfrak{p}^\varsigma$. By [WWE18, Lemma 5.9.4], for any ?-ordinary Cayley–Hamilton representation $\rho : D_? \to E$, the morphism $E^? \xrightarrow{\pi} E$ with $\rho \cong \pi \circ \boldsymbol{\rho}^?$ kills $J^?$; so, π factors through $E^{?\text{-ord}} := E^?/J^?$.

Definition 5.6. *Let $? \in \{\mathfrak{p}, \mathfrak{p}^\varsigma\}$ and $J^{?\text{-}ord}_{R^u} \subset R^u$ be the ideal generated by the subsets $\pi^?(\mathrm{Tr}(\boldsymbol{\rho}^?)(J^?))$ and $\pi^?(\det(\boldsymbol{\rho}^?)(J^?))$ and let $J^{?\text{-}ord}$ be the two-sided ideal of E^u generated by $\pi^?(J^?)$ and $J^{?\text{-}ord}_{R^u}$. Let $E^{?\text{-}ord} := E^u/J^{?\text{-}ord}$ and $R^{?\text{-}ord} := R^u/J^{?\text{-}ord}_{R^u}$.*

Then by [WWE18, Proposition 5.9.7], the pair $(R^{?\text{-ord}}, H \to E^{?\text{-ord}})$ gives the universal ?-ordinary Cayley–Hamilton representation.

Definition 5.7. *We define $R^{ord} := R^u/(J^{\mathfrak{p}\text{-}ord}_{R^u} + J^{\mathfrak{p}^\varsigma\text{-}ord}_{R^u})$ and $E^{ord} := E^u/(J^{\mathfrak{p}\text{-}ord} + J^{\mathfrak{p}^\varsigma\text{-}ord})$.*

Note that E^{ord} (resp. R^{ord}) is the "push-out" of the two morphisms $E^u \to E^{\mathfrak{p}\text{-ord}}$ and $E^u \to E^{\mathfrak{p}^\varsigma\text{-ord}}$ (resp. $R^u \to R^{\mathfrak{p}\text{-ord}}$ and $R^u \to R^{\mathfrak{p}^\varsigma\text{-ord}}$) in the category of GMA's (resp. p-profinite local W-algebras); so, automatically E^{ord} is a R^{ord}-GMA. Therefore, $(R^{ord}, H \to E^{ord})$ is the universal pair of the universal ordinary Cayley–Hamilton pseudo character ring and the universal Cayley–Hamilton representation. In other words, $(R^{ord}, H \to E^{ord})$ represents the functor

$$\mathcal{D}^{ord}_F : A \mapsto \{(E, D : E \to A, \rho^{\mathcal{E}} : H \to E^\times) : \text{ordinary}\}/\cong,$$

where E is an ordinary A-GMA with a lift $\mathcal{E}$ of idempotents, $D : E \to A$ is a determinant such that $D \otimes_A \mathbb{F} = D_{\overline{\varphi}\oplus\overline{\varphi}_\varsigma}$ and $\rho : H \to E^\times$ is a Cayley–Hamilton representation with $D(\rho(h)) = \det(\rho(h))$. Call a determinant $D : H \to A$ and a pseudo-character $T : H \to A$ ordinary if it has a lifting to an ordinary Cayley–Hamilton representation into an A-GMA.

Lemma 5.8. *We have a canonical isomorphism $R^{ps,ord} \cong R^{ord}$.*

Proof. By Lemma 5.2 (4), $\mathrm{Tr}(\pi)$ for Wiles' pseudo representation is a pseudo character. The determinant $\det(\pi)$ is multiplicative and determined by $\mathrm{Tr}(\pi)$ as $p > 2$. Indeed, writing $\pi = (a, d, x)$, x is determined by a and d by (W1), and assuming 2 is invertible, we have $a(g) = \frac{1}{2}(\mathrm{Tr}(\pi(g) - \mathrm{Tr}(\pi(gc)))$ and $d(g) = \frac{1}{2}(\mathrm{Tr}(\pi(g) + \mathrm{Tr}(\pi(gc)))$ as we recalled just after (W3). Therefore $\det(\pi)(r) = a(r)d(r) - x(r, r)$ is determined by $\mathrm{Tr}(\pi)$ as long as 2 is invertible. By universality of R^{ord}, we have the morphism $R^{ord} \xrightarrow{\pi} R^{ps,ord}$ sending (T^u, D^u) to $(\mathrm{Tr}(\boldsymbol{\pi}^{ps,ord}), \det(\boldsymbol{\pi}^{ps,ord}))$. Since $\mathrm{Tr}(\pi^{ps,ord})$ determines $\pi^{ps,ord}$, $R^{ps,ord}$ is generated by the values of $\mathrm{Tr}(\boldsymbol{\pi}^{ps,ord})$, and hence π is surjective. Writing $\boldsymbol{\rho}^{ord} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we have an ordinary pseudo representation (a, d, x) with $x(h, h') = b(h)c(h')$; so, by the universality, we have a morphism $\iota : R^{ps,ord} \to R^{ord}$. Writing $\boldsymbol{\pi}^{ps,ord} = (\mathbf{a}, \mathbf{d}, \mathbf{x})$, by definition $\iota \circ (\mathbf{a}, \mathbf{d}, \mathbf{x}) = (a, d, x)$ and $\pi \circ T^u = \mathrm{Tr}(\boldsymbol{\pi}^{ps,ord})$, these two maps are inverse each other as desired. □

6. Explicit form of the universal reducible Cayley–Hamilton representation

We continue to assume (H0–1). We make explicit the reducible locus R^{red} of the ordinary universal ring R^{ord} and the universal reducible R^{red}-*GMA* E^{red}. The explicit form here is the key to the proof of Theorem C.

Let $\mathcal{J} \subset R^{ord}$ be the ideal of the reducibility locus $\mathrm{Spec}(R^{red})$ (see [FGS, §1.5.1] and [WWE17, §3.3–5]); so, R^{red} is given by $R^{ord}/\mathcal{J}$. The algebra R^{red} is equipped with a universal R^{red}-GMA E^{red} and a universal reducible Cayley–Hamilton representation $\boldsymbol{\rho}^{red} : H \to E^{red}$ (see [WWE18, Proposition 7.3.1]). Write the entries of the universal Cayley–Hamilton representation $H \to E^{red}$ as ρ_{ij}, and put $T^{red} = \rho_{11} + \rho_{22}$. Over the reducibility locus, $\rho_{11} \oplus \rho_{22}$ is a representation of H deforming $\overline{\varphi} \oplus \overline{\varphi}_{\varsigma}$. Recall the universal deformation $\Phi : H \to W[C]^{\times}$ of the character $\overline{\varphi}$ unramified outside $\mathfrak{c}\mathfrak{p}\infty$.

Since $(W[C], \Phi)$ is universal among characters of H deforming $\overline{\varphi}$, we have a morphism of CNL_W $g : W[C] \to R^{red}$ with $g \circ \Phi = \rho_{11}$. Since R^{red} is generated by the values of T^{red} and $\det(\boldsymbol{\rho}^{red})$ has values in $W[C]^{\times}$, by p-distinguishedness (and Hensel's lemma), we can solve the values of the character ρ_{11} mod $\mathcal{J}$ out of the information of T^{red}. Thus R^{red} is actually generated by the values of the character ρ_{11}, and hence g is surjective. Define a $W[C]$-GMA by $E(\Phi \oplus \Phi_{\varsigma}) = \left(\begin{smallmatrix} W[C] & 0 \\ 0 & W[C] \end{smallmatrix}\right)$. Since $\Phi \oplus \Phi_{\varsigma} : H \to E(\Phi \oplus \Phi_{\varsigma})^{\times}$ for the universal character $\Phi : H \to W[C]$ is a Cayley–Hamilton representation deforming $E(\overline{\varphi}_{\mathfrak{p}} \oplus \overline{\varphi}_{\mathfrak{p}^{\varsigma}})$, we have a universal map $f : E^{red} \to E(\Phi \oplus \Phi_{\varsigma})$, which induces $f_{11} : R^{red} \to W[C]$ with $f_{11} \circ \rho_{11} = \Phi$. Thus f_{11} is onto as $W[C]$ is generated by the values of Φ over W. Since $f_{11} \circ g$ and $g \circ f_{11}$ are both onto, they are isomorphisms. This shows

Lemma 6.1. *The canonical morphism: $R^{red} \to W[C]$ is a surjective isomorphism of Λ-algebras.*

By this lemma, $W[C]$-modules $\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W$ and $\varsigma\mathcal{Y}(\varphi^-)\varsigma^{-1} \otimes_{\mathbb{Z}_p[\varphi^-]} W$ are naturally R^{red}-modules.

We have the universal Cayley–Hamilton pseudo character $T^? : H \to R^?$ for $? = ord, red$. By [FGS, Theorem 1.4.4 (i)], we have the universal (surjective) Cayley–Hamilton representation $\boldsymbol{\rho}^? : R^?[H] \to E^? = \left(\begin{smallmatrix} R^? & B^? \\ C^? & R^? \end{smallmatrix}\right)$. Surjectivity of $\boldsymbol{\rho}^?$ follows from the construction of $E^?$ as the maximal GMA quotient of $R^?[H]$ with the property ? (see [Ch14, §1.22]). By [FGS, Proposition 1.5.1] or [WE15, §7.3], $\mathcal{J}$ is the image (under the GMA product law of E^{ord}) of $B^{ord} \otimes_{R^{ord}} C^{ord}$ in R^{ord}, and $R^{red} = R^{ord}/\mathcal{J}$.

Proposition 6.2. *We have*

$$B^{red} \cong \mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W \quad \text{and} \quad C^{red} \cong \varsigma\mathcal{Y}(\varphi^-)\varsigma^{-1} \otimes_{\mathbb{Z}_p[\varphi^-]} W$$

as R^{red}-modules, where $\mathcal{Y}(\varphi^-)$ and $\varsigma\mathcal{Y}(\varphi^-)\varsigma^{-1}$ are as in Definition 3.8.

Proof. Write $W[C]^{\vee}$ for the Pontryagin dual of $W[C]$. Let

$$X_n = W[C]^{\vee}[p^n] = \{x \in W[C]^{\vee} | p^n x = 0\} \cong (W[C]/p^n W[C])^{\vee}.$$

Note that $W[C]^{\vee} = \varinjlim_n X_n$ and X_n/X_{n-1} is a free $\mathbb{F}[C]$-module of rank 1. Since X_n is a finite module, as Λ-modules $X_n \cong W/p^n W[C]$ which is a cohomologically trivial C-module. Define $X_n(\phi)$ by the module X_n with H-action given by $\phi = \Phi, \Phi_{\varsigma}$ and Φ^-. By [FGS, Theorem 1.5.5] applied to $E^{red} \otimes_{R^{red}} W[C]/p^n W[C]$, we have an injective Λ-linear map

$$\iota_n : \mathrm{Hom}_{R^{red}}(B^{red}, X_n) \hookrightarrow \mathrm{Ext}^1_{W[H]}(X_n(\Phi_{\varsigma}), X_n(\Phi)) = H^1(H, X_n(\Phi^-)).$$

Let $\Phi_n^- := \Phi^-$ mod $p^n W[C]$; so, $\mathrm{Im}(\Phi_n^-) = C$. By inflation-restriction sequence, we have an exact sequence

$$H^1(\mathrm{Im}(\Phi_n^-), X_n(\Phi^-)) \to H^1(H, X_n(\Phi^-)) \to \mathrm{Hom}_H(\mathrm{Ker}(\Phi_n^-), X_n(\Phi^-)) \to H^2(\mathrm{Im}(\Phi_n^-), X_n(\Phi^-)).$$

Since $\mathrm{Im}(\Phi_n^-) \cong C$ and $X_n(\Phi^-)$ is a cohomologically trivial C-module, $H^j(\mathrm{Im}(\Phi_n^-), X_n(\Phi^-)) = 0$ $(j = 1, 2)$. In the construction of ι_n, writing (ρ_{ij}^{red}) for the universal reducible Cayley–Hamilton representation and taking an element $f \in \mathrm{Hom}_{R^{red}}(B^{red}, X_n)$, Bellaïshe and Chenevier made a Cayley–Hamilton representation

$$x \mapsto \begin{pmatrix} \rho_{11}^{red} & f \circ \rho_{12}^{red} \\ 0 & \rho_{22}^{red} \end{pmatrix} \tag{6.1}$$

in [FGS, §1.5.3 (12)]. Note $\rho_{11}^{red} = \Phi$ and $\rho_{22}^{red} = \Phi_{\varsigma}$. Thus each element $f \in \mathrm{Hom}_{R^{red}}(B^{red}, X_n)$ is sent to a homomorphism $f \circ \rho_{12} \in \mathrm{Hom}_H(\mathrm{Ker}(\Phi_n^-), X_n(\Phi^-))$. This Cayley–Hamilton representation is ordinary and upper triangular; so, the extension class can possibly ramify at $\mathfrak{p}$ and unramified at $\mathfrak{p}^{\varsigma}$. Thus, the image of ι_n lands in

$$\mathrm{Hom}_{W[C]}(\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W, X_n(\Phi^-)) \subset \mathrm{Hom}_H(\mathrm{Ker}(\Phi^-), X_n(\Phi^-)).$$

In other words, we get

$$\iota_n : \mathrm{Hom}_{R^{red}}(B^{red}, X_n) \hookrightarrow \mathrm{Hom}_{W[C]}(\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W, X_n(\Phi^-)). \tag{6.2}$$

Pick $\phi \in \mathrm{Hom}_{W[C]}(\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W, X_n)$. Then ϕ corresponds to an extension $X_n(\Phi) \hookrightarrow \mathcal{E} \twoheadrightarrow X_n(\Phi_\varsigma)$. Taking $x \in \mathcal{E}$ projecting down to the image of $1 \in W[C](\Phi_\varsigma)$ in $X_n(\Phi_\varsigma)$, we define $f : H \to X_n = X_n(\Phi)$ by $f(h) = hx - \Phi_\varsigma(h)x$ and a Cayley–Hamilton representation $\rho : H \to \begin{pmatrix} W[C] & X_n \\ 0 & W[C] \end{pmatrix}$ by

$$\rho(h) := \begin{pmatrix} \Phi(h) & f(h) \\ 0 & \Phi_\varsigma(h) \end{pmatrix},$$

whose trace is a deformation of the pseudo-character τ. Therefore, by the universality of E^{red}, we have a unique map $\underline{\phi} \in B^{red} \to X_n$ inducing this Cayley–Hamilton representation. This $\underline{\phi}$ recovers ϕ and $\iota_n(\underline{\phi}) = \phi$; so, $\iota_n : \mathrm{Hom}_{W[C]}(B^{red}, X_n) \to \mathrm{Hom}_{W[C]}(\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W, X_n)$ is onto and hence is an isomorphism. Passing to the injective limit of $X_n = (W[C]/p^nW[C])^\vee$ with respect to n, we get an isomorphism

$$\begin{aligned}\iota_\infty : (B^{red})^\vee \cong \mathrm{Hom}_{W[C]}(B^{red}, W[C]^\vee) &\cong \mathrm{Hom}_{W[C]}(\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W, W[C]^\vee) \\ &\cong (\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W)^\vee.\end{aligned} \tag{6.3}$$

For the augmentation map $a : W[C] \to W$, the pairing $(x, y) = a(xy)$ gives rise to an isomorphism $W[C] \cong \mathrm{Hom}_{W[C]}(W[C], W)$; so, $W[C]$ is a Gorenstein (see the bottom of page 199 of [H16] for an argument showing $W[C]$ is actually a local complete intersection over W). By taking Pontryagin dual, we find $B^{red} \cong \mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W$. The other identity $C^{red} \cong \varsigma\mathcal{Y}(\varphi^-)\varsigma^{-1} \otimes_{\mathbb{Z}_p[\varphi^-]} W$ can be proven similarly taking a lower triangular representation similar to ρ. □

Lemma 6.3. *We have $E^{ord}/\mathcal{J}E^{ord} \cong E^{red}$ canonically and in particular, $B^{ord}/\mathcal{J}B^{ord} \cong B^{red}$ and $C^{ord}/\mathcal{J}C^{ord} \cong C^{red}$.*

Proof. The Cayley–Hamilton representation $\boldsymbol{\rho}^{ord} \otimes 1$ into $E^{ord} \otimes_{R^{ord}} R^{red} = E^{ord}/\mathcal{J}E^{ord}$ is reducible in the sense of [FGS, §1.5.1]. By the remark just after Lemma 6.1, we have a surjective morphism of R^{red}-GMA $\pi : E^{red} \to E^{ord}/\mathcal{J}E^{ord}$ such that $\pi \circ \boldsymbol{\rho}^{red} \cong \boldsymbol{\rho}^{ord} \otimes 1$. Since the image of $\boldsymbol{\rho}^{ord}$ generates E^{ord} over R^{ord}, π is surjective. Since $\boldsymbol{\rho}^{red} : H \to E^{red}$ is ordinary, we have a surjective morphism $\varpi : E^{ord} \twoheadrightarrow E^{red}$ with $\varpi \circ \boldsymbol{\rho}^{ord} = \boldsymbol{\rho}^{red}$; so, ϖ factors through $E^{ord}/\mathcal{J}E^{ord}$. Thus the composites $\pi \circ \varpi$ and $\varpi \circ \pi$ are both onto. Since the GMA's are noetherian, we conclude $\pi \circ \varpi$ and $\varpi \circ \pi$ are isomorphisms. They are identity maps as $\varpi \circ \boldsymbol{\rho}^{ord} = \boldsymbol{\rho}^{red}$ and $\pi \circ \boldsymbol{\rho}^{red} \cong \boldsymbol{\rho}^{ord} \otimes 1$. Thus we conclude $E^{ord}/\mathcal{J}E^{ord} \cong E^{red}$ as R^{ord}-GMA, which implies the isomorphisms of the lemma. □

7. Modularity of R^{ord}: proof of Theorem C

Recall the pseudo-character τ given by the trace of $E(\overline{\varphi}_{\mathfrak{p}} \oplus \overline{\varphi}_{\mathfrak{p}^\varsigma})$. We first note

Proposition 7.1. *Assume* (H0–1). *Let $\mathbb{T}_F$ be the local ring of the p-ordinary cuspidal F-Hilbert modular big Hecke algebra of prime-to-p level $N_{F/\mathbb{Q}}(\mathfrak{c})$ with tame Neben character $\varphi\varphi_\varsigma$ whose residual pseudo-character is given by τ. Then the following assertions hold:*

1. *We have a pseudo character $T_F : H \to \mathbb{T}_F$ deforming τ such that $T_F(\mathrm{Frob}_\mathfrak{l})$ is given by the projection of the Hecke operator $T(\mathfrak{l})$ in $\mathbb{T}_F$ for all primes outside $pN_{F/\mathbb{Q}}(\mathfrak{c})$, and there exists a $\mathbb{T}_F$-GMA $E_{\mathbb{T}_F} = \begin{pmatrix} \mathbb{T}_F & B_{\mathbb{T}_F} \\ C_{\mathbb{T}_F} & \mathbb{T}_F \end{pmatrix}$ with an ordinary Cayley–Hamilton representation $\rho_{\mathbb{T}_F} : H \to E^\times_{\mathbb{T}_F}$ such that $\mathrm{Tr}(\rho_{\mathbb{T}_F}) = T_F$ with ideal $\mathcal{J}$ of reducibility over H which is the image of $B_{\mathbb{T}_F} \otimes_{\mathbb{T}_F} C_{\mathbb{T}_F}$.*
2. *We have a pseudo character $T_+ : H \to \mathbb{T}_+$ deforming τ such that $T_+(\mathrm{Frob}_\mathfrak{l})$ is given by the projection of the Hecke operator $T(l)$ in $\mathbb{T}_+$ for all primes outside $pN_{F/\mathbb{Q}}(\mathfrak{c})$ with $\chi(l) = 1$, and there exists a $\mathbb{T}_+$-GMA $E_{\mathbb{T}_+} = \begin{pmatrix} \mathbb{T}_+ & B_{\mathbb{T}_+} \\ C_{\mathbb{T}_+} & \mathbb{T}_+ \end{pmatrix}$ with an ordinary Cayley–Hamilton representation $\rho_{\mathbb{T}_+} : H \to E^\times_{\mathbb{T}_+}$ such that $\mathrm{Tr}(\rho_{\mathbb{T}_+}) = T_+$ with ideal $\mathcal{J}_+$ of reducibility over H which is the image of $B_{\mathbb{T}_+} \otimes_{\mathbb{T}_F} C_{\mathbb{T}_+}$.*

Since the proof is the same, we deal with the first assertion involving $\mathbb{T}_F$.

Proof. Since the prime-to-p conductor of $\varphi\varphi_\varsigma$ equals the level $N_{F/\mathbb{Q}}(\mathfrak{c})$, the algebra $\mathbb{T}_F$ is reduced by the same argument proving Lemma 2.1 via the Hilbert modular version of the theory of new forms. By [Ch14, Proposition 1.29], pseudo character and determinant are equivalent notion (as $p > 2$). For each minimal ideal P of $\mathbb{T}_F$, we have the Galois representation $\rho_P : H \to GL_2(\mathbb{T}_F/P \otimes_\Lambda Q)$ for the quotient field Q of Λ with $\mathrm{Tr}(\rho_P)(\sigma), \det(\rho_P)(\sigma) \in \mathbb{T}_F/P$ (by using Wiles' construction [Wi88] or by [FGS, Theorem 1.4.4 (ii)]). Put $\rho_F = \oplus_P \rho_P$ as representation having values in $\mathrm{GL}_2(\mathbb{T}_F \otimes_\Lambda Q)$. Then $D_{\mathbb{T}_F} := \det(\rho_F)$ is a determinant with values in $\mathbb{T}_F$ in the sense of Definition 5.3, and hence by [FGS, Theorem 1.4.4 (ii)], it is associated to a Cayley–Hamilton representation as in the proposition. □

Lemma 7.2. *Under* (H0–1) (*resp.* (H0–3)), *the ring* $\mathbb{T}$ *is generated over* $\mathbb{T}_+$ (*resp. over* Λ) *by* $\mathrm{Tr}(\rho_{\mathbb{T}}(\mathrm{Frob}_l))$ *for* r_- *primes* l (*resp. a single prime* l) *inert in* F *outside* Np, *where* $r_- = \dim_{\mathbb{F}} \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \varphi^-)$.

Proof. By definition, $\mathbb{T}$ is generated by the image $a(l) = \mathrm{Tr}(\mathrm{Frob}_l)$ of $T(l)$ (here we write $T(l)$ for $U(l)$ even if $l|Np$). Let $\mathbb{T}'$ be the subring of $\mathbb{T}$ generated over Λ by $a(l)$ for all $l \nmid Np$. By Chebotarev density theorem, $\mathrm{Tr}(\rho_{\mathbb{T}})$ has values in $\mathbb{T}'$. Thus for example, by Wiles' construction from his pseudo representation attached to $\rho_{\mathbb{T}}$, we have the Galois representation $\rho_{\mathbb{T}'} : G \to \mathrm{GL}_2(\mathbb{T}')$ isomorphic to $\rho_{\mathbb{T}}$ after extending scalars to $\mathbb{T}$. If $l|N$ and either $\overline{\rho}|_{D_l}$ is irreducible or $\rho_{\mathbb{T}'}|_{D_l} \cong \left(\begin{smallmatrix}\psi & 0\\ 0 & \psi'\end{smallmatrix}\right)$ with both ψ and ψ' ramifies, $a(l) = 0$; so, we can ignore such primes. Assume $l|N$ and $\rho_{\mathbb{T}'}|_{I_l} \cong \left(\begin{smallmatrix}\psi & 0\\ 0 & 1\end{smallmatrix}\right)$. By minimality (H1), ψ ramifies and has order prime to p. Thus $H_0(I_l, \rho_{\mathbb{T}'}) \cong \mathbb{T}'$ on which $\mathrm{Frob}_{\mathfrak{l}}$ for a (well-chosen) prime $\mathfrak{l}|l$ in F acts by $a(l)$; so, $a(l) \in \mathbb{T}'$. If φ ramifies at p, the same argument shows $a(p) \in \mathbb{T}'$. If φ is unramified at p, choosing a representative $\phi \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ of $\mathrm{Frob}_{\mathfrak{p}}$, by (H0), $\rho_{\mathbb{T}'}(\phi)$ has two distinct eigenvalues modulo $\mathfrak{m}_{\mathbb{T}'}$. By Hensel's lemma, the eigenvalues are in $\mathbb{T}'$; so, each eigenspace is free of rank 1 over $\mathbb{T}'$. By ordinarity, one of the eigenspaces has action of ϕ via multiplication by an element $\delta \in \mathbb{T}'$ with $\delta \equiv \overline{\varphi}_\varsigma(\phi) \mod \mathfrak{m}_{\mathbb{T}'}$. On this eigenspace, ϕ acts via multiplication by $a(p) = \delta \in \mathbb{T}$; so, $a(p) \in \mathbb{T}'$. This shows $\mathbb{T} = \mathbb{T}'$. Since $\sigma(a(l)) = \chi(l)a(l)$ for $\chi = \left(\frac{F/\mathbb{Q}}{}\right)$ and $\mathbb{T} = \Lambda[\Theta]$ for Θ with $\sigma(\Theta) = -\Theta$ under (H0–3) by Theorem 4.1, we can choose an inert prime l such that the image of $a(l)$ in t^* generates t^* over $\mathbb{F}$. Thus $a(l)$ generates $\mathbb{T}$ over Λ under (H0–3).

If we suppose only (H0–1), by Proposition 3.6, $\mathbb{T}$ is generated over $\mathbb{T}_+$ by Θ_j ($j = 1, \ldots, j_{r_-}$) with $\sigma(\Theta_j) = -\Theta_j$; so, we need r_- primes l with $\chi(l) = -1$ to choose Θ_j among $a(l)$s. □

Let $\mathbb{T}_- := \{x \in \mathbb{T} | \sigma(x) = -x\}$. Then $\mathbb{T}_- = \Theta\mathbb{T}_+$ under (H0–2) by Theorem 3.4. Extend the character $\overline{\varphi}$ to a function on G just by 0 outside H to have the following standard realization of the induced representation:

$$\overline{\rho}(\tau) = \begin{pmatrix} \overline{\varphi}(\tau) & \overline{\varphi}(\tau\varsigma) \\ \overline{\varphi}(\varsigma^{-1}\tau) & \overline{\varphi}(\varsigma^{-1}\tau\varsigma) \end{pmatrix}.$$

Then if $\chi(\tau) = -1$ ($\Leftrightarrow \tau \notin H$), we have

$$(\overline{\rho} \otimes \chi)(\tau) = \begin{pmatrix} 0 & -\overline{\varphi}(\tau\varsigma) \\ -\overline{\varphi}(\varsigma^{-1}\tau) & 0 \end{pmatrix} = j\overline{\rho}(\tau)j^{-1}$$

for $j := \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$. If $\chi(\tau) = 1$ ($\Leftrightarrow \tau \in H$), $\overline{\rho}(\tau)$ is diagonal commuting with j; so,

$$(\overline{\rho} \otimes \chi)(\tau) = \overline{\rho}(\tau) = j\overline{\rho}(\tau)j^{-1}.$$

Thus we conclude $\overline{\rho} \otimes \chi = j\overline{\rho}j^{-1}$.

Here is a more explicit version of $E_{\mathbb{T}_+}$:

Lemma 7.3. *Assume* (H0–1). *After conjugating* $\rho_{\mathbb{T}}$ *under a suitable element in* $\mathrm{GL}_2(\mathbb{T})$, *we can arrange* $\rho_{\mathbb{T}}|_H$ *to have values in the* $\mathbb{T}_+$*-GMA* $E_+ := \left(\begin{smallmatrix}\mathbb{T}_+ & \mathbb{T}_-\\ \mathbb{T}_- & \mathbb{T}_+\end{smallmatrix}\right)$ *so that* $\rho_{\mathbb{T}}(c) = \mathrm{diag}[-1, 1]$ *and* $\rho_{\mathbb{T}}(\delta) = \mathrm{diag}[\varphi(\delta), \varphi_\varsigma(\delta)]$ *for* $\delta \in \Delta_{\mathfrak{p}}$ *and the complex conjugation* c *chosen in* (D2), *where the product law:* $\mathbb{T}_- \otimes_{\mathbb{T}_+} \mathbb{T}_- \to \mathbb{T}_+$ *is given by* $b \otimes c = bc$ *with the product* bc *in* $\mathbb{T}$.

Proof. Recall from (s6) the deformation functor giving rise to $R_{\mathbb{Q}}$:

$$\mathcal{D}(A) := \{\rho : G \to \mathrm{GL}_2(A) : p\text{-}ordinary\ |(\rho \bmod \mathfrak{m}_A) = \overline{\rho}\}/\Gamma(\mathfrak{m}_A). \tag{7.1}$$

We have the involution σ on $R_{\mathbb{Q}}$ given in the introduction. We let χ act on D by

$$\rho \mapsto j(\rho \otimes \chi)j^{-1} \approx \rho^\sigma.$$

Recall the ideal of reducibility $\mathcal{J}_+$ defined in Proposition 7.1. Since $j\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)j^{-1} = \left(\begin{smallmatrix} a & -b \\ -c & d \end{smallmatrix}\right)$ and $(\rho_{\mathbb{T}}|_H \mathrm{mod}\ \mathcal{J}_+) = \Phi \oplus \Phi_\varsigma$ is diagonal, we have $uj(\rho_{\mathbb{T}} \otimes \chi)(uj)^{-1} = \rho_{\mathbb{T}}^\sigma$ with $u \in 1 + \mathcal{J}_+ M_2(\mathbb{T})$. Write $U = uj$. Applying σ, we get $U^\sigma(\rho_{\mathbb{T}}^\sigma \otimes \chi)U^{-\sigma} = \rho_{\mathbb{T}}$; so, we have

$$U\rho_{\mathbb{T}}U^{-1} = U(\rho_{\mathbb{T}} \otimes \chi)U^{-1} \otimes \chi = \rho_{\mathbb{T}}^\sigma \otimes \chi = U^{-\sigma}\rho_{\mathbb{T}}U^\sigma.$$

Thus $ju^\sigma ju = U^\sigma U = z \in Z := 1 + \mathcal{J}_+\mathbb{T}$. Since $1 + \mathcal{J}_+ M_2(\mathbb{T})$ is p-profinite, letting σ acts on $1 + \mathcal{J}_+ M_2(\mathbb{T})$ by $x \mapsto x^{\widetilde{\sigma}} := jx^\sigma j$, we can write $u = v^{\widetilde{\sigma}-1} \in (1 + \mathcal{J}_+ M_2(\mathbb{T}))$ for $v \in 1 + \mathcal{J}_+ M_2(\mathbb{T})$. Replacing $\rho_{\mathbb{T}}|_H$ by $v^{-1}j\rho_{\mathbb{T}}jv|_H$, we find $j\rho_{\mathbb{T}}|_H j^{-1} = \rho_{\mathbb{T}}^\sigma|_H$. In other words, $\rho_{\mathbb{T}}|_H$ has values in $E_+ = \left(\begin{smallmatrix} \mathbb{T}_+ & \mathbb{T}_- \\ \mathbb{T}_- & \mathbb{T}_+ \end{smallmatrix}\right)$. □

Here is a slightly more detailed version of Theorem C.

Theorem 7.4. *Suppose* (H0–2). *We have canonical isomorphisms for R^{ps} as in* Lemma 5.1*:*

$$R^{ord} \cong \mathbb{T}_F \cong R^{ps} \cong \mathbb{T}_+.$$

All the rings above are local complete intersection over Λ.

Proof. Let Θ be a generator of I as in Corollary 3.7. By Lemma 7.2, we may assume that $\Theta = \mathrm{Tr}(\rho_{\mathbb{T}}(\mathrm{Frob}_l))$ for a prime l inert in F outside Np. For any prime q outside Np inert in F, we have $\mathrm{Tr}(\rho_{\mathbb{T}}(\mathrm{Frob}_q^2)) + \det(\rho_{\mathbb{T}}(\mathrm{Frob}_q))$. Since $\det(\rho_{\mathbb{T}}(\mathrm{Frob}_q)) \in \Lambda$ and $\mathrm{Frob}_q^2 \in H$, we find that $\mathbb{T}_+$ is generated over Λ by the trace of $\rho_{\mathbb{T}}|_H$; so, $\beta : R^{ord} \to \mathbb{T}_+$ is surjective. By Lemma 7.3, we regard $\rho_{\mathbb{T}}|_H$ as a Cayley-Hamilton representation of H with values in the $\mathbb{T}_+$-GMA E_+ inside $M_2(\mathbb{T})$. Since $I = (\Theta)$ is the minimal ideal of reducibility of $\mathbb{T}$ such that $\rho_{\mathbb{T}}$ mod I is an induced representation of a character from H, for $\Theta_+ := \Theta^2$, $(\Theta_+) = I \cap \mathbb{T}_+$ is the minimal ideal such that $\rho_{\mathbb{T}} : H \to E_+ \otimes_{\mathbb{T}_+} \mathbb{T}_+/I_+$ is reducible; so, (Θ_+) is the ideal of reducibility for $\rho_{\mathbb{T}}|_H$, $\mathcal{J}$ surjects down to I_+.

Recall the ideal $\mathcal{J}$ of the reducible locus of R^{ord}. Since $R^{red} = R^{ord}/\mathcal{J}$ and $E^{red} = E^{ord}/\mathcal{J}E^{ord}$ by Lemma 6.3, we have $B^{red} = B^{ord}/\mathcal{J}B^{ord}$ and $C^{red} = C^{ord}/\mathcal{J}C^{ord}$. By Proposition 6.2 combined with cyclicity over $W[C]$ of $\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W$ (Theorem 3.9), we find $B^{ord}/\mathcal{J}B^{ord}$ is cyclic over R^{ord}. By Nakayama's lemma, B^{ord} is cyclic over R^{ord}. Similarly C^{ord} is cyclic over R^{ord}. By [FGS, Proposition 1.5.1], $\mathcal{J}$ is the image in R^{ord} of $B^{ord} \otimes_{R^{ord}} C^{ord}$ under the product law of E^{ord}; so $\mathcal{J}$ is cyclic. Therefore $\mathcal{J}$ is a principal ideal generated by an element $\eta \in R^{ord}$. Multiplication by $\eta : R^{ord}/\mathcal{J} = R^{red} \to \mathcal{J}/\mathcal{J}^2$ is surjective.

By Lemma 6.1, we have $R^{red} \cong W[C]$. Therefore we have a surjective Λ-linear map $W[C] \twoheadrightarrow \mathcal{J}/\mathcal{J}^2$. Since $\mathcal{J}/\mathcal{J}^2$ surjects onto $I_+/I_+^2 \cong W[C]$, the composed map $W[C] \twoheadrightarrow \mathcal{J}/\mathcal{J}^2 \twoheadrightarrow I_+/I_+^2 = W[C]$ is an onto W-linear map. Comparing the W-rank, it is an isomorphism; so, we find in particular that $\mathcal{J}/\mathcal{J}^2 \cong I_+/I_+^2$. By Theorem 3.4, Θ is not a zero divisor, and therefore Θ_+ is not a zero divisor. Since Θ_+ is not a zero divisor in $\mathbb{T}_+$, we have a commutative diagram:

$$\begin{array}{ccc} \mathcal{J}/\mathcal{J}^2 & \xrightarrow{\sim} & I_+/I_+^2 \\ \text{onto}\downarrow{\scriptstyle j\mapsto\eta^{n-1}j} & & \wr\downarrow \quad i \mapsto \Theta_+^{n-1}i \\ \mathcal{J}^n/\mathcal{J}^{n+1} & \xrightarrow{\text{onto}} & I_+^n/I_+^{n+1}, \end{array}$$

which tells us that all arrows are isomorphism for all $n \geq 2$; so, $\mathcal{J}^n/\mathcal{J}^{n+1} \cong I_+/I_+^{n+1}$ for all $n \geq 0$ (here $I_+^0 := \mathbb{T}_+$ and $\mathcal{J}^0 := R^{ord}$). The filtrations $\{\mathcal{J}^n\}_n$ of R^{ord} and $\{I_+^n\}_n$ are separated and exhaustive, the graded rings $\mathrm{gr}_{\mathcal{J}}(R^{ord})$ is isomorphic to $\mathrm{gr}_{I_+}\mathbb{T}_+$; so, $R^{ord} \cong \mathbb{T}_+$ by [BCM, IV.2.8, Corollaries 1 and 2].

The local complete intersection property follows from Corollary 3.7 (1) which shows that $\mathbb{T}_+$ is a local complete intersection over Λ. □

Remark 7.5. We can prove also in an automorphic way that the p-adically cuspidal Hecke algebra $\mathbb{T}_F$ has reducible locus $\mathbb{T}_F/I_+$ as in the proof of the above theorem. Here is a brief sketch of the argument, assuming for simplicity that $\mathfrak{c}$ is a split prime $\mathfrak{q}$ and F has strict class number 1. Thus the level $N = N(\mathfrak{c})$ is a rational prime q. Let $\phi : Cl_F^+(\mathfrak{q}\mathfrak{p}^\infty) \to \overline{\mathbb{Q}}^\times$ be a deformation of φ. Write $\mathfrak{p}^r$ for the $\mathfrak{p}$-conductor of ϕ. Consider a Hilbert modular base change $\widehat{\theta}(\phi)$ of $\theta(\phi)$, which has Neben type character $(1, \phi\phi_\varsigma, \phi\phi_\varsigma)$ and level Np^r of Hodge weight $\kappa = (0,0)$ in the sense of [HMI, §2.3.2]. The form $\widehat{\theta}(\phi)$ has eigenvalue $\phi(\mathfrak{l}) + \phi(\mathfrak{l}^\varsigma)$ for $T(\mathfrak{l})$ for all primes $\mathfrak{l}$; so, it is an Eisenstein series

$E := E(\phi, \phi_\varsigma)$, where if $\mathfrak{l}|Np^r$, we wrote $T(\mathfrak{l})$ for $U(\mathfrak{l})$. The $\mathfrak{q}$-component of $\phi\phi_\varsigma$ is equal to $\varphi_\mathfrak{q}$ if $\mathfrak{l} = \mathfrak{q}$. Let $f = f(\phi)$ be a p-ordinary stabilization of E so that $f|U(\mathfrak{l}) = \phi(\mathfrak{p}^\varsigma)f$ for $\mathfrak{l} = \mathfrak{p}, \mathfrak{p}^\varsigma$. We claim that f is p-adically cuspidal without using p-adic technique. Let $M_1(Np^r, \phi\phi_\varsigma)$ be the space of Hilbert modular forms of Neben type character $(1, \phi\phi_\varsigma, \phi\phi_\varsigma)$, level Np^r and of Hodge weight $\kappa = (0, 0)$. A local involution $w = w_\mathfrak{q}$ coming from $\tau = \left(\begin{smallmatrix} 0 & -1 \\ \varpi & 0 \end{smallmatrix}\right) \in \mathrm{GL}_2(F_\mathfrak{q})$ for a totally positive generator ϖ of $\mathfrak{q}$ is defined on adelic forms by $g|w(x) := g(x) \mapsto \varphi(\det(x))g(x\tau)$ for $g \in M_1(Np^r, \phi\phi_\varsigma)$. Then, in the same manner as in [MFM, (4.6.22-23)], we have a commutative diagram

$$\begin{array}{ccc} M_1(Np^r, \phi\phi_\varsigma) & \xrightarrow[\sim]{w} & M_1(Np^r, \varphi^{-2}\phi\phi_\varsigma) \\ {\scriptstyle T(\mathfrak{l})}\downarrow & & \downarrow{\scriptstyle \varphi^{-1}(\mathfrak{l})T(\mathfrak{l})} \\ M_1(Np^r, \phi\phi_\varsigma) & \xrightarrow[\sim]{w} & M_1(Np^r, \varphi^{-2}\phi\phi_\varsigma) \end{array}$$

for primes $\mathfrak{l} \neq \mathfrak{q}$. Thus $E|w$ is proportional to $E' := E(\varphi^{-1}\phi, \varphi^{-1}\phi_\varsigma)$. If $\varphi^{-1}\phi$ is non-trivial, E' does not have constant term at ∞, and hence E does not have constant term at $w(\infty)$. Thus we may assume that $\phi = \varphi$. Since w commutes with $\mathfrak{p}$-stabilization and $f|U(\mathfrak{p}) = \varphi(\mathfrak{p}^\varsigma)f$, we find $f|w|T(\mathfrak{p}) = \varphi^{-1}\varphi_\varsigma(\mathfrak{p})f|w$, and hence the constant term of f is proportional to the constant term of the $\mathfrak{p}$-stabilization $E' - E'(\varpi z)$ (having $U(\mathfrak{p})$-eigenvalue $\varphi^{-1}\varphi_\varsigma(\mathfrak{p})$), writing z for the Hilbert modular variable. Thus, even if $\phi = \varphi$, f does not have constant term at $w(\infty)$. The same argument replacing $\mathfrak{q}$ by $\mathfrak{q}^\varsigma$ tells us that $f(\phi)$ does not have constant term at (p-adically) unramified cusps. Therefore the local ring of the cuspidal big Hecke algebra acting non-trivially on $f(\phi)$ (for all such ϕ) is the cuspidal Hecke algebra $\mathbb{T}_F$, and we note that I_+ is given by the annihilator of $\{f(\phi)\}_\phi$ in $\mathbb{T}_F$.

Remark 7.6. We keep the notation and assumptions of the previous remark. We assume $\mathfrak{c} + \mathfrak{c}^\varsigma = O$. Consider the universal character $\boldsymbol{\kappa} : \mathrm{Gal}(F\mathbb{Q}_\infty/F) \to \Lambda^\times$ unramified outside p deforming the identity character. Thus $\boldsymbol{\kappa}([l, \mathbb{Q}]) = t^{\log_p(l)/\log_p(\gamma)}$ for $\gamma = 1 + p$ for a prime $l \neq p$. Here $\mathbb{Q}_\infty/\mathbb{Q}$ is the cyclotomic $\mathbb{Z}_p$-extension. For $(\eta, \xi) = (\phi, \phi_\varsigma)$ or (ϕ_ς, ϕ) as an ordered pair, we can think of a Λ-adic Eisenstein series $E(\eta, \xi\boldsymbol{\kappa})$ whose Λ-adic eigenvalue for $T(\mathfrak{l})$ is given by $\eta(\mathfrak{l}) + \xi(\mathfrak{l}^\varsigma)\boldsymbol{\kappa}(\mathrm{Frob}_\mathfrak{l})$ for primes outside $N(\mathfrak{c})$. Then weight $(0, k-1)$ specialization $E_k(\eta, \xi\boldsymbol{\kappa}_{k-1})$ for $k > 1$ of $E(\eta, \xi\boldsymbol{\kappa})$ is not cuspidal, where $\boldsymbol{\kappa}_{k-1} = \boldsymbol{\kappa} \mod (t - \gamma^{k-1})$. Indeed, w as in Remark 7.5 essentially interchanges $E_k(\eta, \xi\boldsymbol{\kappa}_k)$ and $E_k(\xi, \eta\boldsymbol{\kappa}_k)$ and the argument proving cuspidality for $k = 1$ fails. Note that $E_1(\phi, \phi_\varsigma\boldsymbol{\kappa}_0)$, $E_1(\phi_\varsigma, \phi\boldsymbol{\kappa}_0)$ and $\widehat{\theta}(\phi)$ have the same $T(\mathfrak{l})$-eigenvalues of $T(\mathfrak{l})$ for $\mathfrak{l} \nmid N(\mathfrak{c})p$, but the following $U(\mathfrak{q})$ and $U(\mathfrak{q}^\varsigma)$ eigenvalues for primes $\mathfrak{q}|\mathfrak{c}$, $\mathfrak{p}$ and $\mathfrak{p}^\varsigma$:

	$E_1(\phi, \phi_\varsigma\boldsymbol{\kappa}_0)$	$E_1(\phi_\varsigma, \phi\boldsymbol{\kappa}_0)$	$\widehat{\theta}(\phi)$
$U(\mathfrak{q})$	$\phi(\mathfrak{q}) = 0$	$\phi_\varsigma(\mathfrak{q}) \neq 0$	$\phi_\varsigma(\mathfrak{q}) \neq 0$
$U(\mathfrak{q}^\varsigma)$	$\phi(\mathfrak{q}^\varsigma) \neq 0$	$\phi(\mathfrak{q}) = 0$	$\phi_\varsigma(\mathfrak{q}) \neq 0$
$U(\mathfrak{p})$	$\phi(\mathfrak{p})$	$\phi_\varsigma(\mathfrak{p}) \neq 0$	$\phi_\varsigma(\mathfrak{p}) \neq 0$
$U(\mathfrak{p}^\varsigma)$	$\phi(\mathfrak{p}^\varsigma) \neq 0$	$\phi(\mathfrak{p})$	$\phi_\varsigma(\mathfrak{p}) \neq 0$

Assuming the conductor of ϕ is prime to $\mathfrak{p}$, $f = E_1(\phi, \phi_\varsigma\boldsymbol{\kappa}_0), E_1(\phi_\varsigma, \phi\boldsymbol{\kappa}_0)$ and $\widehat{\theta}(\phi)$ lifts to three Λ-adic forms of prime-to-p level $N(\mathfrak{c})$ and Neben character $(1, \phi\phi_\varsigma, \phi\phi_\varsigma)$ given by two Eisenstein families $E(\phi, \phi_\varsigma\boldsymbol{\kappa})$ and $E(\phi_\varsigma, \phi\boldsymbol{\kappa})$ and a unique cuspidal family θ associated to $\mathbb{T}_F$ under $p \nmid h_{F(\varphi^-)}$, and they never intersect over $\mathrm{Spec}(\Lambda)$ by (H0). However these families at weight 1 points have same eigenvalues for $T(\mathfrak{l})$ for primes $\mathfrak{l}$ outside $N(\mathfrak{c})p$. This is not contradictory to Wiles' proof of Iwasawa's main conjecture [Wi90], because our ordinarity is different from the one Wiles used as described in Section 5.4. Note that the two Eisenstein families $E(\phi, \phi_\varsigma\boldsymbol{\kappa})$ and $E(\phi_\varsigma, \phi\boldsymbol{\kappa})$ interchange under the action of $\mathrm{Gal}(F/\mathbb{Q})$ switching two variables of Hilbert modular forms indexed by archimedean places of F, but the local ring $\mathbb{T}_F$ carrying the family θ is invariant under $\mathrm{Gal}(F/\mathbb{Q})$ as it is the base-change from $\mathbb{Q}$.

8. Modularity of the universal ordinary Cayley–Hamilton representation

We now give an explicit form of the universal ordinary Cayley–Hamilton representation. This supplies us with an explicit matrix form of the inertia subgroup at p of $\mathrm{Im}(\rho_\mathbb{T})$ which is a key step towards the proof of Theorems C and D. Since we already know $R^{ord} \cong \mathbb{T}_+$ by Theorem 7.4, we show that $\rho_\mathbb{T}|_H$ normalized as in Lemma 7.3 gives the universal Cayley–Hamilton representation.

Theorem 8.1. *Assume* (H0–2). *We have* $E^{ord} = \begin{pmatrix} \mathbb{T}_+ & B_+ \\ C_+ & \mathbb{T}_+ \end{pmatrix} \cong \begin{pmatrix} \mathbb{T}_+ & \mathbb{T}_- \\ \mathbb{T}_- & \mathbb{T}_+ \end{pmatrix} =: E_+$ *with* $B_+ \otimes_{\mathbb{T}_+} C_+ \cong \mathbb{T}_- \otimes_{\mathbb{T}_+} \mathbb{T}_- \to \mathbb{T}_+$ *given by* $\Theta b \otimes \Theta c \mapsto \Theta^2 bc$ *(the product in* $\mathbb{T}$*), and* $\rho_{\mathbb{T}}|_H : H \to E_+$ *as chosen in* Lemma 7.3 *gives the universal ordinary Cayley–Hamilton representation.*

Proof. By Lemma 7.3, $\rho_{\mathbb{T}}|_H$ suitably conjugated in $\mathrm{GL}_2(\mathbb{T})$ has values in $E_+ = \begin{pmatrix} \mathbb{T}_+ & \mathbb{T}_- \\ \mathbb{T}_- & \mathbb{T}_+ \end{pmatrix}$. By Theorem 7.4, $R^{ord} \cong \mathbb{T}_+$, and E^{ord} is a $\mathbb{T}_+$-GMA. Therefore we can write $E^{ord} = \begin{pmatrix} \mathbb{T}_+ & B_+ \\ C_+ & \mathbb{T}_+ \end{pmatrix}$ with $\mathbb{T}_+$-modules B_+ and C_+. We know $\mathcal{J} = \Theta_+\mathbb{T}_+$ for $\Theta_+ = \Theta^2$. The universal $\mathbb{T}_+$-GMA morphism $\phi : (E^{ord}, \boldsymbol{\rho}^{ord}) \to (E_+, \rho_{\mathbb{T}}|_H)$ induces $\mathbb{T}_+$-linear morphisms $\phi_B : B_+ \to \mathbb{T}_-$ and $\phi_C : C_+ \to \mathbb{T}_-$. Since we have the isomorphism $i : E^{ord} \otimes_{R^{ord}} R^{red} \cong E^{red}$ by Lemma 6.3, the morphism $\phi_? \otimes 1 : ?^{red} = ?_+ \otimes_{R^{ord}} R^{red} \to \mathbb{T}_-/\Theta_+\mathbb{T}_-$ $(? = B, C)$ is induced by this canonical isomorphism i. The result [FGS, Theorem 1.5.5] is valid for any Cayley–Hamilton representation not necessarily the universal E^{red}. Applying this theorem of Bellaïsche–Chenevier to E_+/Θ_+E_+, replacing B^{red} by $\mathbb{T}_-/\Theta_+\mathbb{T}_- = \mathbb{T}_-/\mathcal{J}\mathbb{T}_-$, we have a morphism in the same manner as in (6.1) and (6.2)

$$j_n : \mathrm{Hom}_{\mathbb{T}_+}(\mathbb{T}_-/\Theta_+\mathbb{T}_-, X_n) \hookrightarrow \mathrm{Hom}_{W[C]}(\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W, X_n(\Phi_-)).$$

Namely, writing $(\boldsymbol{\rho} \mod (\Theta_+)) = (\rho_{ij})$, $j_n(f') = f' \circ \rho_{12} \in \mathrm{Hom}_{W[C]}(\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W, X_n(\Phi_-))$ for $f' \in \mathrm{Hom}_{\mathbb{T}_+}(\mathbb{T}_-/\Theta_+\mathbb{T}_-, X_n)$. Passing to the injective limit (with respect to n), we get as in (6.3) a $W[C]$-linear injection $j_\infty : (\mathbb{T}_-/\Theta_+\mathbb{T}_-)^\vee \hookrightarrow (\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W)^\vee$. Taking the dual, we get the surjective bottom horizontal morphism in the following commutative digram:

$$\begin{array}{ccc} \mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W & \xrightarrow[\iota_\infty^\vee]{\sim} & B^{red} \\ \| \downarrow & & \downarrow \phi_B \otimes 1 \\ \mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W & \xrightarrow[j_\infty^\vee]{\twoheadrightarrow} & \mathbb{T}_-/\Theta_+\mathbb{T}_-. \end{array}$$

The commutativity of this diagram follows since ϕ_B is compatible with the construction of ι_n and j_n by universality (i.e., $j_n(f') = f' \circ \rho_{12} = f' \circ (\phi_B \otimes 1) \circ \rho_{12}^{red} = \iota_n(f' \circ (\phi_B \otimes 1))$). Thus ϕ_B is a onto $W[C]$-linear morphism:

$$W[C] \overset{(*)}{\cong} \mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W \twoheadrightarrow \mathbb{T}_-/\Theta_+\mathbb{T}_- = \Theta\mathbb{T}_+/\Theta_+\Theta\mathbb{T}_+ \cong W[C],$$

where the identity $(*)$ follows from Theorem 3.9. Comparing the W-rank, surjectivity implies an isomorphism

$$\phi_B \otimes 1 : \mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W \cong \mathbb{T}_-/\Theta_+\mathbb{T}_-$$

of $W[C]$-modules.

Recall the ς-conjugate Galois group $\mathcal{Y}_\varsigma(\varphi_\varsigma^-)$ of $\mathcal{Y}(\varphi^-)$ in Definition 3.8. Replacing $\mathcal{Y}(\varphi^-)$ and B^{red} by $\mathcal{Y}_\varsigma(\varphi_\varsigma^-)$ and C^{red} in the above argument, we conclude that $\phi_C \otimes 1$ is also onto.

Since $B_+/\mathcal{J}B_+ \cong \mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W = \mathbb{T}_-/\Theta_+\mathbb{T}_-$ by Proposition 6.2 and Lemma 6.3, ϕ_B and ϕ_C are surjective by Nakayama's lemma. From $\mathbb{T}_+ \cong \mathbb{T}_-$ $(x \mapsto \Theta x)$ as $\mathbb{T}_+$-modules, $\mathbb{T}_-$ is free of rank 1 over $\mathbb{T}_+$, and therefore ϕ_B and ϕ_C must be $\mathbb{T}_+$-linear isomorphisms. Thus we conclude $E^{ord} = E_+$ and $\boldsymbol{\rho} = \rho_{\mathbb{T}}|_H$, as desired. □

Normalize $\rho_{\mathbb{T}}$ such that $\rho_{\mathbb{T}}|_H$ has values in $\begin{pmatrix} \mathbb{T}_+ & \mathbb{T}_- \\ \mathbb{T}_- & \mathbb{T}_+ \end{pmatrix}$, and write simply $\boldsymbol{\rho}$ for the Cayley–Hamilton representation $\rho_{\mathbb{T}}|_H$ which is isomorphic to $\boldsymbol{\rho}^{ord}$.

9. Local Iwasawa theory

Let $k/\mathbb{Q}_p$ (inside $\overline{\mathbb{Q}}_p$) be a Galois extension with $p \nmid [k : \mathbb{Q}_p] < \infty$. Write F_∞/k for the cyclotomic $\mathbb{Z}_p$-extension inside $\overline{\mathbb{Q}}_p$. Let $\Gamma := \mathrm{Gal}(F_\infty/k) = \gamma^{\mathbb{Z}_p}$ and put $\Gamma_n = \Gamma^{p^n}$. Set $F_n := F_\infty^{\Gamma_n}$ and write $\mathfrak{o}_n$ for the p-adic integer ring of F_n. Let L (resp. L_n) be the maximal abelian p-extension of F_∞ (resp. F_n). Write $X_n := \mathrm{Gal}(L_n/k_n)$ and $X := \mathrm{Gal}(L/F_\infty)$. We have $\mathrm{Gal}(L/\mathbb{Q}_p) = \mathrm{Gal}(F_\infty/\mathbb{Q}_p) \ltimes X$, and Γ (resp. $\mathrm{Gal}(F_\infty/\mathbb{Q}_p)$) acts on X by conjugation. Therefore the commutator subgroup of $\mathrm{Gal}(L/k_n)$ is given by $(\gamma^{p^n} - 1)X$, and we have the corresponding exact sequence at each level n: $1 \to X/(\gamma^{p^n} - 1)X \to \mathrm{Gal}(L_nF_\infty/F_\infty) \to \Gamma_n \to 1$.

Let k_∞/k be the unramified $\mathbb{Z}_p$-extension inside $\overline{\mathbb{Q}}_p$ with its n-th layer k_n, and put $\Upsilon := \mathrm{Gal}(k_\infty/k)$ and $\mathcal{F}_n := F_\infty k_n$. Let $\mathcal{L}$ (resp. $\mathcal{L}_n$) be the maximal abelian p-extension of $\mathcal{F}_\infty$

(resp. $\mathcal{F}_n$). Set $\mathcal{X} := \mathrm{Gal}(\mathcal{L}/\mathcal{F}_\infty)$. Pick a lift $\phi \in \mathrm{Gal}(\mathcal{L}/k)$ of the Frobenius element $[p, \mathbb{Q}_p]^f$ (for the residual degree f of $k/\mathbb{Q}_p$) generating $\mathrm{Gal}(k_\infty F_\infty/F_\infty)$ and a lift $\widetilde{\gamma} \in \mathrm{Gal}(\mathcal{L}/k)$ of the generator γ of $\mathrm{Gal}(F_\infty/k) = \Gamma$. The commutator $\tau := [\phi, \widetilde{\gamma}]$ acts on $\mathcal{X}$ by conjugation, and $(\tau - 1)x := [\tau, x] = \tau x \tau^{-1} x^{-1}$ for $x \in \mathcal{X}$ is uniquely determined independent of the choice of $\widetilde{\gamma}$ and ϕ. Define $L' \subset \mathcal{L}$ and $L'_n \subset \mathcal{L}_n$ by the fixed field of $(\tau - 1)\mathcal{X}$, which is independent of the choice of $\widetilde{\gamma}$ and ϕ. Let $X' = \mathrm{Gal}(L'/\mathcal{F}_\infty)$ and $X'_n = \mathrm{Gal}(L'_n/\mathcal{F}_n)$. Since $p \nmid [k : \mathbb{Q}_p]$, we can split $\mathrm{Gal}(\mathcal{F}_\infty/\mathbb{Q}_p) = \mathrm{Gal}(k/\mathbb{Q}_p) \ltimes \mathrm{Gal}(\mathcal{F}_\infty/k)$, and regard X' as a $\mathbb{Z}_p[\mathrm{Gal}(k/\mathbb{Q}_p)]$-module through the conjugation action of $\mathrm{Gal}(k/\mathbb{Q}_p) \subset \mathrm{Gal}(\mathcal{F}_\infty/k)$. We quote the following result from [EMI, §1.12.2] and [H21, Proposition A.4.1 (3)]:

Proposition 9.1. *Let $\eta : \mathrm{Gal}(k/\mathbb{Q}_p) \to \mathbb{Z}_p[\eta]^\times$ be a character. Write $\mathbb{Z}_p(\eta)$ for the a free $\mathbb{Z}[\eta]$-module of rank 1 on which $\mathrm{Gal}(k/\mathbb{Q}_p)$ acts by η. Then the η-isotypic component $X'[\eta] = X' \otimes_{\mathbb{Z}_p[\mathrm{Gal}(k/\mathbb{Q}_p)]} \mathbb{Z}_p(\eta)$ is a cyclic $\mathbb{Z}_p[\eta][[\Gamma \times \Upsilon]]$-module (i.e., it is generated topologically over $\mathbb{Z}_p[\eta][[\Gamma \times \Upsilon]]$ by one element).*

10. Explicit form of p-inertia group, proof of Theorem D

Recall $\boldsymbol{\rho} = \rho_{\mathbb{T}}|_H$ normalized as in Lemma 7.3. Pick a prime $\wp|\mathfrak{p}$ of $F(\boldsymbol{\rho})$. Let $\overline{I}_{\mathfrak{p}}$ (resp. $\overline{I}_{\mathfrak{p}^\varsigma}$, $\overline{D}_{\mathfrak{p}}$) be the $\mathfrak{p}$-inertia (resp. $\mathfrak{p}^\varsigma$-inertia, $\mathfrak{p}$-decomposition) subgroup of $H_p := \mathrm{Gal}(F(\boldsymbol{\rho})/F(\overline{\rho}))$ corresponding to $\wp$ and $\wp^\varsigma$. We choose $\boldsymbol{\rho}$ so that $\boldsymbol{\rho}(\overline{D}_{\mathfrak{p}})$ is upper triangular with unramified quotient character $\boldsymbol{\delta}$. Regard $[p, \mathbb{Q}_p]^f \in \overline{D}_{\mathfrak{p}}$ for the residual degree f of $\mathfrak{P} = \wp \cap F(\overline{\rho})$, and write $\boldsymbol{\rho}([p, \mathbb{Q}_p]^f) = \begin{pmatrix} u^{-f} & * \\ 0 & u^f \end{pmatrix}$ with $u = \boldsymbol{\delta}([p, \mathbb{Q}_p]) \in \mathbb{T}_+^\times$. Let $\mathbb{F}_1$ be the subfield of $\mathbb{F}$ generated by the values of $\overline{\varphi}$ over D_p and $W_1 = W(\mathbb{F}_1)$ (the Witt vector ring with coefficients in $\mathbb{F}_1$). Put $\Lambda_0 := \mathbb{Z}_p[[T]] \subset \Lambda_1 := W_1[[T, a]] \subset \mathbb{T}$ for $a = u^{2f} - 1$ ($u = \boldsymbol{\delta}([p, \mathbb{Q}_p])$). Note $u^f - 1 \in \mathfrak{m}_{\mathbb{T}}$; so, the symbol $W_1[[T, a]]$ makes sense and it is the closed subalgebra of $\mathbb{T}$ generated by T and a over W_1. Recall the subgroup $\Delta \subset H$ with $\Delta \cong \mathrm{Gal}(F(\overline{\rho})/F)$ defined in §5.1.

Theorem 10.1. *Let the notation be as above. Suppose* (H0). *Then by conjugating $\boldsymbol{\rho}$ by a diagonal element in $E_+^\times$, we can choose a non-zero divisor θ satisfying $\theta^\sigma = -\theta$ so that we have*

$$\boldsymbol{\rho}(\overline{I}_{\mathfrak{p}}) = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix} \right) \middle| a \in t^{\mathbb{Z}_p}, b \in \theta\Lambda_1 \right\} \quad (t = 1 + T)$$

and $\boldsymbol{\rho}(\overline{I}_{\mathfrak{p}^\varsigma}) = J\boldsymbol{\rho}(\overline{I}_{\mathfrak{p}})J^{-1}$, where $J = \boldsymbol{\rho}(\varsigma) = \begin{pmatrix} 0 & \varphi(\varsigma^2) \\ 1 & 0 \end{pmatrix}$. If further we assume (H0–2), *replacing θ by $a\theta$ for a unit $a \in \mathbb{T}_+^\times$ by conjugating $\boldsymbol{\rho}$ by $\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix} \right)$, we may choose θ to be a generator of $\mathbb{T}$ over $\mathbb{T}_+$ with $\sigma(\theta) = -\theta$; in other words, we have $a\theta = \Theta$ for Θ as in* Theorem 3.4.

Replacing φ by the Teichmüller lift of $\overline{\varphi}$, we assume that φ has order prime to p in the proof.

Proof. From the definition of Λ-algebra structure of $\mathbb{T}$ and p-ordinarity, we know

$$\boldsymbol{\rho}(\overline{I}_{\mathfrak{p}}) \subset M(\mathbb{T}) \cap E^{ord} \quad \text{and} \quad \boldsymbol{\rho}(\overline{I}_{\mathfrak{p}^\varsigma}) = J\boldsymbol{\rho}(I_{\mathfrak{p}})J^{-1}$$

for the mirabolic subgroup $M(\mathbb{T}) := \left\{ \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix} \right) \middle| a \in \mathbb{T}^\times, b \in \mathbb{T} \right\}$. Since $\mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) = [p, \mathbb{Q}_p]^{\widehat{\mathbb{Z}}} \ltimes \mathbb{Z}_p^\times$ for the maximal abelian extension $\mathbb{Q}^{ab}/\mathbb{Q}$ and the local Artin symbol $[p, \mathbb{Q}_p]$, we find

$$\boldsymbol{\rho}(\overline{I}_{\mathfrak{p}}) \subset \left\{ \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix} \right) \middle| a \in t^{\mathbb{Z}_p}, b \in \mathbb{T}_- \right\}$$

by the shape of E^{ord}, and $\det(\boldsymbol{\rho}(\overline{I}_{\mathfrak{p}})) = t^{\mathbb{Z}_p} \subset \Lambda_0^\times$. Thus we have an extension $1 \to \mathcal{U} \to \boldsymbol{\rho}(\overline{I}_{\mathfrak{p}}) \to t^{\mathbb{Z}_p} \to 1$. Recall the element ϕ_0 we fixed to normalize Wiles' pseudo representation (see (W2)). By [H15, Lemma 1.4], this extension canonically split by the action of the element $\phi_0 \in \Delta$ with $\mathcal{U}$ characterized to be an eigenspace on which ϕ_0 acts by φ^- (or $c \in \Delta$ acts by $\varphi^-(c) = -1$); so, we may assume to have a section $s : t^{\mathbb{Z}_p} \hookrightarrow \boldsymbol{\rho}(\overline{I}_{\mathfrak{p}})$ identifying $t^{\mathbb{Z}_p}$ with $\left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix} \right) \middle| a \in t^{\mathbb{Z}_p} \right\}$. Thus $\mathcal{U}$ is made of unipotent matrices. Here we used the assumption (H0). Defining

$$I_1 = \{\tau \in \overline{I}_{\mathfrak{p}} : \tau|_K = 1\}$$

for the unique $\mathbb{Z}_p$-subextension $K/F(\overline{\varphi}^-)_{\mathfrak{P}}$ of $F(\overline{\varphi}^-)_{\mathfrak{P}}[\mu_{p^\infty}]$, we have $\mathcal{U} = \boldsymbol{\rho}(I_1)$, since $\mathcal{U}$ is made of unipotent matrices, .

Regard $\mathcal{U}$ as an additive submodule inside $\mathbb{T}_-$ and φ^- as an abelian irreducible $\mathbb{Z}_p$-representation acting on $W = \mathbb{Z}_p[\varphi]$ regarded as a $\mathbb{Z}_p$-module. Apply Proposition 9.1 to the splitting field k of $\varphi^-|_{D_p}$ under the notation there. Then the Galois group $X'[\varphi^-]$ is cyclic over $W_1[[\Gamma \times \Upsilon]]$ ($\Gamma = t^{\mathbb{Z}_p}$) and surjects onto $\mathcal{U}$. Since the action of $W_1[[\Gamma \times \Upsilon]]$ factors through Λ_1, by Proposition 9.1, $\mathcal{U}$ is cyclic over Λ_1. Since $\mathbb{T}$ is Λ_1-torsion-free, we have $\mathcal{U} \cong \Lambda_1$ as long as $\mathcal{U} \neq 0$. Thus we conclude $\boldsymbol{\rho}(I_1) = \mathcal{U} = \left\{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \middle| a \in \theta\Lambda_1\right\}$ inside $\boldsymbol{\rho}(H)$ (for a suitable choice of $\theta \in \mathbb{T}_-$ by Lemma 7.3).

In [Z14], indecomposability over the p-inertia group of a Hilbert modular Galois representation (over a totally real field K) attached to a weight 2 non-CM cusp form is proven unconditionally if $2 \nmid [K : \mathbb{Q}]$. Since $\boldsymbol{\rho} = \rho_{\mathbb{T}}|_H$ and $I_p \subset H$, we can apply the result of [Z14] to modular specializations of $\boldsymbol{\rho}$ (i.e., $K = \mathbb{Q}$ not F). Thus taking a weight 2 elliptic Hecke eigenform g belonging to a given irreducible non CM component Spec($\mathbb{I}$) of Spec($\mathbb{T}$), the Galois representation ρ_g of g is indecomposable over $\overline{I}_{\mathfrak{p}}$; so, $\mathcal{U} \otimes_{\Lambda_1} \mathbb{I} \neq 0$. This shows the image of θ in $\mathbb{I}$ is non-zero. While if $\mathbb{I}$ is a CM component, then the image of θ vanishes in $\mathbb{I}$ as $\pi \circ \rho_{\mathbb{T}}$ for $\pi : \mathbb{T} \to \mathbb{I}$ is an induced representation. By minimality (i.e., N is the prime-to-p-conductor of $\overline{\rho}$), $\mathbb{T}$ is reduced by Lemma 2.1. Since Spec($\mathbb{T}$) does not have any CM irreducible components (as explained just below Theorem D), θ is a non-zero divisor of $\mathbb{T}$. This shows the desired expression for $\boldsymbol{\rho}(\overline{I}_{\mathfrak{p}})$. Since $\boldsymbol{\rho}(\overline{I}_{\mathfrak{p}^{\varsigma}}) = J\boldsymbol{\rho}(\overline{I}_{\mathfrak{p}})J^{-1}$, we obtain the expression of $\boldsymbol{\rho}(\overline{I}_{\mathfrak{p}^{\varsigma}})$.

We now assume (H1–2) in addition to (H0). If the $\mathbb{T}_+$-span $\mathbb{T}_+ \cdot \mathcal{U}$ of $\mathcal{U}$ is smaller than $\mathbb{T}_- = \Theta\mathbb{T}_+$, we have $\mathcal{U}\mathbb{T}_+ \subset \Theta\mathfrak{m}_+\mathbb{T}_+ = \mathfrak{m}_+\mathbb{T}_-$ for the maximal ideal $\mathfrak{m}_+$ of $\mathbb{T}_+$ as $\mathbb{T}_-$ is free of rank 1 over $\mathbb{T}_+$. Let $F(\varphi^-)_{\mathfrak{P}}$ be the completion at $\mathfrak{P} = \wp \cap F(\varphi^-)$. Recall $\mathcal{U} = \boldsymbol{\rho}(I_1)$. Thus we may write $\boldsymbol{\rho}(\tau) = \left(\begin{smallmatrix} 1 & u(\tau) \\ 0 & 1 \end{smallmatrix}\right)$ for $\tau \in I_1$. Let $\overline{u} := u \mod \mathfrak{m}_+\mathbb{T}_-$ which has values in $\mathbb{T}_-/\mathfrak{m}_+\mathbb{T}_- \cong \mathbb{F}$. Let $H(\varphi^-) := \mathrm{Ker}(\varphi^- : H \to W^\times)$. Since $\mathbb{T}_-/\Theta\mathbb{T}_- = \mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W$ and $\Theta^2\mathbb{T}_+$ defines the reducible locus of $\boldsymbol{\rho}$ by Proposition 6.2, this homomorphism extends to a non-zero homomorphism $\overline{u} : H(\varphi^-) \to \mathbb{F}$ with $\overline{u}(\tau h \tau^{-1}) = \overline{\varphi}^-(\tau)\overline{u}(h)$ (for $\tau \in H$) unramified outside $\mathfrak{p}$ over $F(\varphi^-) = F(\overline{\rho})$. Since $F(\overline{\rho})^{(p)}/F(\overline{\rho})$ only ramifies at p, $\overline{u}$ is unramified at $\mathfrak{c}\mathfrak{c}^{\varsigma}$. Since $\boldsymbol{\rho}(\overline{I}_{\mathfrak{p}^{\varsigma}})$ is lower triangular contained in $jM(\mathbb{T})j^{-1}$, $\overline{u}$ is unramified everywhere. Since $Cl_{F(\varphi^-)} \otimes_{\mathbb{Z}_p[\Delta]} \overline{\varphi}^- = 0$ by (H2), this is a contradiction as $\overline{u} \neq 0$ on $H(\varphi^-)$. Thus $\mathbb{T}_+$-span of $\overline{u}(I_1)$ is $\mathbb{F}$; so, $\mathbb{T}_+$-span of $u(I_1)$ is equal to $\mathbb{T}_-$ by Nakayama's lemma. Thus $\mathbb{T}_+u(I_1) \not\equiv 0 \mod \mathfrak{m}_+\mathbb{T}_-$; so, we may assume that $\Theta \in u(I_1)$ and hence $\theta = \Theta$. □

Proposition 10.2. *Assume* (H0–1). *Recall the universal character $\Phi : H \to W[C]^\times$. Let $L := F(\Phi^-)$ and $W(\varphi^-)$ be the rank one W-free module on which Δ acts by φ^-. Then we have a $W[C]$-linear surjection: $Cl_L \otimes_{\mathbb{Z}[\Delta]} W(\varphi^-) \twoheadrightarrow \mathbb{T}_-/(\theta\mathbb{T}_+ + I_+\mathbb{T}_-)$; so, $\mathbb{T}_-/(\theta\mathbb{T}_+ + I_+\mathbb{T}_-)$ is finite.*

Proof. Write $\overline{\theta}$ for the image of $\theta \in \mathbb{T}_-$ in $\mathbb{T}_-/I_+\mathbb{T}_-$. Since $\mathbb{T}_-$ is a $\mathbb{T}_+$-module and $\mathbb{T}_+/I_+ \cong W[C]$ (Lemma 3.1), we can think of $W[C]\overline{\theta} \subset \mathbb{T}_-/I_+\mathbb{T}_-$. The pull back by $\mathbb{T}_- \twoheadrightarrow \mathbb{T}_-/I_+\mathbb{T}_-$ of $W[C]\overline{\theta}$ to $\mathbb{T}_-$ is equal to $\theta\mathbb{T}_+ + I_+\mathbb{T}_-$. By conjugation action, $\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W$ is a $W[C]$-module. Note that $\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W$ is the upper nilpotent part B^{red} of the universal reducible Cayley-Hamilton representation, and $R^{ord}/\mathcal{J}R^{ord} = \mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi^-]} W$ by Proposition 6.2 and Lemma 6.3. Let I_0 be the wild inertia subgroup at $\mathfrak{p}$ in $\mathrm{Gal}(F(\boldsymbol{\rho})/F(\overline{\rho}))$. As in the proof of Theorem 10.1, we have an exact sequence $0 \to \mathcal{U}_0 \to I_0 \twoheadrightarrow \Gamma \to 1$ for the Galois group Γ of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$. Lift $c \in C = \mathrm{Gal}(F(\Phi)/F(\varphi))$ to $\widetilde{c} \in \mathrm{Gal}(F(\boldsymbol{\rho})/F(\varphi))$ so that $\boldsymbol{\rho}(\widetilde{c})$ is upper triangular. This is possible by the form of the universal Cayley–Hamilton representation studied in Section 6. We let $\widetilde{c}$ act on I_0 and its unipotent part $\mathcal{U}_0$ by conjugation. The $W[C]$-module structure (through the identification $W[C] = \mathbb{T}_+/I_+$) of $\mathbb{T}_-/I_+\mathbb{T}_-$ is induced by the conjugation action of $\widetilde{c}$ on the inertia groups, $\widetilde{c}I_0\widetilde{c}^{-1}$ and $\widetilde{c}\mathcal{U}_0\widetilde{c}^{-1}$ only depends on $c \in C$; so, we write them as cX for $X = I_0, I_1$ and $\mathcal{U}_0, \mathcal{U}$. Note that $c\overline{\theta}$ is the image of a generator (over Λ_1) of the unipotent part $c\mathcal{U}$. Write $\overline{\mathcal{U}}_0$ for the image of $\mathcal{U}_0$ in $\mathcal{Y}(\varphi^-)$. Consider the quotient $\mathcal{C} := (\mathcal{Y}(\varphi^-) \otimes_{\mathbb{Z}_p[\varphi_-]} W)/W[C]\mathcal{U}_0$ for $W[C]$-span $W[C]\mathcal{U}_0$ of $\overline{\mathcal{U}}_0$. Then $\mathcal{C}$ is the scalar extension to W of the Galois group of the maximal p-abelian extension unramified everywhere of $L = F(\Phi^-)$ on which Δ acts by φ^-, that is, $Cl_L \otimes_{\mathbb{Z}[\Delta]} \varphi^-$. Therefore we conclude $\mathcal{C} = Cl_L \otimes_{\mathbb{Z}[\Delta]} \varphi^-$ which is finite. Since $W[C]\overline{\mathcal{U}}_0$ has image $(W[C]\overline{\theta} + I_+\mathbb{T}_-)/I_+\mathbb{T}_- = (\theta\mathbb{T}_+ + I_+\mathbb{T}_-)/I_+\mathbb{T}_-$ in $\mathbb{T}_-/I_+\mathbb{T}_-$, $\mathcal{C}$ surjects down to $\mathbb{T}_-/(\theta\mathbb{T}_+ + I_+\mathbb{T}_-)$, and therefore $\mathbb{T}_-/(\theta\mathbb{T}_+ + I_+\mathbb{T}_-)$ is finite. □

Corollary 10.3. *Assume* (H0–1). *Then we have $\theta\mathbb{T} \cap \Lambda = (\langle\varepsilon\rangle - 1)$.*

Proof. By Lemma 3.1, $\theta\mathbb{T}_+$ has image $W[C]\overline{\theta}$ in $\mathbb{T}_-/I_+\mathbb{T}-$, and $\mathbb{T}_-/(\theta\mathbb{T}_+ + I_+\mathbb{T}_-)$ is finite by Proposition 10.2. Pick $\lambda \in \Lambda$ such that $\lambda \notin (\langle\varepsilon\rangle - 1)$ and $\Lambda/(\lambda) = W$. Let $X^\lambda := X[\frac{1}{\lambda}] = X \otimes_\Lambda \Lambda[\frac{1}{\lambda}]$ for $X = \mathbb{T}_\pm, I, I_\pm$. By $|\mathbb{T}_-/(\theta\mathbb{T}_+ + I_+\mathbb{T}_-)| < \infty$, we have $\mathbb{T}_-^\lambda = \theta\mathbb{T}_+^\lambda + I_+\mathbb{T}_-^\lambda$. Suppose $\mathbb{T}_-^\lambda = \theta\mathbb{T}_+^\lambda + I_+^n\mathbb{T}_-^\lambda$ for some $n > 0$. Then

$$\mathbb{T}_-^\lambda = \theta\mathbb{T}_+^\lambda + I_+^n(\theta\mathbb{T}_+^\lambda + I_+\mathbb{T}_-^\lambda) = \theta\mathbb{T}_+^\lambda + I_+^{n+1}\mathbb{T}_-^\lambda.$$

Thus by induction, $\mathbb{T}_-^\lambda = \theta\mathbb{T}_+^\lambda + I_+^n\mathbb{T}_-^\lambda$ for any $n > 0$, and we conclude

$$\mathbb{T}_-^\lambda = \bigcap_n (\theta\mathbb{T}_+^\lambda + I_+^n\mathbb{T}_-^\lambda).$$

Consider $M := \mathbb{T}_-/\theta\mathbb{T}_+$ which is a $\mathbb{T}_+$-module of finite type. Then by Krull's intersection theorem [CRT, Theorem 8.9], $N := \bigcap_{n>0} I_+^n M$ has an element $a \equiv 1 \mod I_+$ such that $aN = 0$. Since I_+ is in the radical $\mathfrak{m}_{\mathbb{T}_+}$, a is a unit in $\mathbb{T}_+$; so, $N = 0$. This shows

$$\bigcap_n (\theta\mathbb{T}_+ + I_+^n\mathbb{T}_-) = \theta\mathbb{T}_+.$$

Since $\Lambda[\frac{1}{\lambda}]$ is Λ-flat, tensoring $\Lambda[\frac{1}{\lambda}]$ over Λ (i.e., localization by inverting λ) commutes with intersection [BCM, I.2.6]; so, we conclude the identity $(*)$ in the following equation:

$$\mathbb{T}_-^\lambda = \bigcap_n (\theta\mathbb{T}_+^\lambda + I_+^n\mathbb{T}_-^\lambda) \overset{(*)}{=} \theta\mathbb{T}_+^\lambda. \tag{10.1}$$

Thus $I^\lambda = I\mathbb{T}^\lambda = (\theta)$. This shows $\theta\mathbb{T}^\lambda \cap \Lambda^\lambda = I^\lambda \cap \Lambda^\lambda = (\langle\varepsilon\rangle - 1)\Lambda^\lambda$ as $\Lambda[\frac{1}{\lambda}]$ is flat over Λ [BCM, I.2.6]. Therefore $(\langle\varepsilon\rangle - 1)/((\theta) \cap \Lambda)$ is a λ-torsion module. We can choose a couple of λs as above, say λ_1, λ_2, so that $(\lambda_1, \lambda_2) = \mathfrak{m}_\Lambda$. Then the Λ-module $(\langle\varepsilon\rangle - 1)/((\theta) \cap \Lambda)$ is λ_j-torsion for $j = 1, 2$ and hence is killed by $\mathfrak{m}_\Lambda^M$ for some $0 \ll M \in \mathbb{Z}$. Since $(\theta) \cap \Lambda$ is a reflexive Λ-module, the Λ-module $(\langle\varepsilon\rangle - 1)/((\theta) \cap \Lambda)$ does not have $\mathfrak{m}_\Lambda$ as an associated prime; so, we conclude $(\langle\varepsilon\rangle - 1)/((\theta) \cap \Lambda) = 0$, as desired. □

For the proof of Theorem 4.1 and Proposition 4.2, what we needed are the following three facts:

(i) $\mathbb{T}' = \Lambda[\Theta]$ (i.e., $\mathbb{T}'$ is generated over Λ by one element).
(ii) $\Theta\mathbb{T}' \cap \Lambda = (\langle\varepsilon\rangle - 1)$ (so, $\Lambda[\Theta]/(\Theta) = (\Lambda + (\Theta))/(\Theta) = \Lambda/(\Lambda \cap (\Theta))$),
(iii) $\mathbb{T}'$ is free of finite rank over Λ,

Since any Λ-torsion-free ring A finite over Λ generated by one element is Λ-free of finite rank, replacing Θ by θ, we can apply the arguments proving Proposition 4.2 to the subalgebra $\Lambda[\theta]$ of $\mathbb{T}$ generated by θ in Proposition 10.2 and obtain the assertion (1)–(5) of the following corollary. The last assertion (6) follows directly from Theorem 10.1:

Corollary 10.4. *Assume* (H0–1). *Let the notation be as in* Proposition 10.2. *Let $\Lambda[\theta]$ be the Λ-subalgebra of $\mathbb{T}$ generated by θ, and put $e_\theta = \mathrm{rank}_\Lambda \Lambda[\theta]$.*

(1) *If $\langle\varepsilon\rangle - 1$ is a prime in Λ, then the ring $\Lambda[\theta]$ is isomorphic to the power series ring $W[[x]]$ of one variable over W; hence, $\Lambda[\theta]$ is a regular local domain and is factorial;*
(2) *The ring $\Lambda[\theta]$ is an integral domain, and for a prime factor P of $\langle\varepsilon\rangle - 1$, the localization $\Lambda[\theta]_P$ of $\Lambda[\theta]$ at P is a discrete valuation ring fully ramified over Λ_P;*
(3) *If p is prime to e_θ, the ramification locus of $\Lambda[\theta]/\Lambda$ is given by* $\mathrm{Spec}(\Lambda/(\langle\varepsilon\rangle - 1))$, *the relative different for $\Lambda[\theta]/\Lambda$ is principal and generated by $\theta^{e_\theta - 1}$ and $\Lambda[\theta]$ is a normal integral domain of dimension 2 unramified outside $(\langle\varepsilon\rangle - 1)$ over Λ;*
(4) *If $p|e_\theta$, $\Lambda[\frac{1}{p}, \theta]$ is a Dedekind domain unramified outside $(\langle\varepsilon\rangle - 1)$ over $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$, and the relative different for $\mathbb{T}[\frac{1}{p}]_{/\Lambda[\frac{1}{p}]}$ is principal and generated by Θ^{e-1};*
(5) *If $e_\theta = 2$, $\Lambda[\theta]$ is a normal integral domain, and one can choose $\theta = \sqrt{1 - \langle\varepsilon\rangle}$;*
(6) *If* (H2) *holds, we have $\theta = \Theta$ up to units in $\mathbb{T}$.*

Proof of Theorem D: By Theorem 10.1, the restriction $\rho_f|_{I_\mathfrak{p}}$ is decomposable if and only if $P|(\theta)$, which is equivalent to $P \nmid (\langle\varepsilon\rangle - 1)$ by Corollary 10.4. This implies that $\theta \not\equiv 0 \bmod P$ if P is outside $V((\langle\varepsilon\rangle - 1)) = \mathrm{Spec}(\mathbb{T}/(\langle\varepsilon\rangle - 1))$. Thus local decomposable points are limited to weight 1 points associated to Artin representation. □

Appendix A. Control of Selmer group

We used in the main text a precise control result and determination of the size (i.e., the characteristic ideal and Fitting ideal) of the adjoint Selmer group, though perhaps it is well known to specialists. We present a detailed exposition of the control in this first appendix. The result is valid for any odd absolutely irreducible p-ordinary p-distinguished representation $\overline{\rho} : G \to \mathrm{GL}_2(\mathbb{F})$ not necessarily induced from F. We only assume that the ramification index of $\overline{\rho}$ at primes outside p is prime to p and write G for the Galois group over $\mathbb{Q}$ of the maximal p-profinite extension unramified outside p of the splitting field of $\overline{\rho}$. Write S for the set of primes $\neq p$ ramified in $F(\overline{\rho})/\mathbb{Q}$ such that $\overline{\rho}|_{I_l} = \overline{\epsilon}_l \oplus \overline{\delta}_l$. By (l) in Section 2, if $l \neq p$ outside S ramifies in $F(\overline{\rho})/\mathbb{Q}$, $\overline{\rho}|_{D_l}$ is irreducible.

Let $\boldsymbol{\kappa} := \det(\boldsymbol{\rho}) : G \to \Lambda^\times$. Then $(\Lambda, \boldsymbol{\kappa})$ represents the deformation functor

$$A \mapsto \{\xi : G \to A^\times | \xi \bmod \mathfrak{m}_A = \det(\overline{\rho})\}.$$

Consider the following deformation functor $D_{\boldsymbol{\kappa}} : CL_{/\Lambda} \to SETS$ slightly different from the one $\mathcal{D}$ defined in (s6) (or (7.1)):

$$D_{\boldsymbol{\kappa}}(A) = \{\rho \in \mathcal{D}(A) | \det(\rho) = i_A \circ \boldsymbol{\kappa}\}/\Gamma(\mathfrak{m}_A),$$

where writing $i_A : \Lambda \to A$ for Λ-algebra structure of A. This functor is again represented by $(R = R_{\mathbb{Q}}, \boldsymbol{\rho})$ regarding R as a Λ-algebra by the W-algebra homomorphism induced by $\det(\boldsymbol{\rho}) : G \to R^\times$. Indeed, if $\rho \in D_{\boldsymbol{\kappa}}(A)$, we have $i_A \circ \boldsymbol{\kappa} = \det(\rho)$. Regarding $\rho \in \mathcal{D}(A)$, we have a unique W-algebra homomorphism $R \xrightarrow{\phi} A$ such that $\phi \circ \boldsymbol{\rho} \approx \rho$, where "$\approx$" is conjugation by $\Gamma(\mathfrak{m}_A)$. Taking determinant, we get $\phi \circ \boldsymbol{\kappa} = \det(\rho)$ showing that ϕ is compatible with i_R and i_A; so, it is a Λ-algebra homomorphism, showing $\mathrm{Hom}_\Lambda(R, A) \cong D_{\boldsymbol{\kappa}}(A)$ by $\phi \leftrightarrow \rho$.

By the condition (l) for $l \in S$, the universal representation $\boldsymbol{\rho}$ is equipped with a basis $(\mathbf{v}_l, \mathbf{w}_l)$ so that $\boldsymbol{\rho}(g)\mathbf{v}_l = \epsilon_l(g)\mathbf{v}_l$ and $\boldsymbol{\rho}(g)\mathbf{w}_l = \delta_l(g)\mathbf{w}_l$ for $g \in I_l$ for the Teichmüller lift ϵ_l and δ_l of $\overline{\epsilon}_l$ and $\overline{\delta}_l$, respectively. At p, for $g \in D_p$, the matrix form of $\boldsymbol{\rho}|_{D_p}$ for this basis is $\left(\begin{smallmatrix} \boldsymbol{\epsilon} & * \\ 0 & \boldsymbol{\delta} \end{smallmatrix}\right)$ with $\boldsymbol{\delta}$ unramified. By representability, each class $c \in D_{\boldsymbol{\kappa}}(A)$ has ρ such that $V(\rho) = V(\boldsymbol{\rho}) \otimes_{R,\iota} A$ for a unique $\iota \in \mathrm{Hom}_{B\text{-alg}}(R, A)$, we can choose a unique $\rho \in c$ is equipped with a basis

$$\{(v_l = \mathbf{v}_l \otimes 1, w_l = \mathbf{w}_l \otimes 1)\}_{l \in S \cup \{p\}}$$

compatible with specialization. We always choose such a specific representative ρ for each class in $D_{\boldsymbol{\kappa}}(A)$ hereafter.

Fix $\rho_0 \in D_{\boldsymbol{\kappa}}(A)$. We study $\mathrm{Sel}(Ad(\rho_0))$. Take an A-module M with finite order and consider the ring $A[M] = A \oplus M$ with $M^2 = 0$. Then $A[M]$ is still p-profinite. Pick $\rho \in D_{\boldsymbol{\kappa}}(A[M])$ such that $\rho \bmod M = \rho_0$. By our choice of representative ρ and ρ_0 as above, we may (and do) assume ρ mod $M = \rho_0$.

Let ρ_0 act on $M_2(A)$ and $\mathfrak{sl}_2(A) = \{x \in M_2(A) | \mathrm{Tr}(x) = 0\}$ by conjugation. Write this representation $ad(\rho)$ and $Ad(\rho)$ as before. Let $ad(M) = ad(A) \otimes_A M$ and $Ad(M) = Ad(A) \otimes_A M$ and regard them as G-modules by the action on $ad(A)$ and $Ad(A)$. Then we define

$$\mathcal{F}(A[M]) = \frac{\{\rho : G \to \mathrm{GL}_2(A[M]) | (\rho \bmod M) = \rho_0, [\rho] \in D_{\boldsymbol{\kappa}}(A[M])\}}{\Gamma(M)}, \tag{A.1}$$

where $[\rho]$ is the isomorphism class in $D_{\boldsymbol{\kappa}}(A)$ containing ρ and $\Gamma(M) := \mathrm{Ker}(\mathrm{GL}_2(A[M]) \to \mathrm{GL}_2(A))$ acts on ρ by conjugation.

Take M finite as above. For $\rho \in \mathcal{F}(M)$, we can write $\rho = \rho_0 \oplus u'_\rho$ letting ρ_0 acts on $M_2(M)$ by matrix multiplication from the right. Then as before

$$\rho_0(gh) \oplus u'_\rho(gh) = (\rho_0(g) \oplus u'_\rho(g))(\rho_0(h) \oplus u'_\rho(h)) = \rho_0(gh) \oplus (u'_\rho(g)\rho_0(h) + \rho_0(g)u'_\rho(h))$$

produces $u'_\rho(gh) = u'_\rho(g)\rho_0(h) + \rho_0(g)u'_\rho(h)$ and multiplying by $\rho_0(gh)^{-1}$ from the right, we get the cocycle relation for $u_\rho(g) = u'_\rho(g)\rho_0(g)^{-1}$:

$$u_\rho(gh) = u_\rho(g) + gu_\rho(h) \ \text{ for } gu_\rho(h) = \rho(g)u_\rho(h)\rho_0(g)^{-1},$$

getting the map $\mathcal{F}(A[M]) \to H^1(G, ad(M))$ which factors through $H^1(G, Ad(M))$. By computation, we can easily verify that ρ is $(1 + M_2(M))$-conjugate to ρ' if and only if u_ρ is cohomologous to $u_{\rho'}$; so, this map is injective A-linear map identifying $\mathcal{F}(A[M])$ with

$$\mathrm{Sel}(Ad(M)) := \mathrm{Ker}(H^1(G, Ad(M)) \xrightarrow{\mathrm{Res}} \frac{H^1(\mathbb{Q}_p, Ad(M))}{F^+_- H^1(\mathbb{Q}_p, Ad(M))}),$$

where $F^+_- H^1(\mathbb{Q}_p, Ad(M)) \subset H^1(\mathbb{Q}_p, Ad(M))$ is a A-submodule spanned by cohomology classes of cocycles $u : G \to Ad(M)$ upper triangular over D_p and upper nilpotent over I_p.

If $M = \varinjlim_i M_i$ for finite A-modules M_i, we just define

$$\mathrm{Sel}(Ad(M)) = \varinjlim_i \mathrm{Sel}(Ad(M_i)).$$

Then for finite M_i, $\mathcal{F}(A[M_i]) = \mathrm{Sel}(Ad(M_i))$ and $\varinjlim_i \mathcal{F}(M_i) = \mathrm{Sel}(\varinjlim_i Ad(M_i))$.

For each $[\rho_0] \in D_{\boldsymbol{\kappa}}(A)$, choose a representative $\rho_0 = \iota \circ \boldsymbol{\rho}$. Then we have a map $\mathcal{F}(A[M]) \to D_{\boldsymbol{\kappa}}(A[M])$ for each finite A-module M sending $\rho \in \mathcal{F}(A[M])$ to the class $[\rho] \in D_{\boldsymbol{\kappa}}(A[M])$. By our choice of ρ, this map is injective.

Conversely pick a class $c \in D_{\boldsymbol{\kappa}}(A[M])$ over $[\rho_0] \in D_{\boldsymbol{\kappa}}(A)$. Then for $\rho \in c$, we have $x \in 1 + M_2(\mathfrak{m}_{A[M]})$ such that $x\rho x^{-1} \mod M = \rho_0$. By replacing ρ by $x\rho x^{-1}$ and choosing the lifted base, we conclude $\mathcal{F}(A[M]) \cong \{[\rho] \in D_{\boldsymbol{\kappa}}(A[M]) | \rho \mod M \sim \rho_0\}$; so, for finite M,

$$\begin{aligned}\mathrm{Sel}(Ad(M)) = \mathcal{F}(A[M]) = \{\phi \in \mathrm{Hom}_{\Lambda\text{-alg}}(R, A[M]) : \phi \bmod M = \iota\} \\ = Der_\Lambda(R, M) \cong \mathrm{Hom}_A(\Omega_{R/\Lambda} \otimes_{R,\iota} A, M).\end{aligned}$$

Thus

$$\mathrm{Sel}(Ad(M)) \cong \mathrm{Hom}_A(\Omega_{R/\Lambda} \otimes_{R,\iota} A, M). \tag{A.2}$$

Theorem A.1 (B. Mazur)**.** *For any $A \in CL_\Lambda$, we have a canonical isomorphism:* $\mathrm{Sel}(Ad(\rho_0))^\vee \cong \Omega_{R/\Lambda} \otimes_{R,\iota} A$. *In particular, if ρ_0 is modular with ι factoring through $\mathbb{T}$, we have* $\mathrm{Sel}(Ad(\rho_0))^\vee = \mathrm{Sel}(Ad(\rho_{\mathbb{T}}))^\vee \otimes_{\mathbb{T}} A$.

The last assertion follows from the transitivity of tensor product:

$$\mathrm{Sel}(Ad(\rho_{\mathbb{T}}))^\vee \otimes_{\mathbb{T}} A = \Omega_{R/\Lambda} \otimes_R \mathbb{T} \otimes_{\mathbb{T}} A = \Omega_{R/\Lambda} \otimes_R A = \mathrm{Sel}(Ad(\rho_0))^\vee.$$

We only prove the first assertion.

Proof. Take the Pontryagin dual $A^\vee := \mathrm{Hom}_B(A, \Lambda^\vee) = \mathrm{Hom}_{\mathbb{Z}_p}(A \otimes_\Lambda \Lambda, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$. Since $A = \varprojlim_i A_i$ for finite rings A_i and $\mathbb{Q}_p/\mathbb{Z}_p = \varinjlim_j p^{-1}\mathbb{Z}/\mathbb{Z}$, $A^\vee = \varinjlim_i \mathrm{Hom}(A_i, \mathbb{Q}_p/\mathbb{Z}_p) = \varinjlim_i A_i^\vee$ is a union of the finite modules $A_i^\vee$. We define $\mathrm{Sel}(Ad(\rho_0)) := \varinjlim_j \mathrm{Sel}(Ad(A_i^\vee))$. Defining $\mathcal{F}(A[A^\vee]) = \varinjlim_i \mathcal{F}_l(A[A_i^\vee])$, we see from compatibility of cohomology with injective limit

$$\mathrm{Sel}(Ad(\rho_0)) = \varinjlim_i \mathrm{Sel}(Ad(A_i^\vee)) = \varinjlim_j \mathrm{Ker}(H^1(G, Ad(A_i^\vee)) \to \frac{H^1(\mathbb{Q}_p, Ad(A_i^\vee))}{F_-^+ H^1(\mathbb{Q}_p, Ad(A_i^\vee))})$$

By the formula (A.2),

$$\begin{aligned}\mathrm{Sel}(Ad(\rho_0)) &= \varinjlim_i \mathrm{Sel}(Ad(A_i^\vee)) = \varinjlim_i \mathrm{Hom}_R(\Omega_{R/\Lambda} \otimes_R A, A_i^\vee) \\ &= \mathrm{Hom}_A(\Omega_{R/\Lambda} \otimes_R A, A^\vee) = \mathrm{Hom}_A(\Omega_{R/\Lambda} \otimes_R A, \mathrm{Hom}_{\mathbb{Z}_p}(A, \mathbb{Z}_p)) \\ &= \mathrm{Hom}_{\mathbb{Z}_p}(\Omega_{R/\Lambda} \otimes_R A, \mathbb{Q}_p/\mathbb{Z}_p) = (\Omega_{R/\Lambda} \otimes_R A)^\vee.\end{aligned}$$

Taking Pontryagin dual back, we finally get

$$\mathrm{Sel}(Ad(\rho_0))^\vee \cong \Omega_{R/\Lambda} \otimes_{R,\iota} A \text{ and } \mathrm{Sel}(Ad(\overline{\rho}))^\vee \cong \Omega_{R/\Lambda} \otimes_R \mathbb{F}$$

as desired. In particular, we have $\mathrm{Sel}(Ad(\boldsymbol{\rho}))^\vee = \Omega_{R/\Lambda}$. □

Appendix B. p-Adic adjoint L-function

In [H16, §6.5.5], we constructed a p-adic L-function interpolating the size of the adjoint Selmer group $\mathrm{Sel}(Ad(\rho))$ for each specialization $\rho_P = \rho_{\mathbb{T}} \mod P$ with $P \in \mathrm{Spec}(\Lambda)$ for each irreducible component of the form $\mathrm{Spec}(\Lambda)$ of $\mathrm{Spec}(\mathbb{T})$. Here we generalize this construction of the L-function $L^{mod} = L^{mod}_{\mathbb{I}} \in \mathbb{I}$ to general irreducible components $\mathrm{Spec}(\mathbb{I})$ of $\mathrm{Spec}(\mathbb{T})$ and glue them together to obtain $L_{\mathbb{T}} \in \mathbb{T}$ having the interpolation property all over $\mathrm{Spec}(\mathbb{T})$ (not just over $\mathrm{Spec}(\mathbb{I})$). Here we keep the notation introduced in Section A, in particular, $(R, \boldsymbol{\rho})$ is the minimal universal deformation ring representing $D_{\boldsymbol{\kappa}}$ and we have a canonical surjective morphism $\iota_{\mathbb{T}} : R \to \mathbb{T}$ such that $\rho_{\mathbb{T}} \approx \iota_{\mathbb{T}} \circ \boldsymbol{\rho}$.

We assume $R = \mathbb{T}$ and (2.3): $\mathbb{T}$ has a presentation $\mathbb{T} = \Lambda[[X_1, \dots, X_r]]/(S_1, \dots, S_r)$ for $r = \dim_{\mathbb{F}} \mathrm{Sel}(Ad(\overline{\rho}))$. Let $\rho : G \to \mathrm{GL}_2(A) \in D_{\boldsymbol{\kappa}}(A)$ be a deformation of $\overline{\rho}$ such that $\rho \cong P \circ \rho_{\mathbb{T}}$. We have an exact sequence for $(P : \mathbb{T} \to A) \in \mathrm{Hom}_{\Lambda\text{-alg}}(\mathbb{T}, A)$

$$\begin{array}{ccccc}(S_1, \dots, S_r)/(S_1, \dots, S_r)^2 \otimes_{\mathbb{T}} A & \longrightarrow & \bigoplus_{j=1}^r A \cdot dX_j & \twoheadrightarrow & \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} A \\ \| \big\downarrow S_j \mapsto dS_j & & \| \big\downarrow & & \wr \big\downarrow \\ \bigoplus_{j=1}^r A \cdot dS_j & \xrightarrow{\ell} & \bigoplus_{j=1}^r A \cdot dX_j & \twoheadrightarrow & \mathrm{Sel}(Ad(\rho))^\vee.\end{array}$$

Then we define

$$L_{\mathbb{T}} := \det(\bigoplus_{j=1}^{r} A\cdot dS_j \xrightarrow{\ell} \bigoplus_{j=1}^{r} \mathbb{T}\cdot dX_j), \tag{B.1}$$

The element $L_{\mathbb{T}}$ gives rise to a p-adic L-function with

$$\mathrm{Spec}(\mathbb{T})(W) \ni P \mapsto |L_{\mathbb{T}}(P)|_p^{-1} = |\mathrm{Sel}(Ad(P\circ\boldsymbol{\rho}))|.$$

Let $\lambda : \mathbb{T} = \mathbb{T} \twoheadrightarrow \mathbb{I}$ be a Λ-algebra surjective homomorphism for an integral domain $\mathbb{I}$ finite torsion-free over Λ. Let $\mathbb{T}_{\mathbb{I}} := \mathbb{T}\otimes_\Lambda \mathbb{I}$ and $\widetilde{\lambda}$ be the composite $\mathbb{T}_{\mathbb{I}} \twoheadrightarrow \mathbb{I}\otimes_\Lambda\mathbb{I} \xrightarrow[\twoheadrightarrow]{a\otimes b\mapsto ab} \mathbb{I}$. Then for each $P \in \mathrm{Spec}(\mathbb{I})(W) = \mathrm{Hom}_{W\text{-alg}}(\mathbb{I}, W)$, $\widetilde{\lambda}$ induces $\Lambda \hookrightarrow \mathbb{T}_{\mathbb{I}} \xrightarrow{\widetilde{\lambda}} \mathbb{I} \xrightarrow{P} W$ by composition.

Writing $\rho_P := P\circ\lambda\circ\boldsymbol{\rho}$. Then $\det\rho_P$ is a deformation of $\det\overline{\rho}$; so, we have a unique morphism $\iota_P : \Lambda \to W$ such that $\iota_P\circ\kappa = \det(\rho_P)$. Since the Λ-algebra structure $\iota : \Lambda \to \mathbb{T}$ of $\mathbb{T} = \mathbb{T}$ is given by $\det(\boldsymbol{\rho}) = \det(\rho_{\mathbb{T}}) = \iota\circ\kappa$, we find out that the above composite is just ι_P.

Let $\mathbb{T}_P = \mathbb{T}_{\mathbb{I}}\otimes_{\mathbb{I},P} W$ under the above algebra homomorphism. Note that

$$\mathbb{T}_P = \mathbb{T}\otimes_\Lambda \mathbb{I}\otimes_{\mathbb{I},P} W \cong \mathbb{T}\otimes_{\Lambda,\iota_P} W$$

by associativity of tensor product.

By construction, we have $\lambda_P : \mathbb{T}_P \to W$ induced by λ. Even if $\iota_P = \iota_{P'}$, λ_P may be different from $\lambda_{P'}$. If λ_P is associated to a Hecke eigenform of weight ≥ 2, we call P a **arithmetic** point. If $\mathbb{T}_P\otimes_W \mathrm{Frac}(W) = \mathrm{Frac}(W)\oplus(\mathrm{Ker}(\lambda_P)\otimes_W \mathrm{Frac}(W))$ as algebra direct sum, we call P **admissible**. If P is admissible, write S_P for the image of $\mathbb{T}_P$ in $(\mathrm{Ker}(\lambda_P)\otimes_W \mathrm{Frac}(W))$. Then define the congruence module $C_0(\lambda_P) := S_P\otimes_{\mathbb{T}_P,\lambda_P} W$. If P is arithmetic, it is admissible. Since $\mathbb{T}_{\mathbb{I}}$ is a complete intersection over $\mathbb{I}$, by a theorem of Tate (see [MR70, Appendix] or [H16, Theorem 6.8]),

$$|C_0(\lambda_P)| = |\Omega_{\mathbb{T}_{\mathbb{I}}/\mathbb{I}}\otimes_{\mathbb{T}_{\mathbb{I}}} \mathbb{I}/P| = |\Omega_{\mathbb{T}/\Lambda}\otimes_{\mathbb{T}} \mathbb{I}/P|. \tag{B.2}$$

If $\rho\in D_{\boldsymbol{\kappa}}(A)$ for W-valued $\kappa = \det(\rho_P)$, then $\rho \in D_{\boldsymbol{\kappa}}(A)$ and hence $\rho = \phi\circ\boldsymbol{\rho}$ for $\phi : \mathbb{T}\to A$. By definition, ϕ factors through

$$\mathbb{T}/R(\det(\boldsymbol{\rho})(g) - \kappa(g))_g R = \mathbb{T}/R(\kappa(g)-\kappa(g))_g R = R\otimes_{\Lambda,\kappa} W.$$

This shows that $\mathbb{T} = R\otimes_{\Lambda,\kappa} W$ for $\kappa : \Lambda = W[[\Gamma]] \to W$ induced by κ. Applying this to $\mathbb{T}_P$, we get $R_{\det(\rho_P)} = \mathbb{T}_P$.

Here is a well known theorem (a combination of (2.3) and an old result of mine [H88]) which shows non-vanishing at arithmetic P of the p-adic L-function $L_{\mathbb{T}}$ interpolating the size of adjoint Selmer group over $\mathrm{Spec}(\mathbb{T})$ (e.g., [MFG, §5.3.6]) for canonical periods $\Omega_{f,\pm}$ of f:

Theorem B.1. *Assume $R = \mathbb{T}$ and (2.3). Let $\lambda : \mathbb{T}\twoheadrightarrow \mathbb{I}$ be a surjective Λ-algebra homomorphism for a domain $\mathbb{I}$ containing Λ and $\widetilde{\lambda} : \mathbb{T}_{\mathbb{I}} \to \mathbb{I}$ be its scalar extension to $\mathbb{I}$. Then there exists $L_{\mathbb{I}}\in\mathbb{I}$ such that $C_0(\lambda) = \mathbb{I}/(L_{\mathbb{I}})$ and for each admissible $P\in\mathrm{Spec}(\mathbb{I})$, $C_0(\lambda_P) = W/P(\lambda(L_{\mathbb{I}}))$ and if $P\circ\lambda\circ\rho_{\mathbb{T}} \cong \rho_f$ for a modular form of weight ≥ 2, we have $|\mathrm{Sel}(Ad(\rho_P)| = |C_0(\lambda_P)| = |W/L_{\mathbb{I}}(P)| = |\frac{L(1,Ad(\rho_f))}{\Omega_{f,+}\Omega_{f,-}}|_p^{-1} < \infty$ (so, $L_{\mathbb{I}}(P)\neq 0$), where $L_{\mathbb{I}}(P) := P(\lambda(L_{\mathbb{I}}))$.*

By (B.2), we need to prove only $|C_0(\lambda_P)| = |W/P(\lambda(L_{\mathbb{I}}))| = |\frac{L(1,Ad(\rho_f))}{\Omega_{f,+}\Omega_{f,-}}|_p^{-1}$. If f is of weight 2 on a modular curve X, for $\mathcal{W} = W\cap\overline{\mathbb{Q}}$, we have $H^1(X,\mathcal{W})[\lambda_P] = \mathcal{W}\omega_+(f)\oplus\mathcal{W}\omega_-(f)$ ($\pm$-eigenspace under the pull-back action of $z\mapsto -\overline{z}$ on the upper half complex plane) and $H^1(X,\mathbb{C}) = \mathbb{C}\delta_+(f) + \mathbb{C}\delta_-(f)$ for $\delta_\pm f = f(z)dz \mp f(-\overline{z})d\overline{z}$. Then $\Omega_{f,\pm}\omega_\pm(f) = \delta_\pm(f)$. We use Eichler-Shimura isomorphism to define $\Omega_{f,\pm}$ for higher weight (see [H16, Theorem 6.28] for details).

Since $L_{\mathbb{I}}(P)\neq 0$ is a key to show local indecomposability of modular Galois representation (Theorem C), we give a sketch of a proof of the non-vanishing in two steps.

Proof. Step. 1: Existence of $L_{\mathbb{I}}$. Write $M^* := \mathrm{Hom}_{\mathbb{I}}(M,\mathbb{I})$ for an $\mathbb{I}$-module M. Let S be the image of $\mathbb{T}_{\mathbb{I}}$ in $\mathfrak{B}\otimes_{\mathbb{I}}\mathrm{Frac}(\mathbb{I})$ for $\mathfrak{B} = \mathrm{Ker}(\widetilde{\lambda})$ in the decomposition $\mathbb{T}\otimes_\Lambda\mathrm{Frac}(\mathbb{I}) = \mathrm{Frac}(\mathbb{I})\oplus(\mathfrak{B}\otimes_{\mathbb{I}}\mathrm{Frac}(\mathbb{I}))$. Let $\mu : \mathbb{T}_{\mathbb{I}}\to S$ be the projection and put $\mathfrak{A} = \mathrm{Ker}(\mu)$. So we have a split exact sequence $\mathfrak{B}\hookrightarrow\mathbb{T}_{\mathbb{I}}\twoheadrightarrow\mathbb{I}$. A local complete intersection $\mathbb{T}_{\mathbb{I}}$ over $\mathbb{I}$ has such a self-dual pairing $(\cdot,\cdot)$ with values in $\mathbb{I}$ such that $(xy,z) = (x,yz)$ for $x,y,z\in\mathbb{T}_{\mathbb{I}}$. Thus $\mathfrak{B}^*\cong\mathbb{T}_{\mathbb{I}}^*/\mathbb{I}^*$, and $\mathbb{I}^*\subset\mathbb{T}_{\mathbb{I}} = \mathbb{T}_{\mathbb{I}}^*$ is a maximal submodule of

$\mathbb{T}_{\mathbb{I}}$ on which $\mathbb{T}_{\mathbb{I}}$ acts through $\widetilde{\lambda}$; so, $\mathbb{I}^* = \mathfrak{A}$ inside $\mathbb{T}_{\mathbb{I}}$. This implies $\mathfrak{B}^* \cong S$; so, S is $\mathbb{I}$-free. In other words, applying $\mathbb{I}$-dual, we get a reverse exact sequence

$$\begin{array}{ccccc} \mathbb{I}^* & \xrightarrow{\hookrightarrow} & \mathbb{T}_{\mathbb{I}}^* & \xrightarrow{\twoheadrightarrow} & \mathfrak{B}^* \\ \wr\downarrow & & \wr\downarrow & & \wr\downarrow \\ ? & \longrightarrow & \mathbb{T}_{\mathbb{I}} & \longrightarrow & S \end{array}$$

This shows $? = \mathfrak{A} \cong \mathbb{I}^* \cong \mathbb{I}$; so, $\mathfrak{A}$ is principal. Define $L_{\mathbb{I}} \in \mathbb{I}$ by $\mathfrak{A} = (L_{\mathbb{I}})$. Note that $C_0(\widetilde{\lambda}) = \mathbb{I}/\mathfrak{A}$.

Step. 2: Specialization property. We have $\mathfrak{B}^* = S$ and a split exact sequence $\mathfrak{B} \to \mathbb{T}_{\mathbb{I}} \to \mathbb{I}$; so, $\mathfrak{B}$ is an $\mathbb{I}$-direct summand of $\mathbb{T}_{\mathbb{I}}$. Tensoring W over $\mathbb{I}$ via P, $\mathfrak{B} \otimes_{\mathbb{I},P} W \to \mathbb{T}_P \to W$ is exact, and we get $\mathfrak{B}_P = \mathfrak{B} \otimes_{\mathbb{I},P} W = \mathrm{Ker}(\lambda_P)$. Since $\mathbb{T}$ is Λ-free of finite rank, $\mathbb{T}_{\mathbb{I}}$ is $\mathbb{I}$-free of finite rank. Thus $\mathfrak{B}$ is $\mathbb{I}$-projective and hence $\mathbb{I}$-free; so, $S \cong \mathfrak{B}^*$ is $\mathbb{I}$-free. Tensoring W over $\mathbb{I}$ via P, we get

$$0 \to \mathfrak{A} \otimes_{\mathbb{I},P} W \to \mathbb{T}_P \to S \otimes_{\mathbb{I},P} W \to 0.$$

Thus if P is admissible, $S_P := S \otimes_{\mathbb{I},\lambda_P} W$ gives rise to the decomposition: $\mathbb{T}_P \otimes_W \mathrm{Frac}(W) = \mathrm{Frac}(W) \oplus (S_P \otimes_W \mathrm{Frac}(W))$. By $\mathfrak{B}_P = \mathfrak{B}_P \otimes_{\mathbb{I},P} W = \mathrm{Ker}(\lambda_P)$, we get $C_0(\lambda_P) = S_P/\mathfrak{B}_P = (S/\mathfrak{B}) \otimes_{\mathbb{I},P} W = C_0(\widetilde{\lambda}) \otimes_{\mathbb{I},P} W$, as desired. □

Tensoring $\mathbb{I}$ with the exact sequence of $\mathbb{T}$-modules:

$$(S_1, \dots, S_r)/(S_1, \dots, S_r)^2 \xrightarrow{f \mapsto df} \Omega_{\Lambda[[X_1,\dots,X_r]]/\Lambda} \otimes_{\Lambda[[X_1,\dots,X_r]]} \mathbb{T} \twoheadrightarrow \Omega_{\mathbb{T}/\Lambda}$$

over $\mathbb{T}$, we get an exact sequence $\bigoplus_j \mathbb{I} dS_j \xrightarrow{d \otimes 1 = \lambda(d)} \bigoplus_j \mathbb{I} dX_j \to \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T},\lambda} \mathbb{I} \to 0$. Since $\mathbb{T}_{\mathbb{I}} = \mathbb{I}[[X_1, \dots, X_r]]/(S_1, \dots, S_r)_{\mathbb{I}}$, we have

$$\Omega_{\mathbb{T}_{\mathbb{I}}/\mathbb{I}} \otimes_{\mathbb{T}_{\mathbb{I}},\widetilde{\lambda}} \mathbb{I} = \bigoplus_j \mathbb{I} dX_j / \bigoplus_j \mathbb{I} dS_j = \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T},\lambda} \mathbb{I}.$$

They have the same characteristic ideals (and Fitting ideals) by Tate's theorem [H16, Theorem 6.8]. Thus in general, we get

$$(\lambda(L_{\mathbb{T}})) = (\lambda(\det(d))) = (\det(d \otimes 1)) = \mathrm{char}(\Omega_{\mathbb{T}_{\mathbb{I}}/\mathbb{I}} \otimes_{\mathbb{T}_{\mathbb{I}},\widetilde{\lambda}} \mathbb{I}) \overset{\text{Tate}}{=} \mathrm{char}(C_0(\widetilde{\lambda})) = (L_{\mathbb{I}}).$$

Thus we obtain

Corollary B.2. *Let the notation and assumption be as in* Theorem B.1. *Then $\lambda(L_{\mathbb{T}}) = L_{\mathbb{I}}$ up to units in $\mathbb{I}$, and if $P \in \mathrm{Spec}(\mathbb{T})(\overline{\mathbb{Q}}_p)$ satisfies $P \circ \lambda \circ \rho_{\mathbb{T}} \cong \rho_f$ for a modular form f of weight ≥ 2, we have $|\mathrm{Sel}(Ad(\rho_P)| = |C_0(\lambda_P)| = |W/L_{\mathbb{T}}(P)| = |\frac{L(1,Ad(\rho_f))}{\Omega_{f,+}\Omega_{f,-}}|_p^{-1} < \infty$ (so, $L_{\mathbb{T}}(P) \neq 0$), where $L_{\mathbb{T}}(P) := P(\lambda(L_{\mathbb{T}}))$.*

The corollary tells us that $L_{mod} \in \mathbb{I}$ glues (up to units) well to $L_{\mathbb{T}}$ so that the image $\lambda(L_{\mathbb{T}})$ of $L_{\mathbb{T}}$ in $\mathbb{I}$ is equal to $L_{\mathbb{I}}$ of $\mathbb{I}$ up to units, and in particular, $L_{\mathbb{T}}(P) \neq 0$ if P is an arithmetic point.

Appendix C. Action of σ on Selmer groups

In this last section, we assume that $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \varphi$ for a real quadratic field F. We identify the "+"-eigenspace $\mathrm{Sel}^+(Ad(\rho_{\mathbb{T}}))^\vee$ under the action of σ with $\Omega_{\mathbb{T}_+/\Lambda}$. We need a general facts on relative dualizing modules. Let B be a commutative p-profinite local ring for a prime $p > 2$. Consider a local B-algebra A finite over B with $B \hookrightarrow A$. Write $\omega_{A/B}$ for the dualizing module for the finite (hence proper) morphism $X := \mathrm{Spec}(A) \xrightarrow{f} \mathrm{Spec}(B) =: Y$ if it exists (in the sense of [Kl80, (6)]). For the dualizing functor $f^!$ from quasi coherent Y-sheaves into quasi coherent X-sheaves defined in [Kl80, (2)], we have $\mathrm{Hom}_A(F, f^! N) = \mathrm{Hom}_B(f_* F, N)$ for any quasi-coherent sheaves F over X and N over Y; so, if $\omega_{A/B}$ exists (i.e., $f^!(N) = N \otimes_B \omega_{A/B}$), taking $F = A$ and $N = B$, we have $\omega_{A/B} = f^!(\mathcal{O}_Y) = \mathrm{Hom}_B(A, B)$ as A-modules. As shown in [Kl80, (21)], $\mathrm{Spec}(A) \xrightarrow{f} \mathrm{Spec}(B)$ has dualizing module if and only if f is Cohen Macaulay (e.g., if B is regular and A is free of finite rank over B). Even if we do not have dualizing module $\omega_{A/B}$, we just define $\omega_{A/B} := \mathrm{Hom}_B(A, B)$ generally.

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

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

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

We now identify the dualizing module with classical "inverse different". Let $C\supset B$ be reduced algebras. By abusing notation, write $\omega_{C/B}:=\mathrm{Hom}_B(C,B)$ in general. Suppose that $\mathrm{Frac}(C)/\mathrm{Frac}(B)$ is étale to have a trace map $\mathrm{Tr}:\mathrm{Frac}(C)\to\mathrm{Frac}(B)$, and $\omega_{\mathrm{Frac}(C)/\mathrm{Frac}(B)}=\mathrm{Frac}(C)\mathrm{Tr}$ by the trace pairing $(x,y)\mapsto\mathrm{Tr}(xy)$. We define a C-fractional ideal (called the inverse different for C/B) by

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

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

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

We now prove

Theorem C.2. *Let $\mathrm{Sel}^+(Ad(\rho_{\mathbb{T}})):=\{x\in\mathrm{Sel}(Ad(\rho_{\mathbb{T}}))|\sigma(x)=x\}$, and suppose* (H0–2). *Then we have a canonical isomorphism $\Omega_{\mathbb{T}_+/\Lambda}\cong\mathrm{Sel}^+(Ad(\rho_{\mathbb{T}}))^\vee$.*

Proof. By Corollary 3.7 (1), we can apply Proposition C.1 to $B=\Lambda$, $D=\mathbb{T}$ and $C=\mathbb{T}_+$. We have the first fundamental exact sequence [CRT, Theorem 25.1]:

$$\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T}\xrightarrow{i}\Omega_{\mathbb{T}/\Lambda}\to\Omega_{\mathbb{T}/\mathbb{T}_+}\to 0. \tag{C.1}$$

We can choose $\Theta\in\mathbb{T}$ which is the image in $\mathbb{T}$ of X in Theorem 2.2 so that $\sigma(\Theta)=-\Theta$ as $\mathbb{T}/I$ is a surjective image of Λ and I is generated by $\mathbb{T}_-$. Then $\mathbb{T}_+=\Lambda[\Theta^2]$, which is a local complete intersection (so, Gorenstein). Thus we get from Proposition C.1, $\mathfrak{d}_{\mathbb{T}/\mathbb{T}_+}\mathfrak{d}_{\mathbb{T}_+/\Lambda}=\mathfrak{d}_{\mathbb{T}/\Lambda}$. By Tate's theorem [MR70, Appendix, (A.3)] or [H16, §6.3.3], $\mathfrak{d}_{X/Y}=\mathrm{Fitt}_X(\Omega_{X/Y})$ for any subset $\{X,Y\}\subset\{\mathbb{T},\mathbb{T}_+,\Lambda\}$ with $X\supset Y$ and $\mathfrak{d}_{\mathbb{T}_+/\Lambda}\mathbb{T}=\mathrm{Fitt}_{\mathbb{T}}(\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T})$, writing $\mathrm{Fitt}(M)$ for the Fitting ideal of a $\mathbb{T}$-module M of finite type (see [MW84, Appendix] for a concise description of the theory of Fitting ideal). Since $X_{/Y}$ is a relative local complete intersection, $\mathfrak{d}_{X/Y}$ is a principal ideal generated by a non-zero divisor again by Tate's theorem.

Suppose relative complete intersection property: $X=Y[[(T)]]/(S)$ for a set of variable $(T):=(T_1,\dots,T_r)$ and a regular sequence $(S):=(S_1,\dots,S_r)\subset\mathfrak{m}_{Y[[(T)]]}$ with X free of finite rank over Y. Then we have the following commutative diagram with exact rows:

$$\begin{array}{ccccc}
(S)/(S)^2 & \longrightarrow & \Omega_{Y[[(T)]]/Y}\otimes_{Y[[(T)]]}X & \twoheadrightarrow & \Omega_{X/Y}\\
\wr\downarrow{\scriptstyle S_j\mapsto dS_j} & & \wr\downarrow & & \|\downarrow\\
XdS_1\oplus\cdots\oplus XdS_r & \xrightarrow{\ell} & XdT_1\oplus\cdots\oplus XdT_r & \twoheadrightarrow & \Omega_{X/Y}.
\end{array}$$

Thus $\mathrm{Fitt}(\Omega_{X/Y})=(\det(\ell))$ and hence $\mathrm{Fitt}(\Omega_{X/Y})$ kills $\Omega_{X/Y}$. If $M\hookrightarrow L\twoheadrightarrow N$ is an exact sequence of $\mathbb{T}$-modules, we have $\mathrm{Fitt}(M)\,\mathrm{Fitt}(N)\subset\mathrm{Fitt}(L)$ and $\mathrm{Fitt}(N)\supset\mathrm{Fitt}(L)$ [MW84, Appendix, 1, 9]. By (C.1), $\mathrm{Fitt}(\mathrm{Im}(i))\,\mathrm{Fitt}(\Omega_{\mathbb{T}/\mathbb{T}_+})\subset\mathrm{Fitt}(\Omega_{\mathbb{T}/\Lambda})$ and $\mathrm{Fitt}(\mathrm{Ker}(i))\,\mathrm{Fitt}(\mathrm{Im}(i))\subset\mathrm{Fitt}(\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T})$. Since $\mathfrak{d}_{X/Y}$ is a principal ideal generated by a non-zero divisor (as already remarked), the identity $\mathfrak{d}_{\mathbb{T}/\mathbb{T}_+}\mathfrak{d}_{\mathbb{T}_+/\Lambda}=\mathfrak{d}_{\mathbb{T}/\Lambda}$ then implies $\mathrm{Fitt}(\mathrm{Im}(i))=\mathrm{Fitt}(\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T})$. Therefore $\mathrm{Fitt}(\mathrm{Ker}(i))=\mathbb{T}$; so, $\mathrm{Ker}(i)$ is killed by $1\in\mathbb{T}$, and i is an injection, and (C.1) is a short exact sequence.

For a module M with σ-action, we write $M^+:=\{x\in M|\sigma(x)=x\}$. Since $\mathbb{T}\cong\mathbb{T}_+[X]/(X^2-\theta)$ for $\theta:=\Theta^2$ by Corollary 3.7 (1), σ acts on $\Omega_{\mathbb{T}/\mathbb{T}_+}\cong(\mathbb{T}/(\Theta))d\theta$ by -1. Thus by taking "+"-eigenspace of the exact sequence $\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T}\hookrightarrow\Omega_{\mathbb{T}/\Lambda}\twoheadrightarrow\Omega_{\mathbb{T}/\mathbb{T}_+}$, we get an isomorphism: $\Omega_{\mathbb{T}_+/\Lambda}\cong\Omega^+_{\mathbb{T}/\Lambda}$, because $\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T}=\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T}_+\oplus\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T}_-$ with $\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T}_+=\Omega_{\mathbb{T}_+/\Lambda}=(\Omega_{\mathbb{T}_+/\Lambda}\otimes_{\mathbb{T}_+}\mathbb{T})^+$. Since $\mathrm{Sel}(Ad(\rho_{\mathbb{T}}))^\vee\cong\Omega_{\mathbb{T}/\Lambda}$ by $R\cong\mathbb{T}$ (see Theorem A.1), we get the desired identity by taking "+" eigenspace of σ. □

References

Books

[BCM] N. Bourbaki, *Algèbre Commutative*, Masson, Paris, 1985–1998.

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

[EMI] H. Hida, *Elementary Modular Iwasawa Theory*, World Scientific, Singapore, to be published in late 2021.

[FGS] J. Bellaïche and G. Chenevier, *Families of Galois representations and Selmer groups.* Astérisque, **324** 2009.

[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`).

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

[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 Monographs in Mathematics, Springer, 2006.

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

Articles

[BD16] J. Bellaïche and M. Dimitrov, On the eigencurve at classical weight 1 points, Duke Math. J. **165** (2016), 245–266.

[Be17] A. Betina, Ramification of the eigencurve at classical RM points, Canad. J. Math. **72** (2020), 57–88.

[BGKK18] G. Boeckle, D. Guiraud, S. Kalyanswamy and C. Khare, Wieferich Primes and a mod p Leopoldt Conjecture, preprint, 31 pages, 2018 (arXiv:1805.00131).

[CPS75] E. Cline, B. Parshall, L. Scott, Cohomology of finite groups of Lie type, I, Publications de l'IHES, **45** (1975), 169–191.

[CWE19] F. Castella and C. Wang-Erickson, Class groups and local indecomposability for non-CM forms", preprint 2018, Posted at `https://arxiv.org/abs/1807.02499`, to appear in Journal of the European Mathematical Society.

[Ch14] G. Chenevier, The p-adic analytic space of pseudocharacters of a profinite group, and pseudorepresentations over arbitrary rings, Automorphic Forms and Galois Representations: Vol. I, London Mathematical Society Lecture Note Series, vol. **414**, Cambridge Univ. Press, Cambridge, 2014, pp. 221-285.

[C99] S. Cho, Deformations of induced Galois representations, Thesis, University of California, Los Angeles, 1999.

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

[Di14] M. Dimitrov, On the local structure of ordinary Hecke algebras at classical weight one points. Automorphic forms and Galois representations. Vol. 2, 1–16, London Math. Soc. Lecture Note Ser., **415**, Cambridge Univ. Press, Cambridge, 2014.

[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.

[DG12] M. Dimitrov and E. Ghate, On classical weight one forms in Hida families. J. Théor. Nombres Bordeaux **24** (2012), 669–690.

[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.

[GV04] E. Ghate and V. Vatsal, On the local behaviour of ordinary Λ-adic representations, Ann. Inst. Fourier (Grenoble) **54** (2004), 2143–2162 (2005).

[H86] H. Hida, Iwasawa modules attached to congruences of cusp forms, Ann. Sci. Ec. Norm. Sup. 4th series **19** (1986), 231–273.

[H88] H. Hida, Modules of congruence of Hecke algebras and L–functions associated with cusp forms, Amer. J. Math. **110** (1988), 323–382.

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

[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.

[H20] H. Hida, Cyclicity of adjoint Selmer groups and fundamental units, Advanced Studies in Pure Math. **86** (2020), 351–411.

[H21] H. Hida, Local indecomposability via a presentation of the Hecke algebra, appendix to "Class groups and local indecomposability for non-CM forms" by F. Castella and C. Wang-Erickson, to appear in Journal of the European Mathematical Society.

[Ka16] S. Kalyanswamy, Remarks on automorphy of residually dihedral representations, Mathematical Research Letters Volume 25 (2018) 1285–1304.

[Kl07] J. Klaška, Short remark on Fibonacci-Wieferich primes, Acta Mathematica Universitatis Ostraviensis, **15** (2007), 21–25.

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

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

[MW84] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, Inventiones Math. **76** (1984), 179–330.

[R84] K. Ribet, Congruence relations between modular forms. Proceedings of the International Congress of Mathematicians, **1** (1984), 503–514, PWN, Warsaw, 1984.

[SS92] Zhi-Hong Sun and Zhi-Wei Sun, Fibonacci numbers and Fermats last theorem, Acta Arithmetica **60** (1992), 371–388.

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

[Th16] Jack A. Thorne, Automorphy of some residually dihedral Galois representations, Math. Ann. **364** (2016), 589–648.

[TU20] J. Tilouine and E. Urban, Integral period relations and congruences, preprint, 2020, posted on arXiv:1811.11166v2 [math.NT].

[WE15] C. Wang-Erickson, Algebraic families of Galois representations and potentially semi-stable pseudodeformation rings, Math. Ann. **371** (2018), 1615–1681.

[WWE17] P. Wake and C. Wang-Erickson, Ordinary pseudorepresentations and modular forms, Proc. Amer. Math. Soc. Ser. B **4** (2017), 53–71.

[WWE18] P. Wake and C. Wang-Erickson, Pseudo-modularity and Iwasawa theory. Amer. J. Math. **140** (2018), 977–1040.

[W74] A. Weil, Exercices dyadiques, Inventiones Math. **27** (1974), 1–22 (Œuvres III, [1974e]).

[Wi88] A. Wiles, On ordinary Λ-adic representations associated to modular forms, Inventiones Math. **94** (1988), 529–573.

[Wi90] A. Wiles, The Iwasawa conjecture for totally real fields, Annals of Mathematics **131** (1990), 493–540.

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

[Z14] B. Zhao, Local indecomposability of Hilbert modular Galois representations. Ann. Inst. Fourier (Grenoble) **64** (2014), 1521–1560.

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